CAPACIDADES TÉCNICAS LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

AUTOR

JAIDER FABIAN CONTRERAS PUENTES

UNIVERSIDAD ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
SINCELEJO, SUCRE
2021

CAPACIDADES TÉCNICAS LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

AUTOR

JAIDER FABIAN CONTRERAS PUENTES

DIRECTOR DE CURSO
JHON FREDY QUINTERO

UNIVERSIDAD ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
SINCELEJO, SUCRE
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Sincelejo, 10 de octubre de 2021

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

El presente informe técnico, permite comprender la importancia del papel que juegan los equipos “Red Team” y “Blue Team” dentro de la ciberseguridad de una organización. Es así como este informe, contempla el análisis de diferentes escenarios asociados con los aspectos éticos, legales y técnicos relacionados con la seguridad informática y de la información de la organización “The WhiteHouse Security”. Inicialmente se realiza la identificación y análisis de conductas y demás aspectos ilegales, contemplados en el acuerdo de confidencialidad dispuesto por esta organización, para firmar con las personas con las que llevará procesos contractuales dentro de la misma, que violen los artículos de la ley 1273 de 2009 referente a la seguridad de la información, y vulneren o transgredan aspectos éticos, tanto a nivel profesional como organizacional, teniendo en cuenta el código de ética, contenido en la ley 842 de 2003.

Desde una perspectiva más técnica, este informe, permite analizar y determinar la causa de la fuga de información dentro de la organización, así como la identificación y análisis de las vulnerabilidades dentro del sistema, para que luego se ejecuten las pruebas de intrusión que logren explotar las vulnerabilidades encontradas, y se culmine con la creación de un usuario con escalación de privilegios y con ello se logre tomar el control de la máquina objeto de estudio. Todo esto se realiza mediante la ejecución de las etapas de pentesting.

Finalmente, este informe considera el análisis de las acciones a revisar y ejecutar cuando se está frente a un ataque informático en tiempo real, dentro de los sistemas informáticos de la organización, permitiendo analizar y determinar medidas de hardenización, considerar el uso de estrategias, controles y herramientas dadas a través del CIS (Center For Internet Security), así como el de las características y funcionalidades de las tecnologías SIEM o software de Información de seguridad y gestión de eventos, y otras herramientas usadas para la detección y contención de ataques informáticos con el fin de fortalecer la ciberseguridad de los sistemas de la organización.

El resultado final de este informe es el de plantear recomendaciones, luego de las actividades realizadas por los equipos Red Team & Blue Team dentro de la organización, en el marco de los criterios éticos, legales y técnicos que permitan la formulación de estrategias de fortalecimiento de la seguridad informática de toda la infraestructura de TI de la organización “The WhiteHouse Security”.

ABSTRACT

This technical report allows us to understand the importance of the role played by the “Red Team” and “Blue Team” within the cybersecurity of an organization. Thus, this report contemplates the analysis of different scenarios associated with the ethical, legal and technical aspects related to computer and information security of the organization "The WhiteHouse Security". Initially, the identification and analysis of behaviors and other illegal aspects is carried out, contemplated in the confidentiality agreement established by this organization, to sign with the people with whom it will carry out contractual processes within it, that violate the articles of Law 1273 of 2009 regarding information security, and violate or violate ethical aspects, both professionally and organizationally, taking into account the code of ethics, contained in law 842 of 2003.

From a more technical perspective, this report makes it possible to analyze and determine the cause of the leakage of information within the organization, as well as the identification and analysis of vulnerabilities within the system, so that the intrusion tests that manage to exploit are then executed. the vulnerabilities found, and culminate in the creation of a user with privilege escalation and thereby take control of the machine under study. All of this is done by running the pentesting stages.

Finally, this report considers the analysis of the actions to review and execute when facing a computer attack in real time, within the computer systems of the organization, allowing to analyze and determine hardenization measures, consider the use of strategies, controls and tools provided through the CIS (Center For Internet Security), as well as the characteristics and functionalities of SIEM technologies or security information and event management software, and other tools used for the detection and containment of computer attacks with in order to strengthen the cybersecurity of the organization's systems.

The final result of this report is to make recommendations, after the activities carried out by the Red Team & Blue Team within the organization, within the framework of the ethical, legal and technical criteria that allow the formulation of strategies to strengthen the IT security for the entire IT infrastructure of the organization “The WhiteHouse Security”.

GLOSARIO

Amenaza: Escenario en el que una acción, que aprovecha una vulnerabilidad compromete la seguridad de un sistema informático.[1]

Ataque informático: Acción que aprovecha explota una vulnerabilidad con el fin de comprometer la seguridad de un sistema informático.[2]

Blue Team: Equipo conformado por profesionales de la seguridad informática que tienen como objetivo proteger los activos críticos de las organizaciones contra cualquier tipo de amenaza, fortaleciendo la seguridad informática para que ningún intruso pueda comprometer la infraestructura TI de esta.[3]

Ciberseguridad: Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.[4]

CIS: Organización cuyo objetivo es el de generar y desarrollar un amplio conocimiento en ciberseguridad, al alcance de todos, con mejores prácticas y controles que sirvan como soluciones que permitan fortalecer la seguridad informática de las organizaciones.[5]

Código de ética: normas y/o reglas que regulan el comportamiento de una persona en el ejercicio de su profesión dentro de una empresa u organización.[6]

CSIRT: (Equipo de respuesta a incidentes informáticos), encargado de accionar cuando ocurre un incidente de seguridad, a través del análisis del código malicioso, la investigación de las condiciones y análisis de cómo se produce el ataque, con el fin de ayudar a restablecer el sistema afectado, y contribuir en la gestión de vulnerabilidades detectadas.[7]

---

[1] (Ambit, Building Solutions Together, 2020)
[2] ibid.
[3] (Emagined, s.f.)
[4] (Kaspersky, s.f.)
[5] (CIS, Center for Internet Security, s.f.)
[6] (Concepto, s.f)
[7] (Searchdatacenter, 2012)

Escalación de Privilegios: acción mediante la cual un atacante luego de explotar una vulnerabilidad, se asigna privilegios de administrador en el sistema comprometido.[8]

Exploit: Secuencia de comandos utilizados para el aprovechamiento de un fallo o vulnerabilidad en un sistema informático, cuyo fin es el acceso no autorizado a dicho sistema, la obtención de permisos de administración y la generación de un ataque de denegación de servicio a este.[9]

Fail2ban: es una aplicación software basada en Python y se usa para prevenir ataques por intrusión a un sistema. Fail2ban opera escaneando los archivos de registro y permite bloquear direcciones IP que evidencian signos maliciosos, como lo son demasiado intentos fallidos de contraseña, búsqueda de exploits, entre otros. Este software se usa para actualizar las reglas del firewall y el bloqueo de direcciones IP durante un período de tiempo específico y provee diferentes filtros para varios servicios (apache, SSH, etc.).[10]

Firewall: Sistema o dispositivo que permite la configuración de reglas de acceso y denegación dentro de un sistema informático. Un firewall puede ser un software o un dispositivo de red que se encarga de la protección y la seguridad perimetral en una infraestructura TI.[11]

KaliLinux: Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.[12]

Ley: Regla o norma establecida por una autoridad superior para regular, de acuerdo con la justicia, algún aspecto de las relaciones sociales.[13]

Nmap: Es una herramienta de fuente abierta que permite el escaneo de puertos y brindar información acerca de hosts de una red, dando facilidad de conocer que hosts se encuentran activos, que puertos se encuentran abiertos, y si existen firewall activados en ellos, así como conocer que servicios se encuentran ejecutándose.[14]

---

[8] (Redeszone, 2020)
[9] (Pandasecurity, s.f.)
[10] (Fail2ban, 2016)
[11] (Mcafee, s.f).
[12] (Ecured, s.f.)
[13] (Oreamuno, s.f.).
[14] (Redeszone, 2021)

Metasploit Framework: Es una herramienta de código abierto, que permite investigar vulnerabilidades y posee una base de datos con una gran variedad de exploits de vulnerabilidades que permiten la explotación de las mismas.[15]

OSSIM: Es un producto de software, de código abierto creado por AlienVault, para la gestión de aspectos seguridad de la información y permite la gestión de eventos (SIEM), proporcionando un SIEM completo con recolección de eventos, que tiene la característica de actuar como un sistema de prevención de intrusos teniendo como base información correlativa de cualquier fuente, que le permite constituirse en una herramienta útil dentro de la seguridad informática.[16]

Payload: Es la carga útil (carga dañina) o datos transmitidos por un exploit que permite detonar un ataque y afectar la seguridad de un sistema informático.[17]

Pentesting: test o pruebas de penetración, diseñadas para determinar el alcance de los fallos de seguridad de los sistemas informáticos o redes de una organización.[18]

Red Team: Equipos conformado por profesionales de la seguridad informática que evalúan la seguridad de los sistemas de manera objetiva, utilizando técnicas y herramientas disponibles para encontrar vulnerabilidades y superar los controles de seguridad a través de ataques simulados, para luego plantear recomendaciones y planes que permitan fortalecer la seguridad de los sistemas e infraestructura TI de las organizaciones.[19]

SIEM: (Security Information and Event Management), es una de tecnología de software muy potente dentro de la seguridad informática que permite, recopilar unificadamente información de todos los sistemas y dispositivos y los eventos presentados alrededor de los mismos, permitiendo a las organizaciones y profesionales en TI, el análisis de toda la información recolectada con el fin de fortalecer la ciberseguridad de estas.[20]

---

[15] (Openwebinars,2018)
[16] (Incibe, s.f)
[17] (PRIETO BRITO, ALEXIA, Qué!, 2020)
[18] (Incibe, 2019)
[19] (Emagined, s.f.)
[20] (SOFECOM, s.f.)

Vulnerabilidad: Debilidad dentro de un sistema informático, que puede ser explotada para comprometer la seguridad de este.[21]

WAF: Web Application Firewall (WAF) es un tipo de firewall que permite garantizar la seguridad del servidor web mediante el análisis de paquetes de petición HTTP / HTTPS y modelos de tráfico.[22]

Wazuh: Es una herramienta software de código abierto que permite la detección y contención de amenazas, permitiendo dar respuesta a los incidentes de seguridad presentados.[23]

[21] Ambit, Building Solutions Together, 2020)
[22] (Oracle, s.f.)
[23] (Wazuh, s.f.)

INTRODUCCIÓN

Los ciberataques a los sistemas informáticos de las empresas son una realidad en aumento, actualmente en el mundo. Estos logran aprovecharse de las vulnerabilidades existentes en los sistemas, y demás aspectos relacionados con la forma como se gestiona la seguridad informática y/o de la información, al interior de las empresas, provocando violaciones y afectaciones a la confidencialidad, integridad y disponibilidad de la información. La seguridad de la información y la ciberseguridad en general, por ende, son aspectos muy importantes que se deben considerar con mucha seriedad para prevenir o mitigar el riesgo de estos ataques a los activos de la empresa. Es por ello, que muchas organizaciones a nivel mundial, han empezado a implementar metodologías que permiten identificar y detectar vulnerabilidades en sus sistemas a través del hacking ético y la contratación de profesionales expertos en seguridad informática, para conformar equipos Red Team y Blue Team, quienes trabajan en conjunto para mejorar los aspectos de ciberseguridad de dichas organizaciones, no solo para prevenirlas de amenazas externas, sino también al interior de la misma, pues muchos de estos ataques son perpetrados en complicidad de personal que labora en las mismas organizaciones.

Este informe permite analizar los diferentes escenarios presentados en la organización “The WhiteHouse Security” en los aspectos de ciberseguridad, desde perspectivas como la ética profesional, el marco legal colombiano, y desde los mismos aspectos técnicos especializados de la práctica de pentesting y demás actividades llevadas a cabo por los equipos Red Team y Blue Team, quienes juegan un papel muy importante en la identificación, análisis y explotación controlada de las vulnerabilidades de un sistema informático, a partir del uso de metodologías y técnicas de intrusión. Así mismo, el resultado de la auditoría desarrollada y presentada a través de este informe, permite definir y establecer las recomendaciones, políticas de seguridad, y medidas de prevención y contención, planteadas por el equipo Blue Team, frente a estos ataques, logrando fortalecer la seguridad informática y/o ciberseguridad de los sistemas de la organización, apoyados en metodologías y herramientas, tales como tecnologías SIEM y la implementación de buenas prácticas de seguridad como las expuestas por la CIS (Center for Internet Security).

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Desarrollar y generar un informe técnico, que permita establecer las capacidades técnicas, legales y de gestión, relacionadas a un equipo Blue Team y Red Team, con el fin de definir las medidas, lineamientos, políticas y procedimientos a implementar dentro de la ciberseguridad de la organización “The WhiteHouse Security”.

1.2. OBJETIVOS ESPECÍFICOS

- Analizar y evaluar las acciones de los equipos Red Team & Blue Team de la organización “The WhiteHouse Security” en el marco de los criterios éticos y legales.

- Identificar, analizar y explotar las vulnerabilidades en un sistema informático de la organización “The WhiteHouse Security”, a partir del uso de metodologías de pentesting y técnicas de intrusión.

- Formular y establecer las medidas y estrategias de contención mediante el análisis de riesgos y vulnerabilidades de la infraestructura TI de la empresa “The WhiteHouse Security” con el fin de fortalecer la ciberseguridad de esta organización.

2. DESARROLLO DEL INFORME.

2.1. MONTAJE BANCO DE TRABAJO

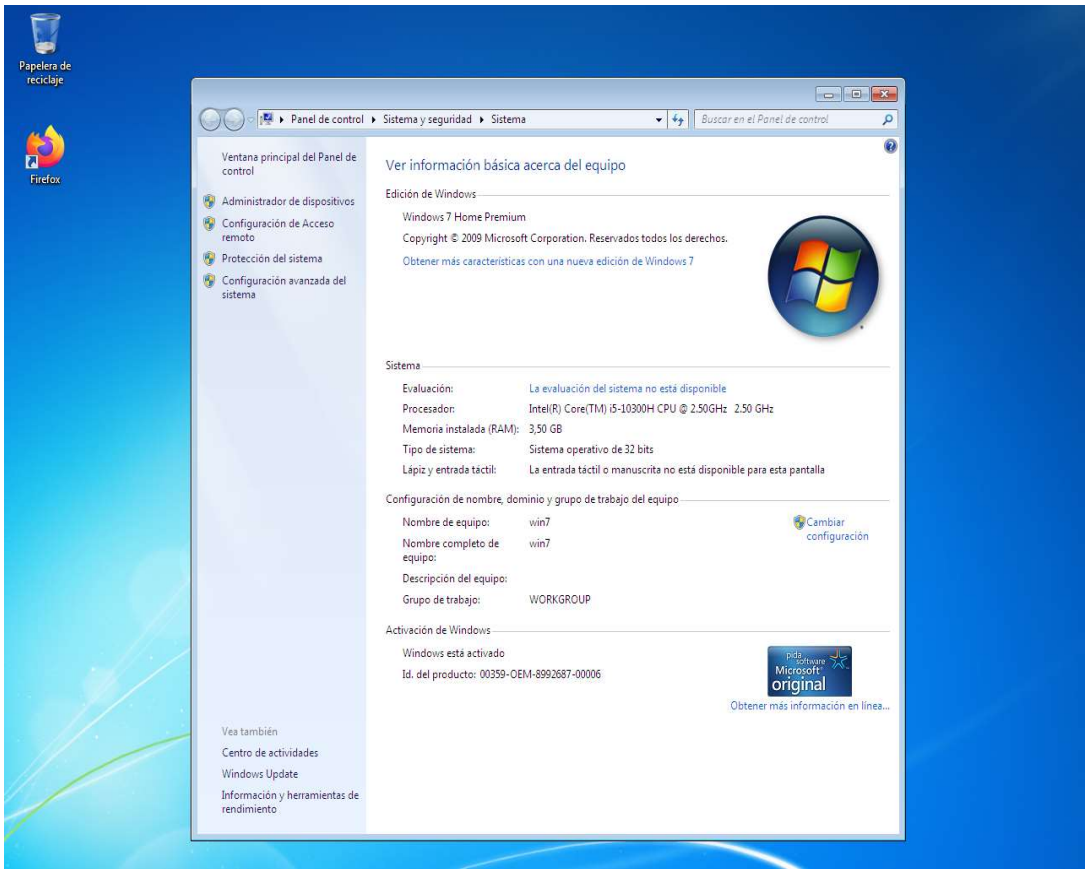
2.1.1. MAQUINA 1: WINDOWS 7 (32 bits)

Se logra evidenciar la instalación de la máquina Windows 7 (32 bits) con nombre **win7** y las siguientes características técnicas principales:

Tabla 1: Características de la máquina 1 (Windows 7 - 32 bits)

Procesador	Intel Core I5 -10300H CPU 2.50GHz
Memoria Ram	4 GB
Disco Duro	50 GB
Sistema Operativo	Windows 7
Tipo de Sistema	32 bits

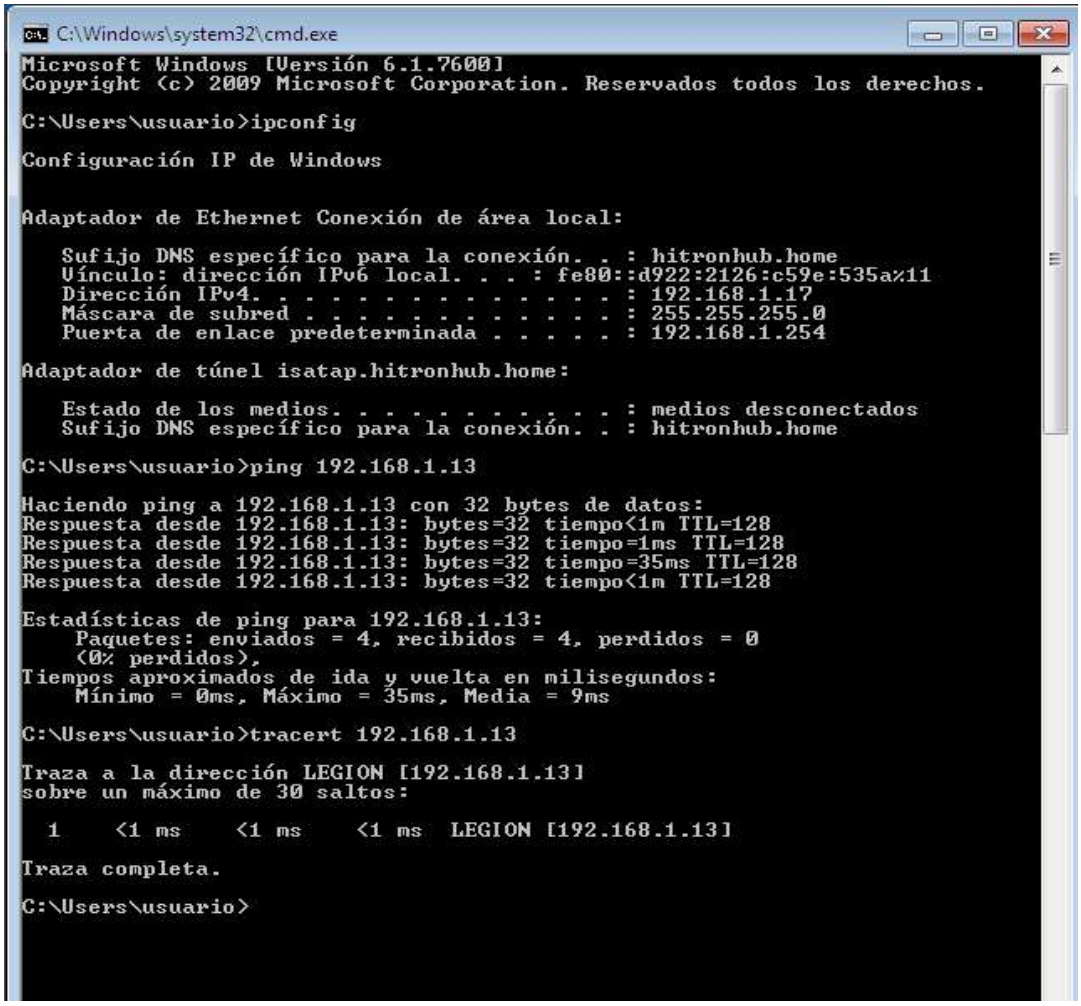
Figura 1: Características de la máquina 1 (Windows 7 - 32 bits)



Fuente 1: el autor

Se evidencia que existe comunicación con el equipo o máquina anfitrión:

Figura 2: Comunicación de la máquina 1 (Windows 7 a 32 bits) con la máquina anfitrión.



Fuente 2: el autor

Se evidencia, primeramente, que la máquina tiene como dirección IPv4 la dirección **192.168.1.17**. Con el comando **ping,** se puede validar a satisfacción, la conexión a la máquina anfitrión con dirección IPv4: **192.168.1.13**. Al igual, se puede corroborar a satisfacción la traza de transmisión de paquetes al utilizar el comando **tracert** hacia la misma dirección IP del equipo anfitrión.

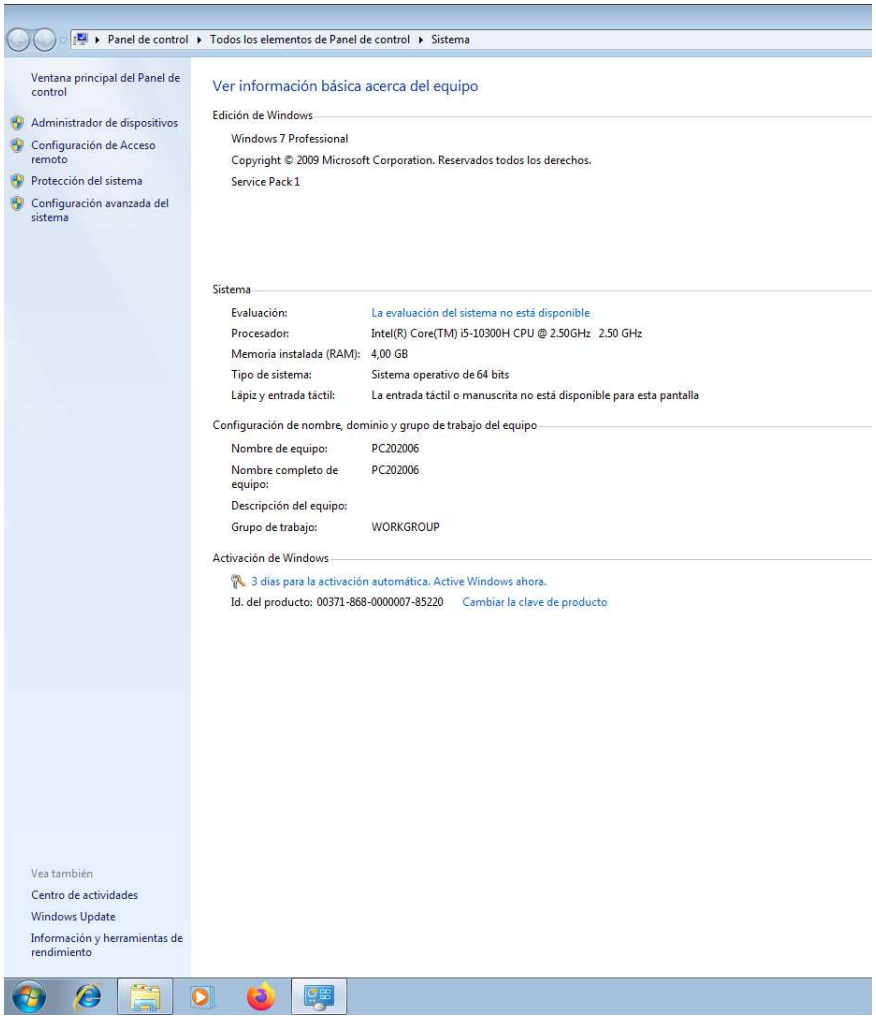
2.1.2. MAQUINA 2: WINDOWS 7 (64 bits)

Se logra evidenciar la instalación de la máquina Windows 7 (64 bits) con nombre **PC202006** y las siguientes características técnicas principales:

Tabla 2: Características de la máquina 2 (Windows 7 a 64 bits)

Procesador	Intel Core I5 -10300H CPU 2.50GHz
Memoria Ram	4 GB
Disco Duro	50 GB
Sistema Operativo	Windows 7
Tipo de Sistema	64 bits

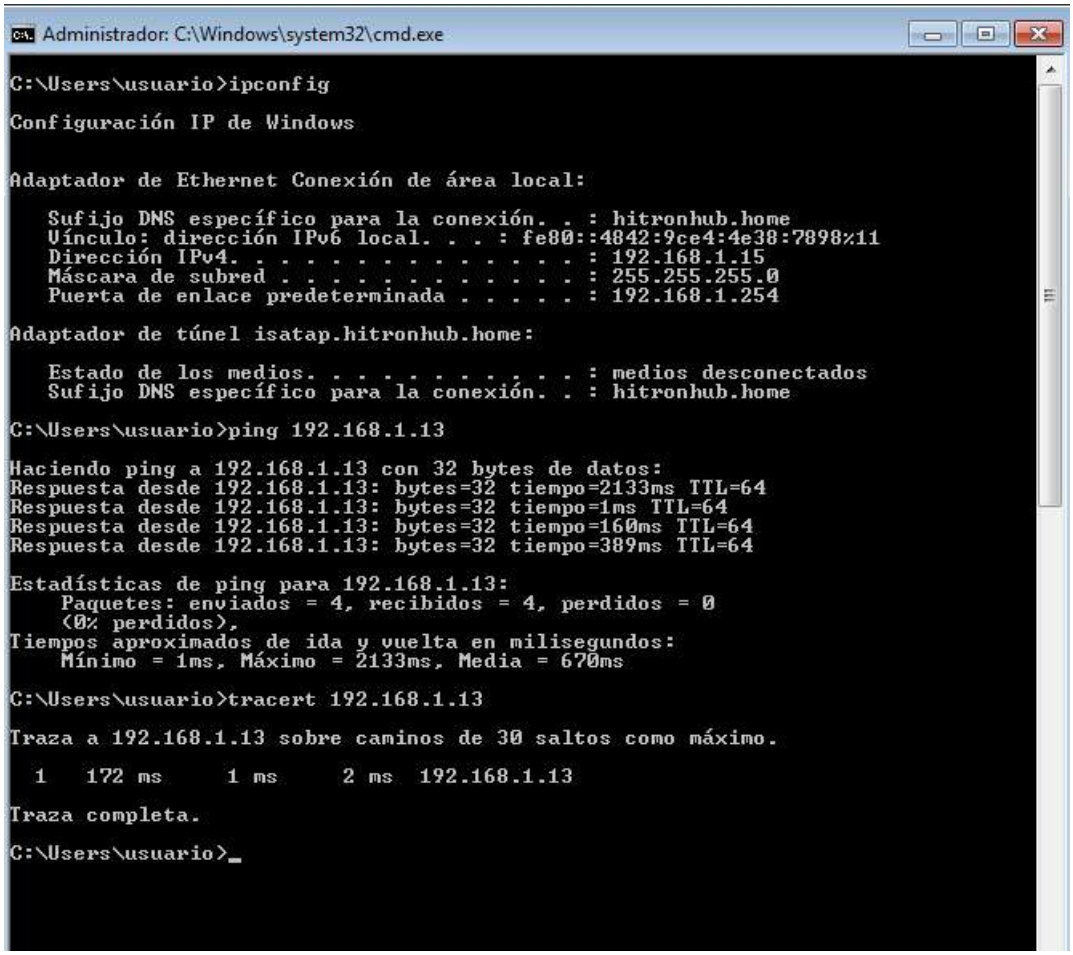
Figura 3: Características de la máquina 2 (Windows 7 a 64 bits)



Fuente 3: el autor

Se evidencia la comunicación con el equipo o máquina anfitrión:

Figura 4: Comunicación de la máquina 2 (Windows 7 a 64 bits) con la máquina anfitrión



Fuente 4: el autor

Se puede evidenciar, que la máquina tiene como dirección IPv4 la dirección **192.168.1.15**. El comando **ping** permite validar la conexión a la máquina anfitrión con dirección IPv4: **192.168.1.13**. Al igual, que el uso del comando **tracert** permite corroborar a satisfacción la traza de transmisión de paquetes hacia la misma dirección IP del equipo anfitrión.

2.1.3. MAQUINA 3: KALILINUX (64 bits)

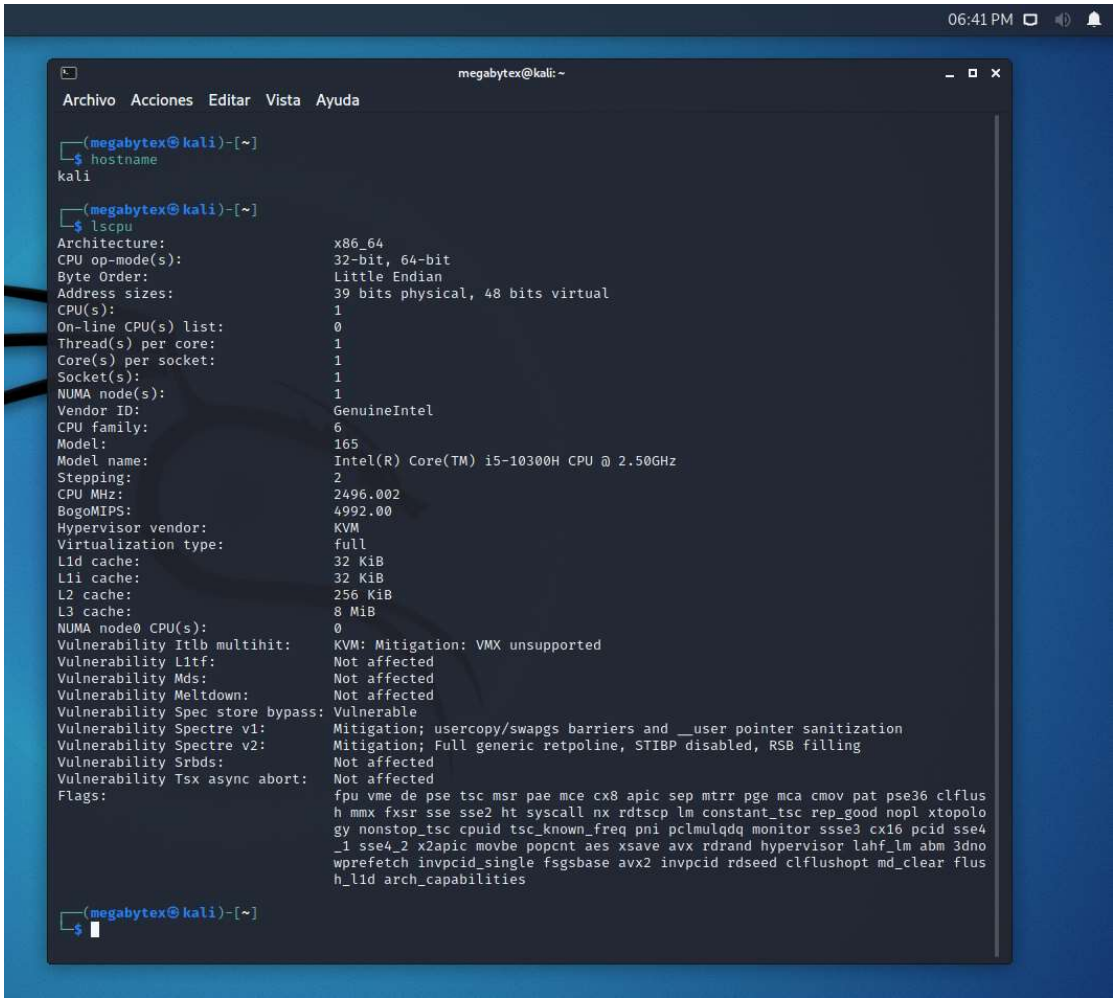
Se evidencia la instalación de la máquina KaliLinux (64 bits) con nombre **Kali** y las siguientes características técnicas principales:

Tabla 3: Características de la máquina 3 (KaliLinux - 64 bits)

Procesador	Intel Core I5 -10300H CPU 2.50GHz

Memoria Ram	4 GB
Disco Duro	20 GB
Sistema Operativo	KaliLinux (Debian 6)
Tipo de Sistema	64 bits

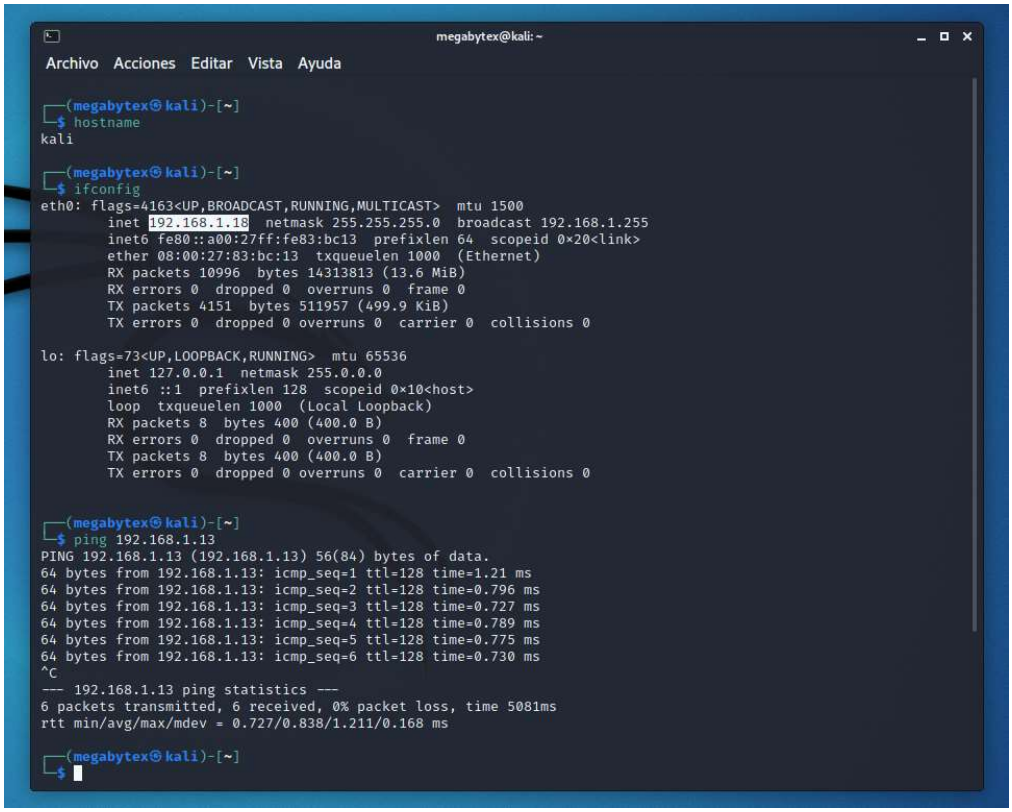
Figura 5: Características de la máquina 3 (KaliLinux - 64 bits)



Fuente 5: el autor

Se valida la comunicación con el equipo o máquina anfitrión:

Figura 6: Comunicación de la máquina 3 (KaliLinux - 64 bits) con la máquina anfitrión.



Fuente 6: el autor

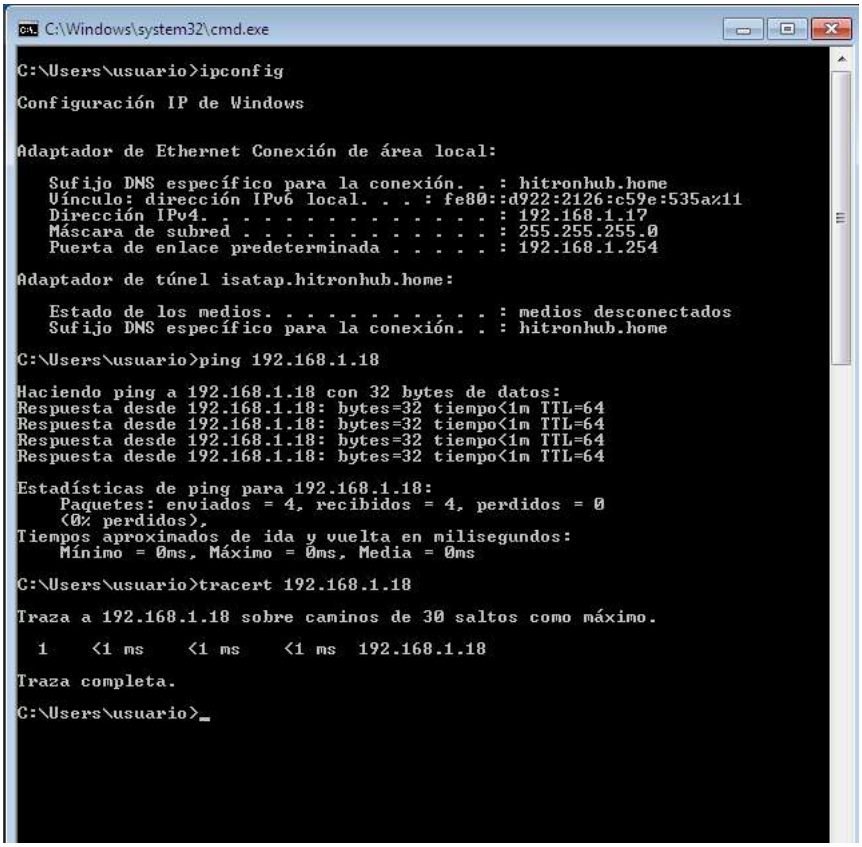
Se evidencia, que la máquina tiene como dirección IPv4 la dirección **192.168.1.18**. Así mismo, el comando **ping** permite evidenciar la conexión a la máquina anfitrión con dirección IPv4: **192.168.1.13**, a satisfacción.

2.1.4. COMUNICACIÓN ENTRE LAS MÁQUINAS VIRTUALES.

A continuación, se evidencia la comunicación entre las máquinas virtuales:

- **Comunicación entre la máquina 1 (Windows 7 – 32 bits) y la máquina 3 (KaliLinux).**

Figura 7: Comunicación de la máquina 1 (Windows 7 - 32 bits) con la máquina 3 (KaliLinux).

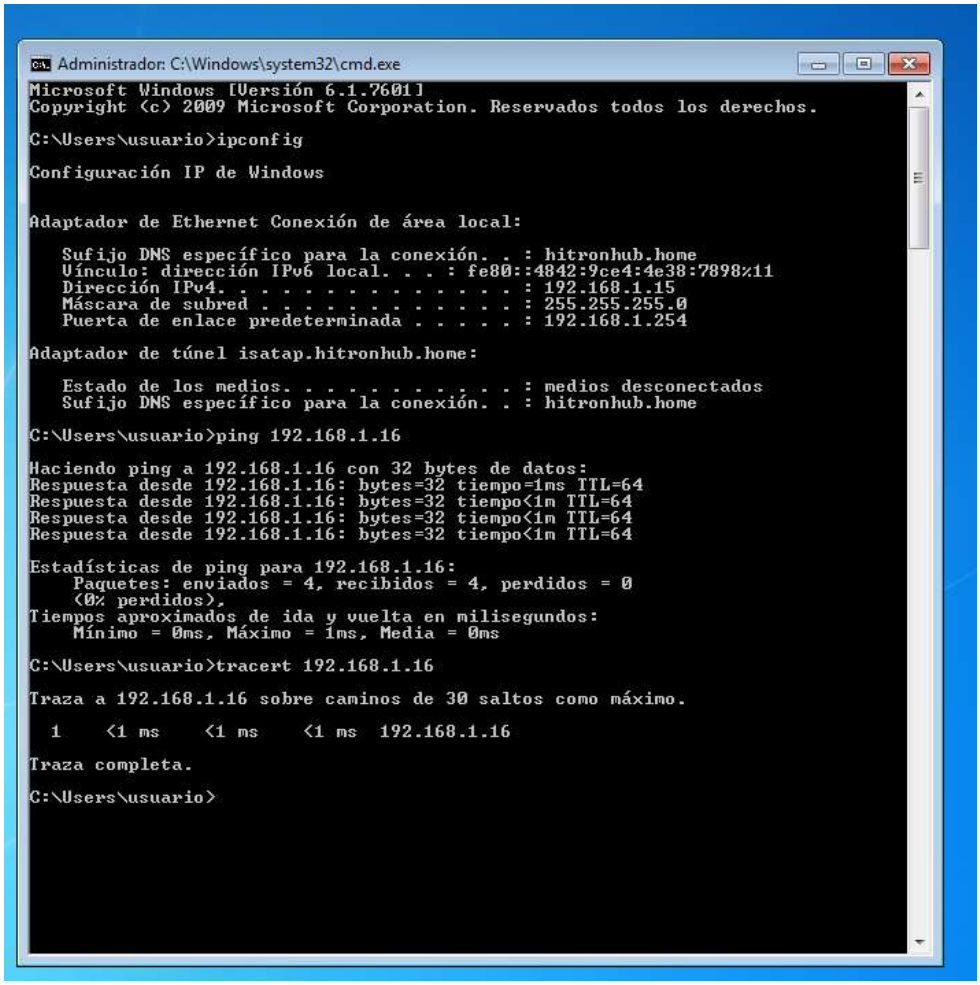


Fuente 7: el autor

En la figura 7, se evidencia, que la máquina Windows 7 (32 bits) tiene dirección IPv4 (**192.168.1.17**) y existe conexión entre dicha máquina y la máquina KaliLinux con dirección IPv4: **192.168.1.18**. De la misma manera, en la figura se puede corroborar a satisfacción la traza de transmisión de paquetes arrojada con el uso del comando **tracert** hacia la misma dirección IP de dicha máquina KaliLinux.

- **Comunicación entre la máquina 2 (Windows 7 – 64 bits) y la máquina 3 (KaliLinux).**

Figura 8: Comunicación de la máquina 2 (Windows 7 - 64 bits) con la máquina 3 (KaliLinux).

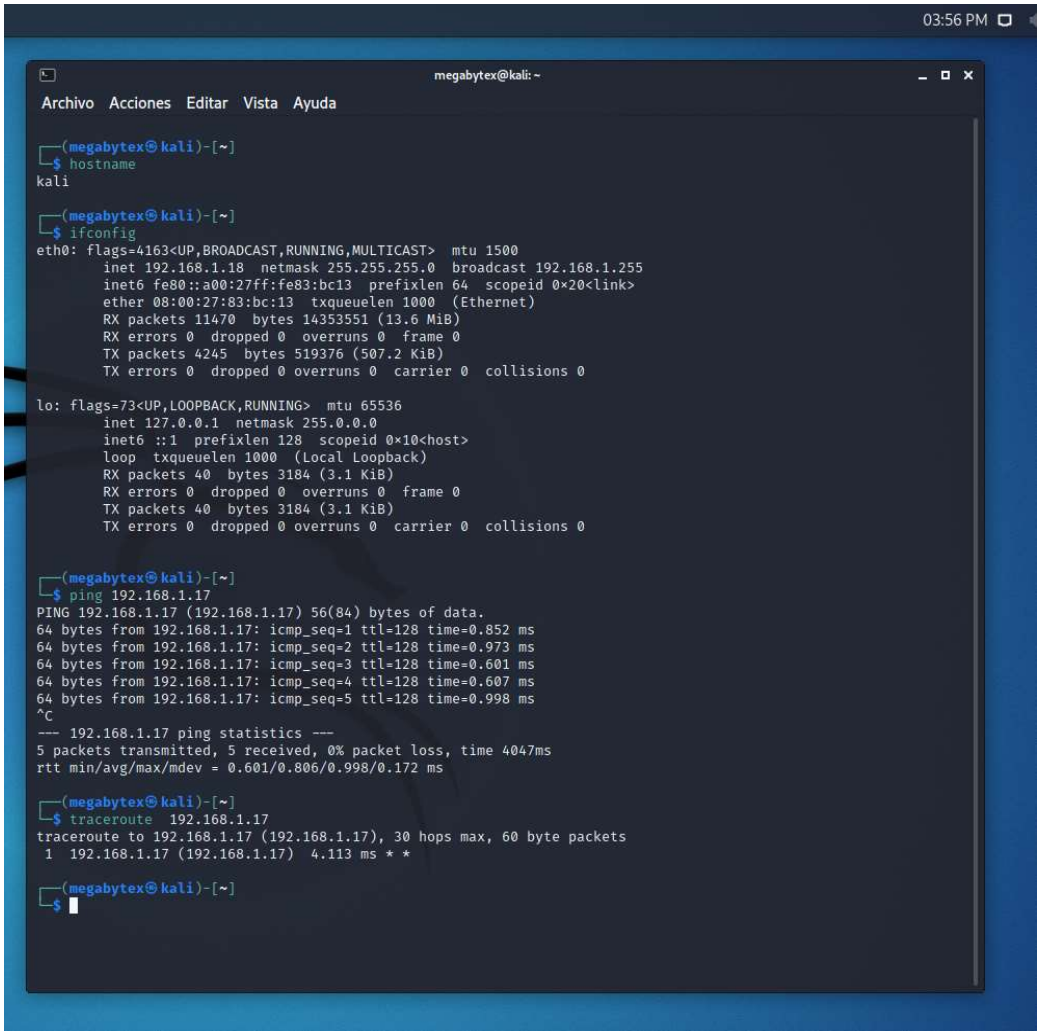


Fuente 8: el autor

En la figura 8, se evidencia, además de la dirección IPv4 (**192.168.1.15**) de la máquina Windows 7 (64 bits), existe conectividad con la máquina KaliLinux con dirección IPv4: **192.168.1.16**. De la misma manera, se puede corroborar en dicha figura, que la traza de transmisión de paquetes al utilizar el comando **tracert** hacia la misma dirección IP de dicha máquina KaliLinux fue exitosa.

- **Comunicación entre la máquina 3 (KaliLinux – 64 bits) y la máquina 1 (Windows 7 – 32 bits).**

Figura 9: Comunicación de la máquina 3 (KaliLinux) con la máquina 1 (Windows 7 - 32 bits).

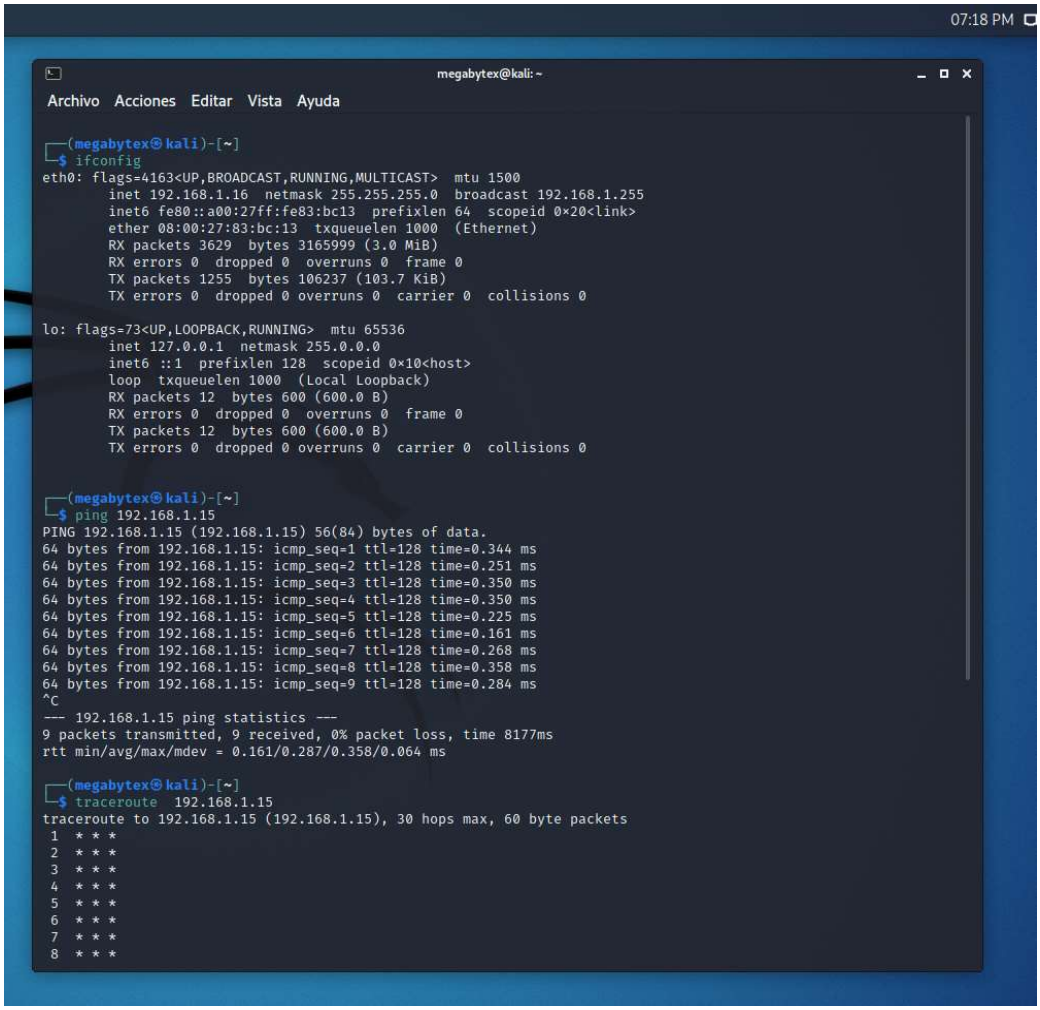


Fuente 9: el autor

En la figura anterior, se evidencia, además de la dirección IPv4 (**192.168.1.18**) de la máquina KaliLinux, que existe conexión a la máquina Windows 7 (32 bits) con dirección IPv4: **192.168.1.17**. De la misma manera, se puede corroborar en esta figura, que la traza de transmisión de paquetes al utilizar el comando **traceroute** hacia la misma dirección IP de dicha máquina Windows 7 (32 bits) fue exitosa.

- **Comunicación entre la máquina 3 (KaliLinux – 64 bits) y la máquina 2 (Windows 7 – 64 bits).**

Figura 10: Comunicación de la máquina 3 (KaliLinux) con la máquina 2 (Windows 7 - 64 bits).



Fuente 10: el autor

En la figura 10, se evidencia, además de la dirección IPv4 (**192.168.1.16**) de la máquina KaliLinux, que existe conectividad a satisfacción con la máquina Windows 7 (64 bits) con dirección IPv4: **192.168.1.15**. De igual forma, se puede corroborar en la misma figura, que la traza de transmisión de paquetes al utilizar el comando **traceroute** hacia la misma dirección IP de dicha máquina Windows 7 (64 bits) fue exitosa.

2.2. ANALISIS ETICO Y LEGAL.

2.2.1. Análisis del “Escenario 2” y “Acuerdo de confidencialidad” de la empresa “The WhiteHouse Security” desde el punto de vista legal y no ético.

Escenario 2: ***“****La organización WhiteHouse Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.*

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

Teniendo en cuenta la situación planteada en el escenario 2 y el acuerdo de confidencialidad anexo a este informe, se logra evidenciar, que el acuerdo mismo, en gran parte de su contenido, es una muestra fidedigna de ilegalidad, que adicionalmente va en detrimento de la ética profesional de las personas a contratar, así como de la ética a nivel organizacional.

Desde el punto de vista legal, si bien la organización pretende con dicho acuerdo, garantizar “legalmente” por escrito que la confidencialidad de la información y los procesos al interior de la organización que se comparten entre las partes involucradas, se encuentren bajo reserva y no divulgación, que es en esencia el objeto de un acuerdo de confidencialidad, ciertamente la información relacionada u obtenida mediante procesos ilegales no debe formar parte de un

acuerdo de confidencialidad, por su naturaleza precisamente ilegal, y mucho menos debería denominarse esta información como confidencial, y con ella advertir prohibiciones en la divulgación o denuncia ante autoridades legales, o responsabilizar a la parte receptora, denominada así en el acuerdo, de las acciones que sobrevengan de la divulgación de este tipo de información ante dichas autoridades.[24] Más allá que los artículos 194 y 308 del código penal colombiano, establezcan y regulen *"la divulgación y empleo de documentos que deben permanecer en reserva o secreto"*, y *"la violación de reserva industrial o comercial"*[25], estos no respaldan penas para la divulgación de información inmersa u obtenida a través procesos ilegales. Así mismo, dicho "acuerdo" muestra ser abusivo y temerario al dejar consignado responsabilidades al profesional que se pretende contratar, si llegase a encontrársele con información ilegal al momento de surtirse un allanamiento por parte de autoridades legales, teniendo en cuenta que esta información pertenece a la organización y es producto de los procesos ilegales ejecutados por esta, y lo que se evidencia en estas cláusulas es simplemente la evasión de responsabilidades ante autoridades competentes, de actividades propias de la organización sumidas de irregularidades e ilegalidad.

Desde el enfoque ético, es importante resaltar que gran parte de lo consignado en este acuerdo, incurre en acciones que van en contra de la ética profesional de las personas a contratar, pues atenta contra el buen accionar de un profesional ético, que siempre busca la excelencia humana, a través de la realización de acciones correctas y la toma de decisiones racionales en pro del bienestar individual y colectivo.[26] Este acuerdo, obliga a los profesionales a contratar, a aceptar el ejercicio de conductas contrarias a la ética profesional y busca transgredir el código de ética mismo, contenido en la ley 842 de 2003, el cual expone ciertos deberes a nivel profesional, entre los que se pueden precisamente destacar los contemplados en el artículo 31, Capitulo 2, *"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.", y el* artículo 39, del mismo capitulo, *"Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo*

[24] (Asuntos Legales, 2019)
[25] (Organización de Estados Americanos, 2000)
[26] Welivesecurity, 2016)

obligación legal de revelarla o requerimiento del Consejo Profesional respectivo.", entre otros.[27]

Adicionalmente, este acuerdo expone a la organización a cuestionamientos en su código de ética organizacional, porque atenta en contra de los valores éticos que una empresa debe contemplar en la consecución de sus metas y en la confianza que genera al interior de sus empleados y su imagen ante la sociedad. En este sentido, Adela Cortina[28], catedrática de Ética en la Universidad de Valencia y directora de la Fundación ETNOR (Ética de los Negocios y las Organizaciones), expone que *"En una organización hay que tener como meta crear un clima ético, con unos valores que todas las personas compartan donde se toman decisiones y se actúa teniendo en cuenta estos valores", "La ética en una organización es rentable, genera confianza y reputación. La responsabilidad social y la ética de empresa es un buen instrumento de gestión".*

En el detalle específico del contenido del acuerdo, se encuentran los siguientes hallazgos, que denotan procesos ilegales y no éticos:

- **Clausula primera: objeto:**

  En esta cláusula del acuerdo, la empresa "The WhiteHouse Security" establece que la información confidencial o sobre **procesos ilegales** al interior de su organización no podrán ser divulgados.

- **Clausula segunda: Definición de información confidencial:**

  En esta cláusula del acuerdo, la empresa "The WhiteHouse Security" define dentro de su información confidencial los "datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"

- **Clausula Tercera. Origen de la información confidencial:**

  En esta cláusula, la empresa "The WhiteHouse Security" expone los orígenes de sus documentos y de la información en general. Inicialmente no se infiere

[27] (Copnia, 2015)
[28] (Floridauniversitaria, 2014)

irregularidad o ilegalidad. Sin embargo, se hace mención que dicha información o documentos se pueden obtener, “independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.”

- **Clausula Cuarta. Obligaciones de la parte receptora**

En esta cláusula, la empresa “The WhiteHouse Security” enfatiza en el enciso o numeral 3, 4 y 9, en no denunciar, compartir o revelar ante las autoridades las actividades sospechosas de espionaje y/o divulgar la información obtenida de manera ilegal compartida en medio de las labores ejercidas en la empresa, o producto de reuniones sostenidas.

Así mismo, en los numerales 7 y 8 atañe al profesional a contratar, denominado parte receptora de la información en dicho acuerdo, responsabilidades frente al mal uso de la información confidencial que le den sus representantes y frente a las autoridades competentes de llegarse a presentar procesos de allanamiento.

- **Clausula Sexta. Responsabilidad:**

En esta cláusula, se logra evidenciar la aseveración por parte de la empresa con mayor firmeza y temeridad, respecto a la responsabilidad de cumplimiento del acuerdo, incluyendo sus irregularidades e ilegalidades, por parte del profesional a contratar, frente a la aceptación de cada una de las cláusulas que denotan ilegalidad, quien deberá asumir la responsabilidad por los perjuicios morales y económicos que puedan sufrir la contra parte o los terceros afectados, como resultado del incumplimiento de las obligaciones contenidas en dicho acuerdo.

- **Clausula Octava. Solución de controversias:**

En correlación con los numerales 7 y 8 de la cláusula cuarta, se menciona en esta cláusula que, de firmarse el acuerdo, aún con sus irregularidades, la persona a contratar es responsable ante las autoridades de la información ilegal que se le encuentre, denominada también por la empresa como información confidencial, dejando libre de responsabilidad legal y penal a “WhiteHouse Security”.

En resumen, este acuerdo constituye una falta grave al marco legal que respalda la concepción de los acuerdos de confidencialidad, la seguridad de la información, contemplada en la ley 1273 de 2009[29] y la ley 842 de 2003 que enmarca el código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares.

2.2.2. Análisis del "Escenario 2" y "Acuerdo de confidencialidad", con relación a la vulneración de la ley 1273 de 2009.

Los artículos de la ley 1273 de 2009, que se vulneran en el denominado "acuerdo" son los siguientes:

- **Artículo 269A:** Acceso abusivo a un sistema informático.
- **Artículo 269C:** Interceptación de datos informáticos.
- **Artículo 269F:** Violación de datos personales, en lo referente a la interceptación de datos.
- **Artículo 269H:** Circunstancias de agravación punitiva, numeral 1; Específicamente en lo concerniente al acceso abusivo sobre redes, sistemas informáticos o de comunicaciones estatales u oficiales, teniendo en cuenta que la empresa "Whitehouse Security" es una organización de reconocimiento mundial que se encarga de asesorar a grandes Gobiernos en ciberseguridad y ciberdefensa, y en ese ámbito se infiere que sus interceptaciones y accesos abusivos a sistemas informáticos, los realice también a gobiernos o funcionarios del mismo.

- **Artículo 269I:** Hurto por medios informáticos y semejantes.
- **Artículo 269J:** Transferencia no consentida de activos, considerando que la información es el principal activo de una organización y la interceptación de esta, se constituye en una transferencia no consentida de la misma.

La cláusula segunda del acuerdo, la cual define dentro de su información confidencial aquella relacionada con "datos secretos producto de chuzadas, aquellos que son el resultado de interceptación de información, accesos abusivos a sistemas informáticos", es la mayor evidencia de la violación cometida por la empresa "The WhiteHouse Security", frente a los artículos de la

[29] (Policía, s.f.)

ley 1273 de 2009, la cual vela, en términos generales, por la protección de la información y de los datos, y propende la preservación integral de los sistemas que utilicen las tecnologías de la información y las comunicaciones. Esta organización sin duda alguna, no solo incurre en acciones delictivas en contravía de lo expuesto en dicha ley, al momento de ejecutar accesos abusivos a sistemas informáticos y realizar interceptaciones de información, sino que también comete violaciones a la Ley 1621 de 2013 o Ley de inteligencia y contrainteligencia, que establece *"la interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el Artículo 15 de la Constitución (derecho a la intimidad) y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales"*[30], y en su Articulo 3, expresa que los únicos autorizados para realizar las interceptaciones son los organismos dentro del Estado (Fiscalía, la Dirección Nacional de Inteligencia, y la Dirección de Inteligencia de la Policía e inteligencia militar), de acuerdo a la naturaleza de la investigación y contando con las autorizaciones legales respectivas.

2.2.3. Análisis de propuesta laboral, basado en el análisis del "escenario 2" y acuerdo, desde el punto de vista legal y ético.

Luego del análisis ético-legal respecto al acuerdo de la empresa "The WhiteHouse Security", se debe rechazar la propuesta de trabajo de esta empresa, teniendo en cuenta que la misma atenta contra la ética personal y profesional, la cual trasciende más allá del poder y el dinero, ya que como seres humanos siempre se debe estar claro frente a la toma de decisiones racionales y correctas, buscando siempre la excelencia y el beneficio individual y colectivo que no perjudique o vaya en detrimento del ejercicio de la profesión y/o afecte a los demás. Todo ingeniero debe tener la responsabilidad de velar por el buen prestigio de la profesión, como lo establece el código de ética en su Articulo 35, referente a los deberes de los profesionales para con la dignidad de sus profesiones. Así mismo, el código de ética, en este mismo artículo establece que, se debe respetar todas las disposiciones legales y reglamentaras que transgredan en actos de las profesiones, las cuales se deben denunciar. En ese mismo sentido, el artículo 34 plantea claramente que no se debe ofrecer o aceptar trabajos que vayan en contra de las disposiciones legales vigentes.[31]

[30] (Dirección nacional de Inteligencia, 2013)
[31] (Copnia, 2015)

Se debe actuar siempre bajo una conducta ética que le dé valor y honor a la profesión de ingeniero, donde se tomen siempre las mejores decisiones, y no se acepten por imposición, conductas tales como las que fueron reflejadas en el acuerdo analizado, que sin duda alguna, se reitera, es una violación completa al código de ética de esta profesión.

2.2.4. Análisis del caso "Operación Andromeda Buggly" desde su posición teniendo en cuenta los aspectos legales y éticos.

El caso "Operación Andrómeda Buggly", es un caso peculiar de inteligencia militar que, según las informaciones oficiales de las autoridades competentes, se salió de control y dejó varios oficiales, suboficiales, y demás uniformados fuera del servicio militar, algunos de ellos presos, al igual que el civil Andrés Sepúlveda, llamado "el hacker". En el caso de los uniformados se les retira del servicio por actuar en contra del código de honor y ética de la institución militar, pero especialmente por cometer delitos penales en contra de la seguridad de la información, mismos delitos cometidos por el civil Sepúlveda. Este caso, pone de manifiesto una operación de inteligencia militar, mal manejada, que utilizaba una fachada, aparentemente legal que buscaba supuestamente adquirir conocimientos dentro del hacking ético, con el fin de detectar amenazas en ciberseguridad. El desmantelamiento de la operación, por parte de la fiscalía, sin duda alguna, expuso públicamente a las fuerzas militares en un escándalo que va en detrimento de la ética y el marco legal colombiano en cuanto a la seguridad de la información y el derecho a la intimidad, expuesto en el artículo 15 de la constitución política, pues en esta fachada se cometían delitos a la ley 1273 de 2009, como la interceptación de datos a través del uso de malware o acceso abusivo a sistemas informáticos, entre otras. La interceptación de comunicaciones no autorizadas también era una de las prácticas delictivas ejercidas dentro de esta operación y adicionalmente el no control de información reservada termina en manos de particulares, como lo reflejó la investigación. Mucha de esta información, incluso fue vendida a terceros y/o particulares, para fines de lucro propio, como se menciona también en la investigación. A pesar de las actuaciones legales de las fuerzas militares y autoridades competentes, quedó en evidencia también, las fallas y falta de control de estas, en este tipo de operaciones, tales como la falta de control sobre el personal que visitaba la

fachada, y el no haber realizado estudios de seguridad para los agentes que hicieron parte de la operación, entre otras.[32]

En resumen, esta operación es un atentado en contra de la ética de las instituciones militares del país, y la sociedad misma, y una violación absoluta al marco legal de la seguridad de la información, que quebranta la confianza en las instituciones que se supone deben velar por la protección y seguridad en todo sentido.

2.3. ANALISIS SITUACIONAL EQUIPO RED TEAM.

SITUACIÓN PROBLEMA: El escenario planteado propone lograr la identificación de los medios por los cuales se está produciendo fugas de información en la organización. Se tiene conocimiento que dicha fuga se está presentando en una de máquinas de cómputo de esta empresa, y adicionalmente se conoce que en éste se encuentra instalada una aplicación llamada “rejetto v. 2.3” bajo el sistema operativo “Windows 7” con arquitectura X64. Se presume que esta aplicación contiene un exploit que puede ser usado por el atacante como Shell Reversa, que le permite abrir una sesión de meterpreter y con ello crear un usuario con escalamiento de privilegios y generar afectaciones a la seguridad de la información de dicho sistema y por ende a la organización.

Es por ello por lo que se realiza un proceso de pentesting para analizar lo solicitado en la situación anterior. A continuación, se evidencian las acciones realizadas en cada una de las fases de las pruebas de penetración, dando alcance a las preguntas planteadas frente a la situación problema:

2.3.1. Herramientas software que se utilizaron para llevar a cabo el pentesting.

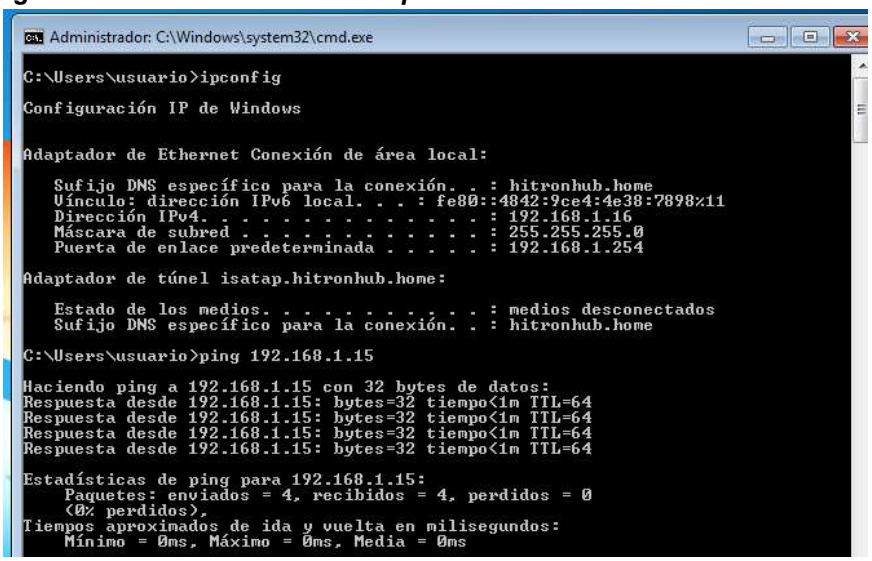
- **Fase de recolección de información.**

En esta fase se recopila la información referente al sistema informático en estudio, es decir, la máquina con sistema operativo Windows 7 x64. Así mismo, se realiza la búsqueda de información sobre la aplicación instalada en esta máquina, denominada **Rejetto en su versión 2.3**, también conocida como **HTTP File Server**, la cual es una aplicación para compartir archivos

[32] (eltiempo.com, 2015)

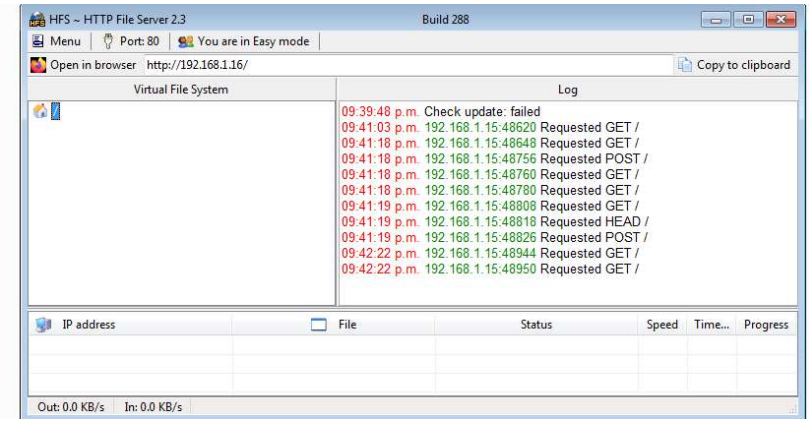
con otras máquinas a través de internet, pero contiene una vulnerabilidad, la cual permite, remotamente a los atacantes puedan desencadenar una violación de acceso de escritura de puntero no válido por medio de peticiones HTTP[33]. Esta vulnerabilidad puede ser explotada a través de uno de los exploits que contiene la herramienta Metaspolit Framework. Adicionalmente, con la identificación de la vulnerabilidad de esta aplicación, se logra determinar que la misma se puede explotar entonces a través del puerto 80. Toda esta información se recopiló a través de las consultas específicas que se realizaron a través del buscador de Google.

Figura 11: Dirección IP de la máquina Windows 7 x64.



Fuente 11: el autor.

Figura 12: Aplicación rejetto instalada en máquina Windows 7 x64.



Fuente 12: el autor.

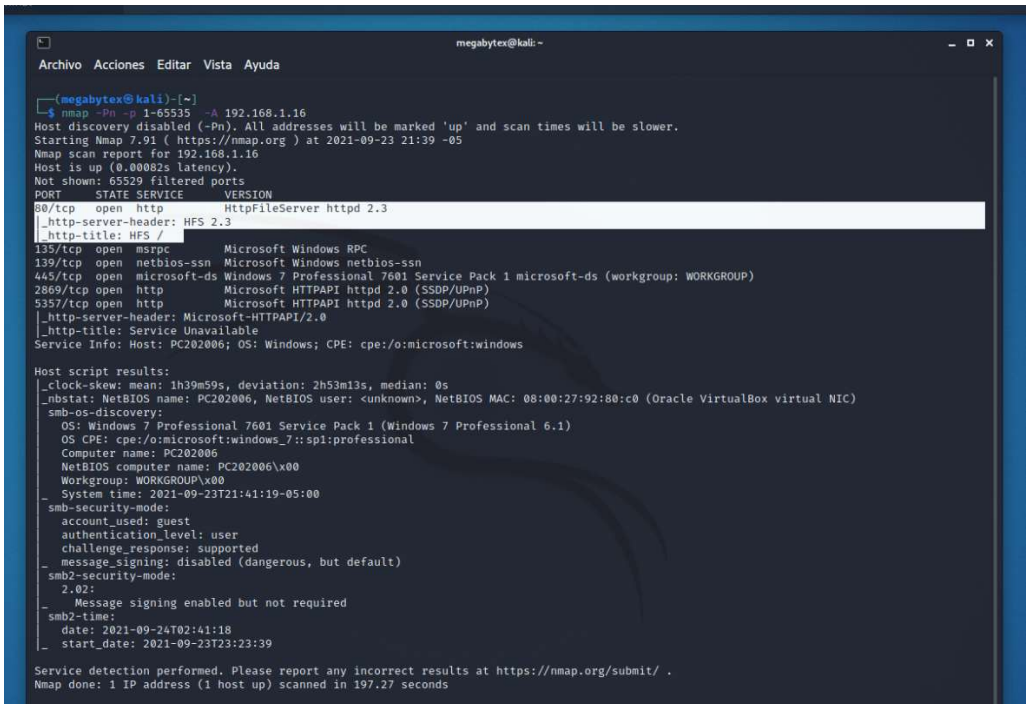
[33] (Incibe-cert, 2021)

- **Fase de Búsqueda y análisis de vulnerabilidades.**

En esta fase se analiza la información recolectada en la anterior etapa con el fin de identificar las vulnerabilidades presentes y elegir el modo más efectivo que permita atacar el sistema y/o la máquina. Adicional a la información recolectada, en esta fase se utiliza la herramienta Nmap para escanear los puertos y servicios de la máquina Windows 7 x64. **Nmap**, es una herramienta de fuente abierta que permite el escaneo de puertos y brindar información acerca de hosts de una red, dando facilidad de conocer que hosts se encuentran activos, que puertos se encuentran abiertos, y si existen firewall activados en ellos, así como conocer que servicios se encuentran ejecutándose, entre otras cosas.[34] A continuación, se evidencia el resultado de escanear los puertos y servicios de la máquina Windows en estudio con la herramienta Nmap:

Primero se escanean todos los puertos de la máquina Windows 7 (Dirección IP: 192.168.1.16) con el comando **nmap -Pn -p 1-65535 -A 192.168.1.16**

Figura 13: Escaneo de puertos con Nmap de la máquina Windows 7 x64.

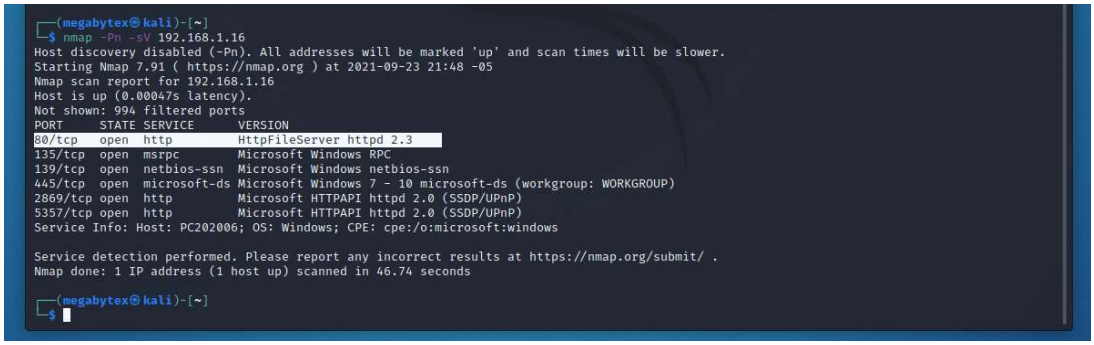


Fuente 13: el autor

[34] (Redeszone, 2021)

De igual forma se escanean los servicios para confirmar los servicios que se ejecutan en cada puerto escaneado con nmap. Para ello se usa el siguiente comando: **nmap -Pn -sV 192.168.1.16**

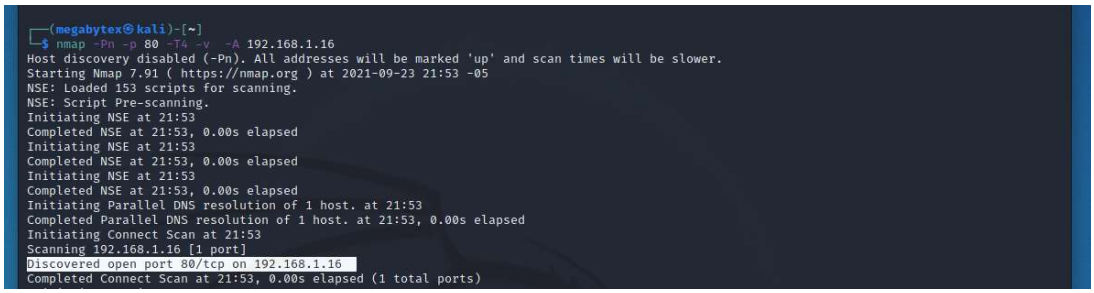
Figura 14: Escaneo de servicios con Nmap de la máquina Windows 7 x64



Fuente 14: el autor

Una vez identificado el puerto 80, con base a la información recolectada en la fase anterior, se evidencia que dicho puerto está abierto y se confirma que el servicio que se encuentra en ejecución en dicho puerto, es el de la aplicación rejetto, también conocido como httpFileServer httpd 2.3. Se ejecuta el comando **nmap -Pn -p 80 T4 -v -A 192.168.1.16** para realizar un escaneo completo sobre dicho puerto y se confirma que el puerto 80 se encuentra activo y abierto.

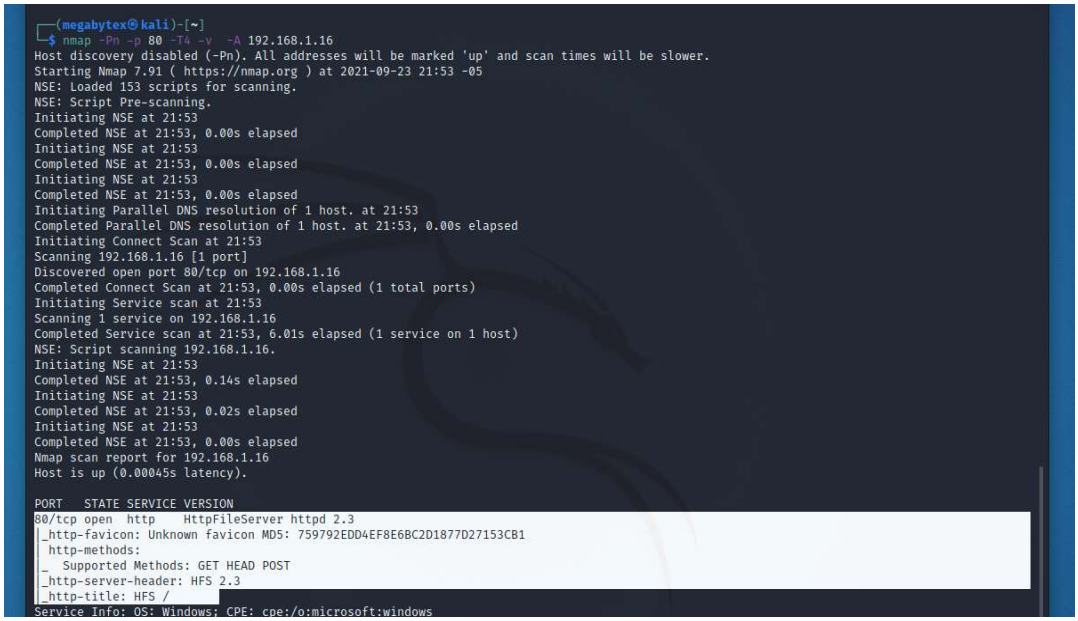
Figura 15: Escaneo completo al puerto 80 con Nmap de la máquina Windows 7 x64



Fuente 15: el autor

Y adicionalmente este comando, muestra más información en relación con los métodos HTTP soportados, entre otros aspectos:

Figura 16:Escaneo completo al puerto 80 realizado a la máquina Windows 7 x64 con Nmap con resultados de métodos HTTP soportados.

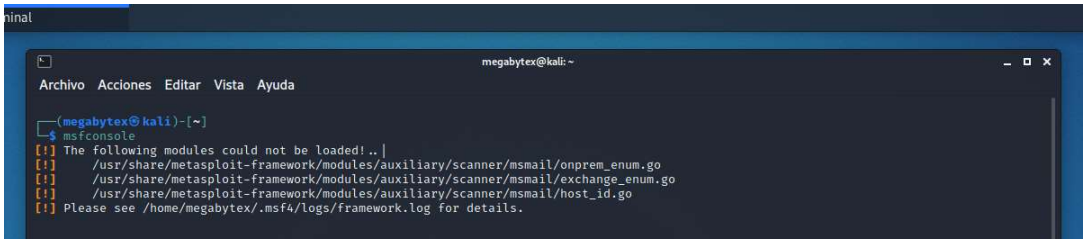


Fuente 16: el autor.

Así mismo, con la herramienta **metasploit-framework**, se realiza la identificación de la vulnerabilidad. **Metasploit-framework**, es una herramienta que permite investigar vulnerabilidades y posee una base de datos con una gran variedad de exploits de vulnerabilidades ya conocidas.[35]

Primeramente, se inicia el servicio de postgresql, motor que administra la base de datos de metasploit-framework, y así mismo, se inicia dicha herramienta a través del comando **msfconsole**, tal como lo muestra la siguiente figura:

Figura 17: Inicio de Metasploit-framework (msfconsole).

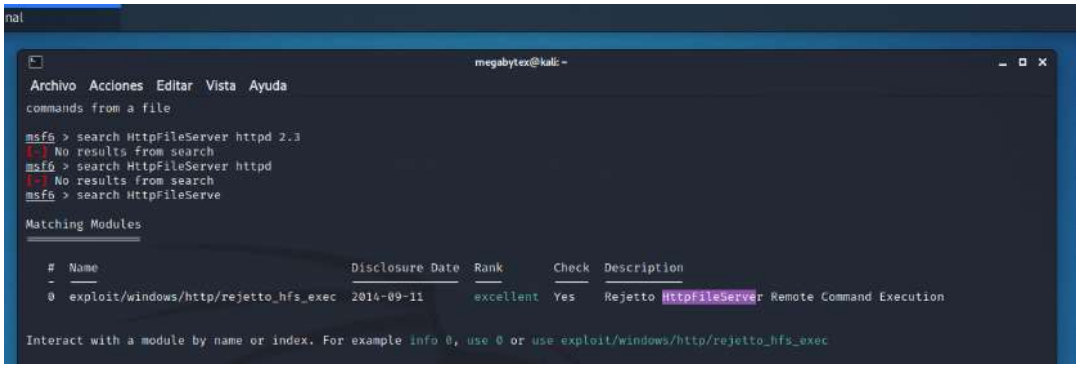


Fuente 17: el autor.

[35] (Openwebinars, 2018)

Luego se realiza la búsqueda de las vulnerabilidades asociadas al servicio HttpFileServer, con el comando **search HttpFileServer** y como resultado arroja la vulnerabilidad asociada.

Figura 18: Búsqueda de vulnerabilidad para el servicio HTTP File Server.

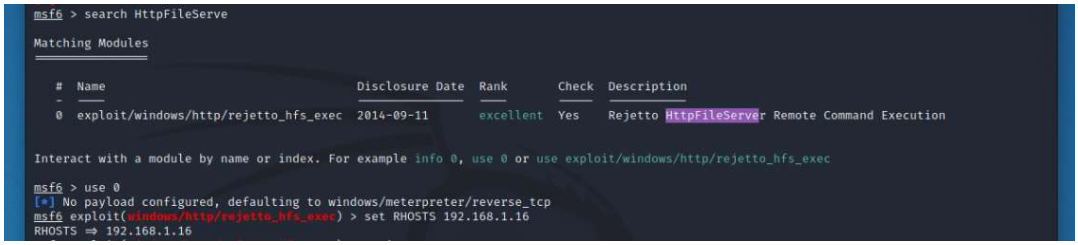


Fuente 18: el autor

- **Fase de Explotación de vulnerabilidades**

Teniendo en cuenta el análisis de vulnerabilidades que se realizó en la anterior fase, en esta fase se realiza la explotación de estas, es decir, se ejecuta el exploit en contra de la vulnerabilidad identificada en la aplicación **rejetto** sobre el puerto 80. En esta fase se utiliza nuevamente la herramienta **Metaspolit-Framework**, la cual permite investigar vulnerabilidades, ya que posee una base de datos con una gran variedad de exploits de vulnerabilidades ya conocidas y contiene también una gran cantidad de módulos denominados payloads, los cuales son los códigos que permiten explotar en sí, las vulnerabilidades. En este caso la búsqueda del exploit indicado para el servicio que ejecuta rejetto, metasploit identificó el exploit "**exploit/windows/http/rejetto_hfs_exec",** como se pudo observar en la figura anterior. Este exploit esta rankeado como "excelente" en metasploit-framework, lo que indica que debe funcionar de manera eficiente en contra de la vulnerabilidad detectada. Es por ello que el comando **use 0** permite seleccionar el exploit de la posición cero en el listado, por ser el único mostrado por metasploit para este servicio.

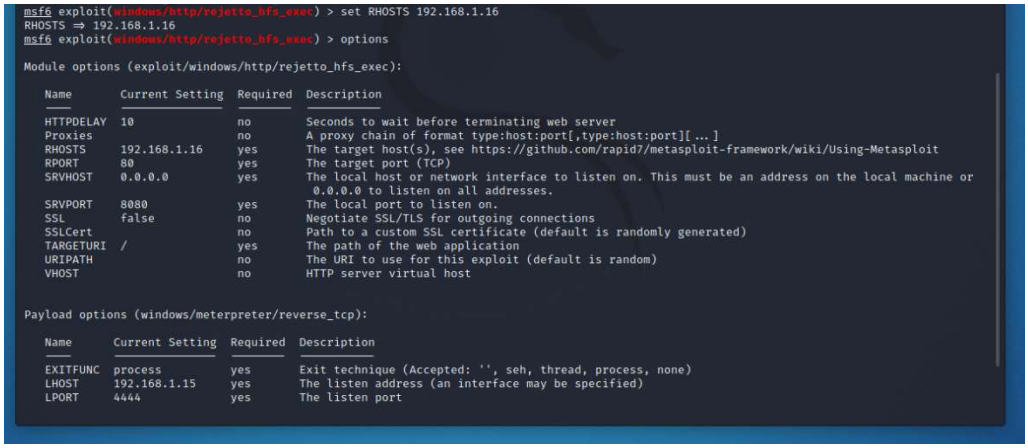
Figura 19: Selección del exploit de la vulnerabilidad asociada al servicio HttpFileServer.



Fuente 19: el autor.

Seguidamente, se ajustan los parámetros de configuración del exploit antes de la realización del ataque, por ello se establece la IP de la máquina a atacar con el comando **set RHOST.** Se revisan las opciones para identificar el **payload** que realizará el ataque con el comando **options**, tal como se muestra en la siguiente figura:

Figura 20: Configuración de los parámetros del exploit para realizar el ataque.

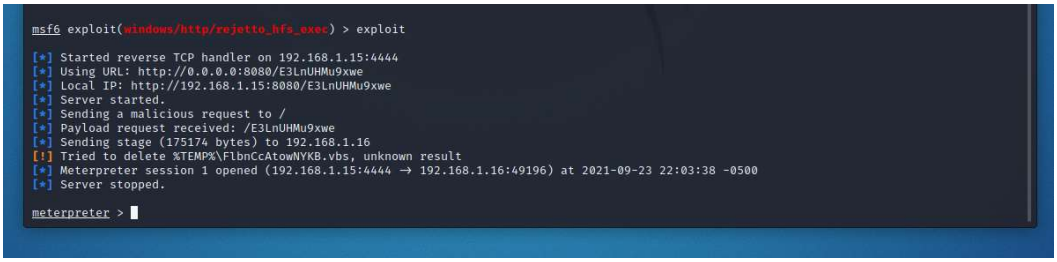


Fuente 20: el autor.

Y finalmente se ejecuta el exploit con el comando **exploit**, aunque también se pudo usar el comando **run.** Una vez se ejecuta el exploit, se puede evidenciar que se estableció la sesión meterpreter y ya se tiene acceso al sistema a través de una Reverse Shell, la cual es una peligrosa técnica**:**[36]

[36] Bytelearning. (15 de Octubre de 2019)

Figura 21: Ejecución del exploit en la máquina Windows 7 x64.

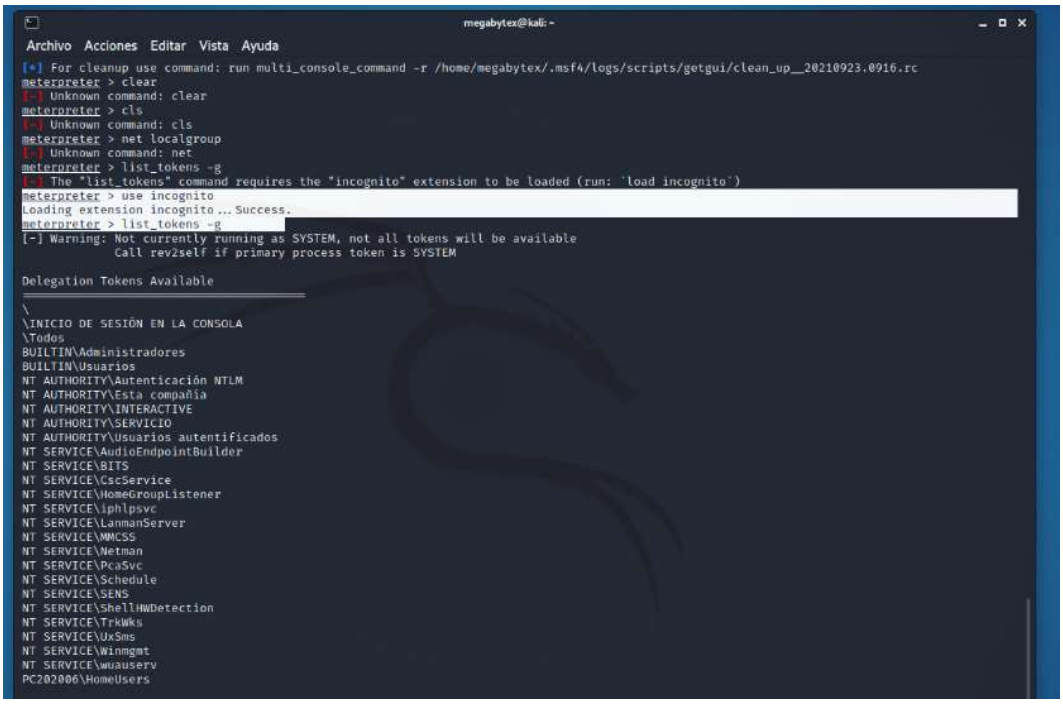


Fuente 21: el autor.

- **Fase Post-Explotación.**

Esta fase, básicamente permite aprovechar la intrusión para ejecutar otras acciones dentro del sistema penetrado, y en la red misma. En este caso particular se realiza la creación de un usuario con el comando run **getgui -u JaiderContreras -p 123456.** Luego se inicia la aplicación incognito con el comando "**use incognito",** para poder revisar los grupos de usuarios existentes con el comando **list_tokens -g,** como se muestra a continuación:

Figura 22: Creación del usuario JaiderContreras en la máquina Windows 7.

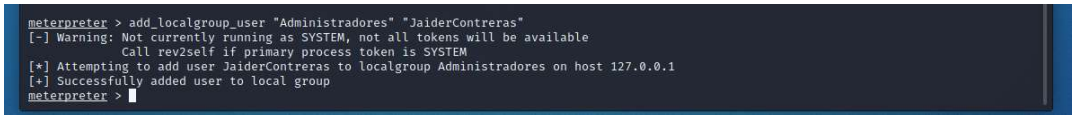


Fuente 22: el autor.

Finalmente se evidencia el escalamiento de privilegios de administrador asociados al usuario creado dentro de la máquina Windows 7, con el fin de

tomar control de dicha máquina. El comando usado es **add_localgroup_user “Administradores” “JaiderContreras”**

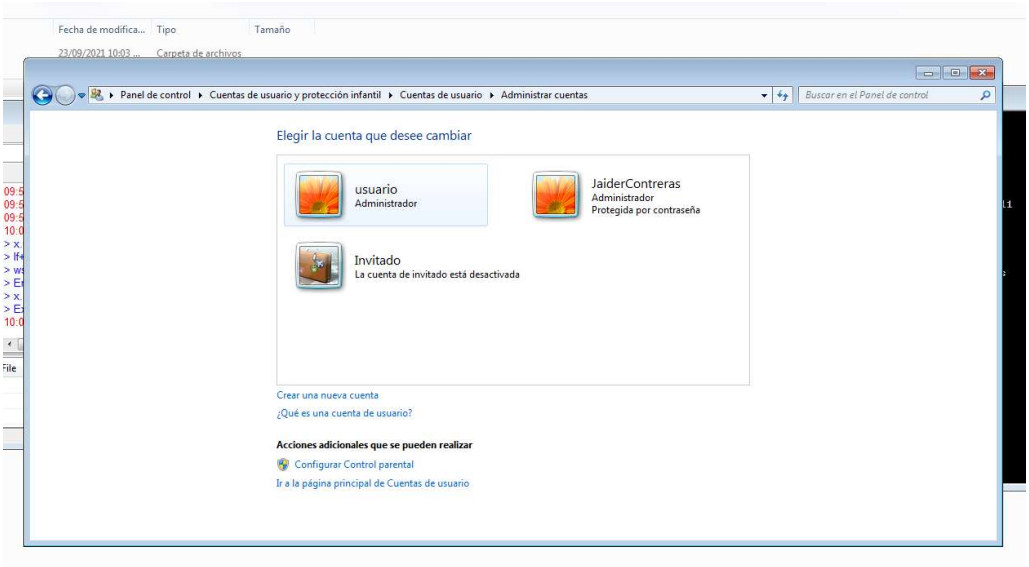
Figura 23: Agregando privilegios de administrador al usuario JaiderContreras dentro de la máquina Windows 7 x64.



Fuente 23: el autor

Se evidencia en la maquina penetrada que el usuario se encuentra creado.

Figura 24: Evidencia de la creación del usuario en la Maquina atacada.



Fuente 24: el autor.

2.3.2. Datos e información del “Escenario 3” que fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 7 X64.

Los datos e informaciones claves para poder identificar el fallo de seguridad inmerso en la máquina Windows 7 x64 son los siguientes:

- El Sistema Operativo instalado en la máquina objetivo, el cual es Windows 7 con arquitectura x64.

- La información consultada y recolectada referente a la aplicación rejetto en su versión 2.3, que se menciona en la situación problema, es un dato muy importante para encontrar la vulnerabilidad a la cual estaba expuesta

la máquina, ya que con el nombre de esta aplicación se pudo encontrar información en Google sobre vulnerabilidades de esta, el nombre alterno con el que se conoce esta aplicación (mismo nombre del servicio que ejecuta la aplicación) y el tipo de vulnerabilidad asociado. Con esto se puede igualmente identificar el puerto que se debe escanear al detalle (puerto 80).

- La información que se menciona sobre Shell Reversa y la sesión de meterpreter, también es un dato importante para identificar la vulnerabilidad de dicho sistema.

2.3.3. Herramientas que se pueden utilizar para identificar los fallos de seguridad de la "máquina Windows 7" e identificación del puerto que abre la aplicación específica.

Las herramientas que se utilizan para identificar la vulnerabilidad asociada a la máquina Windows 7 x64 son las siguientes:

- El Buscador Google, el cual permite consultar información referente a la aplicación rejetto, el nombre del servicio y el puerto de ejecución de esta. Así mismo, las informaciones que se consultan, evidencian el tipo de vulnerabilidad asociado a esta aplicación.

- La herramienta Nmap, es una herramienta clave para el escaneo de puertos y confirmar la información consultada.

- La herramienta metasploit-framework permitió permite encontrar la vulnerabilidad asociada al servicio de la aplicación rejetto y el exploit que se puede usar para aprovechar la vulnerabilidad detectada.

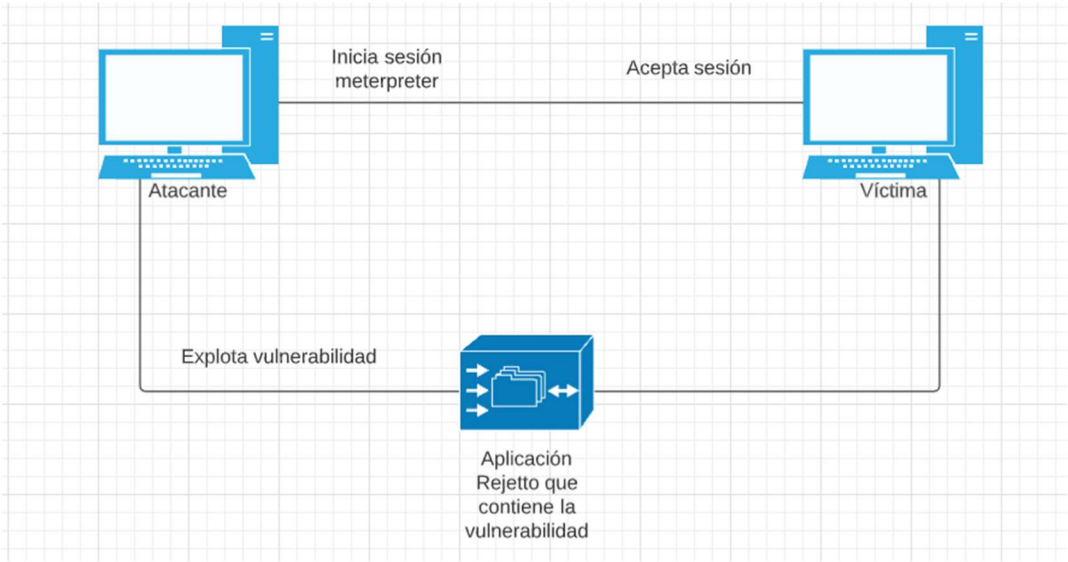
El puerto que abre la aplicación "rejetto" es el puerto 80 (HTTP).

2.3.4. Descripción de la afectación que produce el ataque a la máquina (Windows 7 X64).

En resumen, la máquina atacante identifica una vulnerabilidad asociada al servicio HttpFileServer de la aplicación rejetto, el cual se ejecuta por el puerto 80. Con la herramienta metasploit-framework, se identifica el exploit con el cual se puede explotar dicha vulnerabilidad, y una vez ejecutado el exploit, el payload asociado inicia una sesión con la máquina víctima, estableciendo una conexión

y generando una reverse Shell, que permite crear un usuario con privilegios de administrador y así tomar control total de la máquina.

Figura 25: Gráfica del ataque informático.

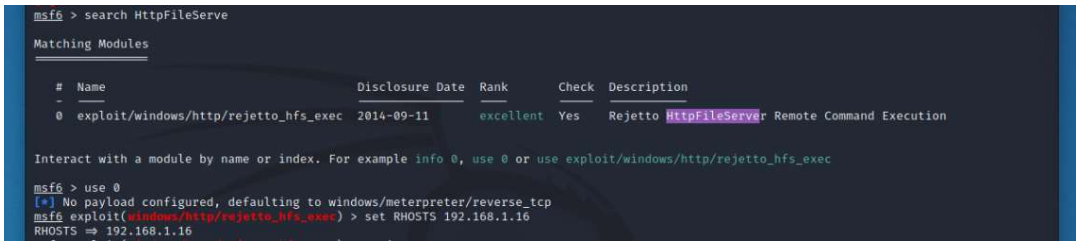


Fuente 25: el autor.

2.3.5. Pasos que se ejecutan para explotar la vulnerabilidad en la máquina Windows 7.

Una vez iniciado metasploit-framework con el comando **msfconsole** y realizada la búsqueda a través del comando **search** sobre el servicio **HttpFileServer** que se ejecuta en el puerto 80 para la aplicación **rejetto,** se identifica el exploit que permite explotar la vulnerabilidad asociada a esta aplicación "**exploit/windows/http/rejetto_hfs_exec".** Luego de ello, se inicia el proceso de explotación de la vulnerabilidad, seleccionando el exploit de la posición cero en el listado, con el comando **use 0:**

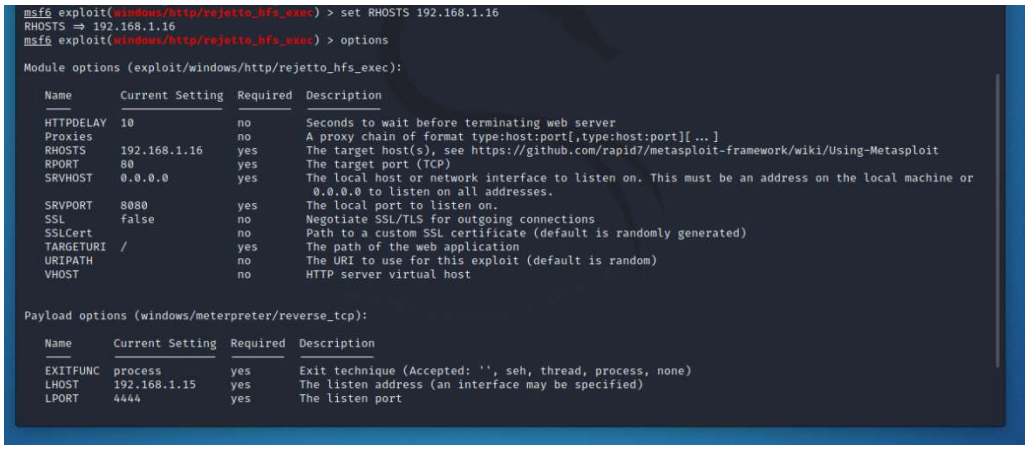
Figura 26: Selección del exploit de la vulnerabilidad asociada al servicio HttpFileServer.



Fuente 26: el autor.

Seguidamente se configuran los parámetros de configuración del exploit antes de realizar el ataque, por ello se establece la IP de la máquina que vamos atacar con el comando **set RHOST,** se revisan las opciones para identificar el **payload** que realizará el ataque con el comando

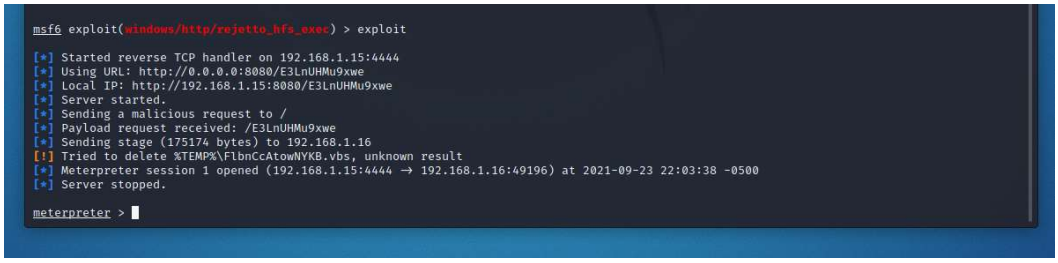
Figura 27: Configuración de los parámetros del exploit para realizar el ataque.



Fuente 27: el autor.

Y finalmente se ejecuta el exploit con el comando **exploit**, aunque también se puede usar el comando **run.** Una vez se ejecuta el exploit, se puede evidenciar que se estableció la sesión meterpreter y ya se tiene acceso al sistema a través de una Reverse Shell, la cual es una peligrosa técnica**:**

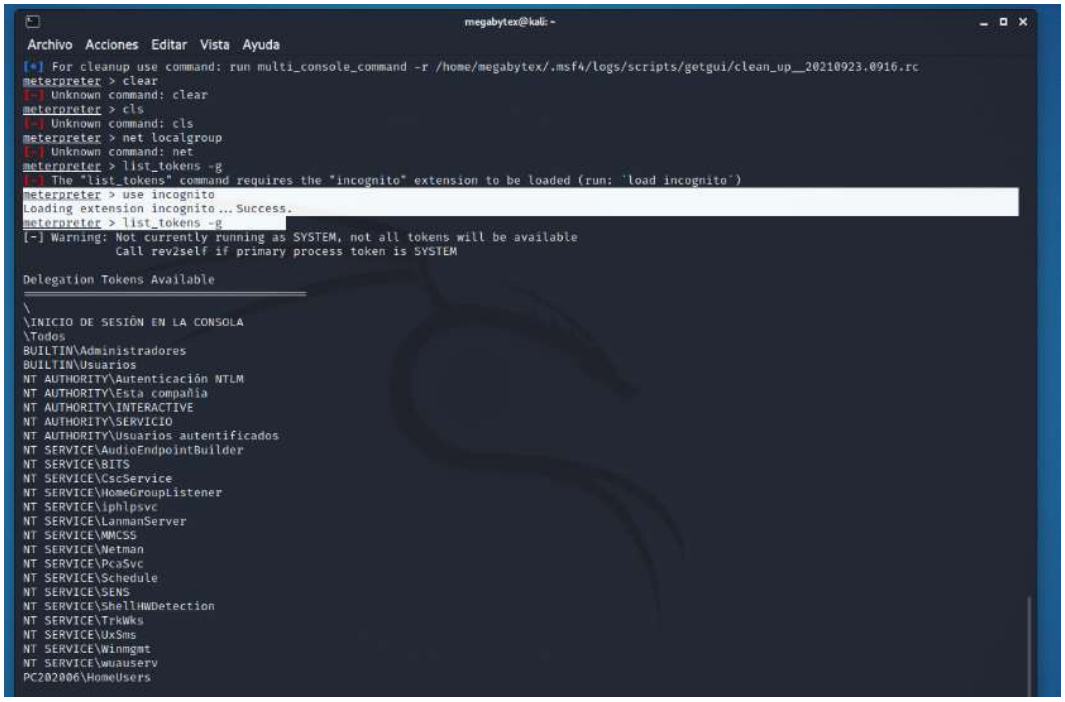
Figura 28: Ejecutación del exploit en la máquina Windows 7 x64.



Fuente 28: el autor.

Posteriormente, se realiza la creación de un usuario con el comando **run getgui -u JaiderContreras -p 123456** y luego se inicia la aplicación **incognito** con el comando "**use incognito",** para poder revisar los grupos de usuarios existentes con el comando **list_tokens -g,** como se muestra a continuación:

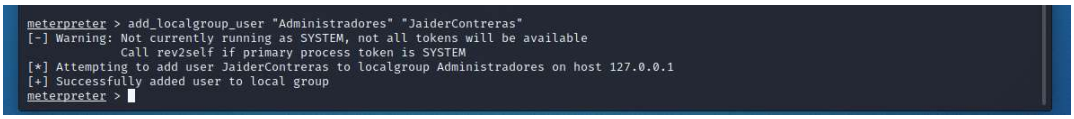
Figura 29: Creación del usuario JaiderContreras en la máquina Windows 7.



Fuente 29: el autor.

Por último, se asocian los privilegios de administrador al usuario creado dentro de la máquina Windows 7, con el fin de tomar posterior control de dicha máquina. El comando que se usa es **add_localgroup_user "Administradores" "JaiderContreras"**

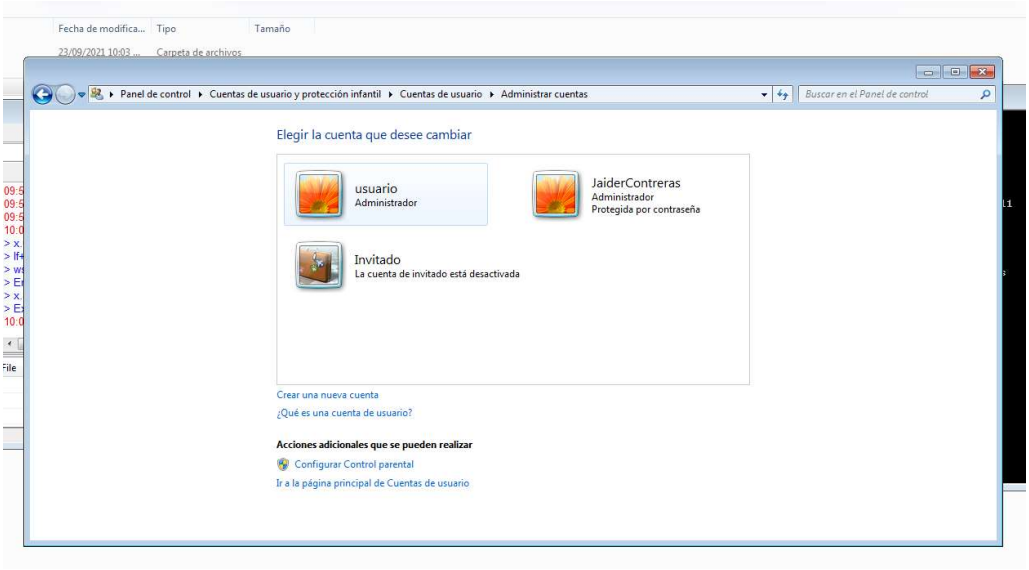
Figura 30: Escalamiento de privilegios de administrador al usuario JaiderContreras dentro de la máquina Windows 7 x64.



Fuente 30: el autor.

Y se logra evidenciar en la maquina atacada, que el usuario **JaiderContreras**, se encuentra creado como administrador.

Figura 31: Evidencia de la creación del usuario en la Maquina atacada.



Fuente 31: el autor.

2.4. ANALISIS SITUACIONAL EQUIPO BLUE TEAM.

2.4.1. Aspectos para indagar y acciones a realizar al encontrarse frente a un ataque en tiempo real.

Con el fin de proteger la información ante ataques informáticos, es importante que las empresas cuenten con planes de acción que permitan gestionar y dar respuesta a los incidentes de seguridad, los cuales van en concordancia con las políticas de seguridad de la información de la organización. Estos planes, comúnmente se dividen en 4 fases, las cuales son prevención, detección, recuperación y respuesta.[37] Por tanto, es esencial ajustar las acciones a realizar con el plan de seguridad de la información de la organización para poder actuar rápidamente frente a un ataque informático. Teniendo en cuenta la situación planteada dentro de la organización “The WhiteHouse Security” respecto a la ejecución de un ataque informático en tiempo real, al interior de esta, se debe revisar y ejecutar las acciones y actividades del plan con el que cuente la misma, desde su segunda fase. Las acciones y actividades a realizar son, entre otras, las siguientes:

- **Fase de Detección:** A través de esta fase se debe identificar los aspectos tales como, el tipo o vector de ataque que se está ejecutando y así poder

[37] (Deloitte, 2021)

identificar posteriormente el tipo de vulnerabilidad que se está explotando. De igual forma se debe identificar sobre que máquina o máquinas y sistemas se está ejecutando el ataque, con el fin de aislar las mismas y mitigar un poco las afectaciones sobre otros equipos y demás dispositivos en la red de la organización y la información misma.

Una vez identificadas las maquinas afectadas, es importante revisar aspectos tales como, el sistema operativo, versión del sistema y/o versión de compilación, nivel y/o estado de actualización de este, si cuenta con los últimos parches de seguridad, revisar si cuenta con antivirus, si tiene firewall activado. Así mismo revisar las cuentas de usuario creadas dentro de estos sistemas, las fechas de creación, los niveles de privilegio, entre otros. Para el caso de la maquina afectada, se evidencia que esta tiene instalado el sistema Operativo Windows 7 con arquitectura de 64 bits, versión de compilación 7601 Service Pack 1, sistema desactualizado sin las últimas actualizaciones de seguridad, no tiene instalado antivirus, y aunque tiene firewall activado, carece de reglas de seguridad específicas que permitan salvaguardar la seguridad del sistema. El sistema de esta máquina cuenta con dos usuarios activos, uno de ellos denominado “usuario” con privilegios de administrador sin contraseña, el otro es un usuario recién creado denominado “JaiderContreras” con privilegios de administrador y es el usuario creado en el sistema con el ataque.

Dentro del sistema de la maquina aislada, se debe revisar de igual forma las aplicaciones que tiene instalada el mismo, su funcionalidad, servicio y puerto de ejecución. Para ello es importante se realice un escaneo de puertos, usando Nmap por ejemplo. Adicionalmente, se debe revisar, si las aplicaciones instaladas se encuentran actualizadas, evitando así riesgos de seguridad. En el caso de la maquina atacada se encontró una aplicación llamada rejetto, que no requiere estar instalada para ejecutarse, la cual se ejecuta en el puerto 80 (http) y posee una vulnerabilidad, fácilmente explotable.

Teniendo en cuenta lo anterior, se debe realizar un análisis de vulnerabilidades en la máquina atacada y así consultar información de las afectaciones que pueda sufrir la misma, y determinar los posibles exploits que se puedan usar y los riesgos asociados a la explotación de estas vulnerabilidades, estableciendo el impacto y las facilidades que genera para el atacante la explotación de dichas vulnerabilidades. En el caso de

la maquina en estudio, se evidencia que la aplicación rejetto tiene asociada una vulnerabilidad en su servicio HTTP File Serve que permite al atacante realizar la intrusión a través del puerto 80 usando peticiones HTTP y tomando control de la maquina con el exploit exploit/windows/http/rejetto_hfs_exec.

Posterior al análisis de vulnerabilidades que se efectúa, se debe realizar la explotación de estas, en un ambiente controlado. Esta actividad permite recrear el ataque, y con ello determinar el impacto generado y nivel de afectación del sistema, la máquina, pero especialmente en la información de la organización.

Finalmente, luego de identificar las vulnerabilidades, analizar las afectaciones de sus explotaciones y determinar el impacto generado en la organización, es preciso establecer medidas de contención, que permitan mejorar la seguridad informática y de la información. Por ende, corresponde en la maquina en estudio, con replica a todos los equipos de la organización realizar las siguientes actividades:

- ✓ Actualizar el sistema operativo con las últimas actualizaciones de seguridad. Así mismo de las aplicaciones instaladas en dicho sistema.
- ✓ Validar las cuentas de usuario autorizadas, cambiando contraseñas, de ser preciso implementar sistema de Directorio Activo y establecer políticas de gestión de usuario seguras, como forzar a cambiar contraseñas cada cierto tiempo, que implementen parámetros de contraseñas seguras, por ejemplo.

- ✓ Instalar y actualizar el antivirus.

- ✓ Mantener actualizado el firmware del firewall y demás dispositivos de red implementados al interior de la organización.

- ✓ Cerrar puertos abiertos que no se requieran tener abiertos y mejorar la seguridad de los puertos que así requieran permanecer abiertos.

- ✓ Establecer reglas en el firewall y demás dispositivos de seguridad perimetral. Por ejemplo, generar reglas para filtrar las conexiones a puertos y servicios, identificados y comprometidos en el ataque.

- ✓ Establecer políticas de bloqueo de direcciones IP en los dispositivos de red.

- ✓ Monitorear los sistemas, máquinas y demás dispositivos de TI y red.

- ✓ Implementar políticas de backups de las bases de datos y sistemas informáticos e información de la organización.

- **Fase de Recuperación:** Luego de restaurar las copias de seguridad del sistema, se deben implementar las medidas mencionadas en la anterior fase junto a las demás medidas de hardenización que permitan mejorar la seguridad de la información.

- **Fase de Respuesta:** Reportar a la alta gerencia, usuarios internos y externos, respecto al incidente sucedido, en busca de generar concientización, espacios de capacitación y el cumplimiento de las políticas de seguridad implementadas o que producto del incidente de seguridad sobrevengan establecer.[38]

2.4.2. Medidas de hardenización para no permitir que se repita el ataque.

De acuerdo a lo expuesto en el anterior punto de este informe, luego del ataque informático a los sistemas informáticos de la organización "WhiteHouse Security", se deben implementar medidas que permitan prevenir y/o mitigar los niveles de riesgo y afectación a la seguridad de la información de todos los sistemas de la organización. Es por ello por lo que, se deben implementar medidas de hardenización tales como:

- Realizar validaciones y gestiones apropiadas de las cuentas de usuario autorizadas, creando contraseñas a los usuarios que no tienen asociada una, y cambiando contraseñas de manera inmediata a las que si cuentan con contraseña. Ninguna cuenta de usuario debe quedar sin la asignación de contraseña, mucho menos una cuenta con privilegios de administrador. Una opción es la de implementar Active Directory para la gestión de credenciales con niveles de privilegios en los equipos y en ese mismo sentido, establecer políticas de contraseñas seguras, solicitudes de cambios de contraseña cada cierto tiempo, entre otras.

[38] (Deloitte, 2021)

- Se deben eliminar las cuentas de usuario que no hayan sido creadas por el administrador de TI de la organización, así como la desactivación o bloqueo de credenciales de usuarios que ya no laboran en la empresa o que no se requieran.

- Se debe validar el software instalado en las máquinas de la organización, así como en los servidores, haciendo un inventario de lo requerido y lo no necesario y en base a ello, desinstalar todo el software que no es necesario en la organización. Así mismo, se debe revisar las actualizaciones de las aplicaciones y/o software que se requiera dejar instalado y actualizarlos con los últimos parches de seguridad y evitar vulnerabilidades que se puedan explotar.

- Mejorar la seguridad de todos los servicios y procesos utilizados en la organización, monitoreando el buen funcionamiento de estos.

- Proceder al cierre de aquellos puertos abiertos que se encuentren sin uso y mejorar la seguridad de los que se requieran abiertos, a través de reglas a nivel de firewall y demás dispositivos de seguridad perimetral.

- Llevar una correcta gestión de Backups de la información de la organización, almacenándolas bajo políticas de seguridad. Estos backups o respaldos de información, se pueden almacenar en una NAS o en la nube. Esto permite que, ante cualquier incidente, se pueda restablecer el sistema con su respectiva información rápidamente, sin afectar por mucho tiempo la continuidad en la prestación de los servicios de la organización.

- Realizar la instalación de dispositivos de seguridad perimetral como lo son, firewalls, IDS, IPS, WAF (Web application firewall) sino se cuenta con ellos. De igual forma se debe activar el firewall a nivel de software en los sistemas operativos de cada máquina.

- Actualizar el sistema operativo con las últimas actualizaciones de seguridad. Así mismo de las aplicaciones instaladas en dicho sistema.

- Instalar en cada maquina y servidor un antivirus y mantenerlo actualizado. Escanear todo archivo que ingrese al equipo y no permitir la apertura de archivos desconocidos.

- No permitir la descarga de archivos provenientes de páginas no oficiales.[39]

- Establecer políticas de seguridad de la información en concordancia con la ISO 27001/2013 y los objetivos de control y sus respectivos controles, con el fin de proteger los datos como mayor activo de la organización, la infraestructura de TI y los sistemas de esta, no solo a nivel de hardware y software, sino a través de políticas orientadas también al correcto uso de toda la infraestructura de TI, incluyendo los equipos, por parte de los usuarios internos y externos. Dentro de las políticas que se pueden establecer e implementar dentro de la organización, teniendo en cuenta los controles de la ISO 27001/2013, se encuentran políticas referentes al correcto uso de los equipos, infraestructura TI y manejo del correo institucional, instalación de software no autorizado, manejo de backups de información, mantenimiento de equipos y sistemas de información, administración y gestión de dispositivos de red y seguridad perimetral, políticas relacionadas con dispositivos de almacenamiento, acceso remoto y manejo de credenciales. Así mismo políticas para la gestión de incidentes de seguridad correlacionadas los controles A16 de la norma ISO 27001.[40]

2.4.3. Diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos.

Aunque en la actualidad estos dos equipos están íntimamente involucrados por las labores que ejercen en pro de la seguridad de la información y/o ciberseguridad, existe una diferencia muy marcada y es que los CSIRT operan más que todo cuando el ataque o incidente de seguridad se produce, su accionar es más de índole reactiva, coordinando las acciones de respuesta ante los incidentes de seguridad. Dentro de las actividades que realizan, se encuentran el análisis del código malicioso, la investigación de las condiciones y análisis de cómo se produce el ataque, con el fin de ayudar a restablecer el sistema afectado, y contribuir en la gestión de vulnerabilidades detectadas. Mientras que

[39] (Hardening, 2020)
[40] (UDistrital, 2017)

en los equipos BlueTeams, su accionar esta más orientado hacia lo preventivo, más allá que estén involucrados con el estudio del sistema atacado, el objetivo de estos, es el de reforzar las medidas de seguridad informática con el fin de prevenir que un ataque informático se vuelva a perpetrar. Los equipos Blueteam, se encargan entonces de diseñar las herramientas de seguridad que permitan prevenir o mitigar los efectos de un ataque informático, son los encargados de orientar y brindar las recomendaciones necesarias para que se puedan prevenir o mitigar en gran medida dichos ataques y brindan la información necesaria, recolectada de sus investigaciones y análisis de sistemas atacados para que otros profesionales y comunidad en general tenga conocimiento de como mitigar y prevenir futuros ataques.[41]

2.4.4. Análisis del Uso de CIS "Center For Internet Security" dentro de un equipo Blue team.

Teniendo como referencia, que CIS (Center For Internet Security), es una organización internacional, encargada de generar y compartir un amplio conocimiento de mejores prácticas en el ámbito de la ciberseguridad, a partir de la interacción de múltiples profesionales en TI de los diferentes campos de la seguridad informática, dedicados a estudiar y afrontar los diversos incidentes de seguridad y/o ataques informáticos, con el fin de implementar controles que permiten contrarrestarlos de manera efectiva, brindando la posibilidad a múltiples empresas y profesionales en general, de contar con una amplia información de mejores prácticas de seguridad informática, en favor de la prevención, mitigación y respuesta ante los ataques informáticos presentados en los diferentes sectores económicos.

Basado en lo anterior, se debe utilizar CIS, como ruta metodológica que permita conocer y aplicar el conocimiento de profesionales en seguridad, sus mejores prácticas, políticas y controles, con el fin de fortalecer la seguridad de la información y/o ciberseguridad al interior de la organización, teniendo la posibilidad de aprender y aumentar la capacidad de prevenir, mitigar, alertar y dar respuesta a los incidentes y/o ataques que afectan la seguridad de esta.

Trabajar con CIS, trae consigo muchos beneficios, entre los cuales se puede mencionar la posibilidad de contar con acceso a múltiples servicios y herramientas, tales como, los 20 controles que apuntan a diferentes aspectos de la seguridad de la información y que permiten fortalecer la misma dentro de las

[41] (Codespaceacademy, 2021).

empresas, desarrollando estrategias efectivas para enfrentar las diferentes amenazas existentes hoy en día.[42]

2.4.5. Funciones y características principales de un SIEM.

SIEM (Security Information and Event Management o Información de seguridad y gestión de eventos), es una herramienta de software de las más potentes de seguridad informática, en la actualidad, capaz de recopilar unificadamente información de todos los sistemas y dispositivos así como de sus eventos, permitiendo a las organizaciones y profesionales en TI, el análisis de la información de los diferentes sistemas y dispositivos, así como el análisis de los eventos presentados alrededor de los mismos. Esta tecnología permite fácilmente, la detección de incidentes de seguridad, basado en la información recolectada, configurando tendencias e identificando patrones fuera de lo común con base a estas.

Con la implementación de esta tecnología se tiene una visión global de la seguridad de la información, ya que esta, con ayuda de la IA (Inteligencia artificial) recopila eficientemente información referente a la seguridad de los dispositivos de red, equipos, servidores, antivirus, controladores de dominio, etc Así como de los eventos presentados. Con esta información recopilada en un punto central y distribuida a través de correo electrónico o publicada en un portal Web creado exclusivamente para ello, es capaz de identificar tendencias, detectar amenazas y generar alertas, que pueden ser investigadas por parte de los profesionales en TI o ciberseguridad, pues la información generada, es recopilada en un completo informe que permite analizar de mejor manera todo lo referente a los aspectos de seguridad informática de la organización.

Algunas de las características de esta tecnología son:

- Facilita la documentación de los eventos de seguridad.

- Permite contar con informes mejor estructurados que facilitan el análisis y entendimiento de los aspectos de seguridad de la información y seguridad informática.

[42] (CIS, Center for Internet Security. s.f.)

- Permite identificar rápidamente las vulnerabilidades de los sistemas y los riesgos de explotación asociados a las mismas.

- Clasifica las amenazas y las diferencia de falsos ataques positivos, optimizando el trabajo de los equipos de seguridad y permitiéndoles centrarse en lo importante.

- Brinda la posibilidad de una mejor gestión de los incidentes de seguridad, teniendo en cuenta prioridades y el impacto a los sistemas informáticos de la organización.

- Permiten la fácil detección de posibles ataques e intrusiones a la seguridad de los sistemas de la empresa, gracias a la recopilación unificada de todos los datos de seguridad de los diferentes equipos y dispositivos de la Infraestructura TI, eventos producidos, las tendencias descubiertas y los patrones fuera de lo común

- Permite la búsqueda y detección de amenazas en registros archivados, los cuales son más difíciles de detectar pos sus periodos largos de inactividad dentro de los sistemas o la red interna.

- Brinda la posibilidad de detener amenazas aún desconocidas, sin la necesidad que el incidente de seguridad o ataque informático se haya producido para eliminarlo, gracias a tecnologías como el machine learning, que permiten predecir este tipo de eventos.[43]

2.4.6. Herramientas de contención de ataques informáticos.

Dentro de las herramientas seleccionadas tenemos las siguientes:

- **OSSIM:** Es un producto de software, de código abierto creado por AlienVault, para la gestión de aspectos seguridad de la información y permite la gestión de eventos (SIEM), proporcionando un SIEM completo con recolección de eventos, que tiene la característica de actuar como un sistema de prevención de intrusos teniendo como base información

[43] (SOFECOM, s.f.)
(ICM, 2020)

correlativa de cualquier fuente, que le permite constituirse en una herramienta útil dentro de la seguridad informática.[44]

- **Fail2ban:** es una aplicación software basada en Python y se usa para prevenir ataques por intrusión a un sistema. Fail2ban opera escaneando los archivos de registro y permite bloquear direcciones IP que evidencian signos maliciosos, como lo son demasiado intentos fallidos de contraseña, búsqueda de exploits, entre otros. Este software se usa para actualizar las reglas del firewall y el bloqueo de direcciones IP durante un período de tiempo específico y provee diferentes filtros para varios servicios (apache, SSH, etc.).[45]

- **WAZUH:** Es una herramienta software de código abierto que permite la detección y contención de amenazas, permitiendo dar respuesta a los incidentes de seguridad presentados.[46]

[44] (Incibe, s.f)
[45] (Fail2ban, 2016)
[46] (Wazuh, s.f.)

CONCLUSIONES.

Para todo profesional en seguridad informática, es importante conocer el marco legal colombiano vigente para la seguridad de la información. Es así como el estudio de la ley 1273 de 2009 se hace relevante para conocer los delitos de esta índole y las sanciones aplicables para aquellas personas que incurran en estos. Este conocimiento, permite de igual forma, realizar un buen ejercicio de la profesión dentro del marco legal, en especial aquellas actividades relacionadas con los equipos Red Team y BlueTeam.

Así mismo, es de gran importancia, hacer una apropiación del código de ética contenido en la ley 842 de 2003, donde se asuman las conductas y disposiciones expuestas en este, con el fin de actuar ética y legalmente en beneficio del ejercicio correcto de la profesión, evitando adicionalmente las sanciones que pueda interponer el COPNIA.

Se logró demostrar las vulnerabilidades existentes del sistema informático en estudio de la organización “The WhiteHouse Security”, a partir del uso de metodologías y técnicas de intrusión como el pentesting, a través de sus diferentes fases, por parte del equipo Red Team, y con ello concluir que la ciberseguridad es un aspecto muy importante que toda organización debe considerar con mucha seriedad, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información. Es vital que estas, cuenten con equipos de profesionales en seguridad que implementen estas metodologías, capaces de identificar vulnerabilidades inmersas en los sistemas informáticos de las organizaciones.

Se logró evidenciar adicionalmente, el papel tan importante que juegan también los equipos Blue Team al interior de las organizaciones, para fortalecer la ciberseguridad a través de metodologías, políticas y medidas de contención y mitigación de los riesgos asociados a los ataques informáticos y/o dar respuesta efectiva a los incidentes de seguridad presentados. Así mismo es importante mencionar que es fundamental el apoyo que la organización brinde a estos equipos en la implementación de herramientas que fortalezcan las habilidades y conocimientos de estos equipos.

En definitiva, el ejercicio de auditoria realizado al sistema informático de la empresa “The WhiteHouse Security”, presentado a través de este informe, permite informar a la alta gerencia respecto a los altos riesgos de seguridad a los que están

expuestos, pero también las medidas que se deben tomar para fortalecer la seguridad informática de esta organización, no solo a nivel técnico sino también a través de la implementación de políticas que involucren la capacitación, sensibilización al personal que labora con la empresa, y clientes externos de ser necesario, tanto en aspectos técnicos como aquellos enmarcados en lo ético y legal. La importancia de contar en la organización con equipos de profesionales especializados en seguridad, como Red Team y Blue Team, para mantener monitoreado y fortalecido la ciberseguridad de los sistemas de esta.

RECOMENDACIONES.

Seleccionar y asignar los profesionales idóneos que elaborarán y/o reestructurarán los acuerdos de confidencialidad y contratos de los profesionales a contratar para conformar los equipos Red Team y Blue Team.

Restructurar completamente, los acuerdos de confidencialidad alineados con el marco ético y legal vigente colombiano, que permita regular las actividades que desarrollarán los profesionales contratados para conformar los equipos Red Team y Blue Team sin beneficio ilegal para la organización o perjuicio de la protección de datos personales o de la seguridad de la información.

Contratar y contar con profesionales en ciberseguridad idóneos que conformen los equipos Red Team y Blue Team para la identificación, análisis, explotación controlada de vulnerabilidades y la implementación de medidas y metodologías de respuesta efectiva a incidentes de seguridad informática y la contención de ataques informáticos hacia los sistemas de la organización.

Implementar medidas de hardenización, tales como el cierre de puertos, eliminación de cuentas de usuario no necesarias, desinstalación de aplicaciones no usadas y la actualización de sistemas operativos y aplicaciones, entre otras. De igual manera, se recomienda el uso de herramientas SIEM para tener un mayor control y monitoreo de la seguridad de los sistemas, dispositivos de red y la infraestructura TI en general de la organización.

Definir, establecer o fortalecer e implementar políticas de ciberseguridad alineadas con los controles expuestos en la ISO 27001 que permita contar con una mejor seguridad de la información y la ciberseguridad en la organización, así como implementar las buenas prácticas y controles de la CIS (Center For Internet Security), como guía de ruta para actuar frente a los ataques informáticos que se presenten y atenten contra la seguridad informática de la empresa.

Establecer o fortalecer políticas referentes al correcto uso de los equipos, infraestructura TI y manejo del correo institucional.

Establecer políticas de control de software no autorizado, o no licenciado.

Definir e implementar políticas relacionadas con los dispositivos de almacenamiento y gestión de backups de la información.

Definir y establecer políticas sobre la gestión y ejecución de mantenimientos preventivos y correctivos de equipos, servidores, sistemas de información y la infraestructura de TI en general de la organización.

Establecer políticas para una correcta configuración, gestión y/o administración de los dispositivos de red y seguridad perimetral, tales como Firewall, IDS o IPS. Así como la configuración estricta de políticas que permitan el filtrado de servicios y puertos para conexiones realizadas a través del puerto 80 y el protocolo HTTP.

Definir e implementar las políticas relacionadas con la gestión de credenciales, así como las políticas de acceso remoto a los equipos y dispositivos de red.

Establecer políticas para la gestión y respuesta efectiva a incidentes de seguridad informática que permitan salvaguardar la ciberseguridad de la organización.

Definir e implementar políticas de actualización de los sistemas operativos, aplicaciones y firmware de los diferentes equipos y dispositivos de la infraestructura tecnológica, especialmente aquellas actualizaciones de seguridad.

Establecer políticas de seguridad que permitan validar que los sistemas y servicios tercerizados de la organización estén acorde a las políticas establecidas al interior de la organización.

Generar en el personal que labora en la empresa y demás usuarios que tengan relación con esta, una cultura de ciberseguridad a través de la socialización, capacitación y exigencia del estricto cumplimiento de las políticas de seguridad que la organización defina e implemente.

Realizar un plan de auditorías de seguridad internas que permitan monitorear, evaluar y tener control de la seguridad de los sistemas informáticos de la organización.

BIBLIOGRAFÍA.

Ambit, Building Solutions Together. (Noviembre 10 de 2020). Recuperado el 09 de Octubre de 2021 de Tipos de Vulnerabilidades y Amenazas informáticas: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas#:~:text=Se%20entiende%20como%20amenaza%20inform%C3%A1tica,o%20invadir%20un%20sistema%20inform%C3%A1tico.

Asuntos Legales (9 de Diciembre de 2019). Recuperado el 12 de Septiembre de 2021 de Acuerdos de Confidencialidad: https://www.asuntoslegales.com.co/consultorio/acuerdos-de-confidencialidad-2941910

Bytelearning. (15 de Octubre de 2019). Recuperado el 22 de Septiembre de 2021 de Reverse shell, una curiosa y al mismo tiempo peligrosa técnica: https://bytelearning.blogspot.com/2019/10/reverse-shell.html

CERT vs. CSIRT vs. SOC: ¿Cuál es la diferencia?. (2019). Recuperado de: https://www.computerweekly.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia

CIS, Center for Internet Security. (s.f.). Recuperado el 05 de Octubre de 2021 de Making the Connected World a Safer Place: https://www.cisecurity.org/

Codespaceacademy. (Julio 29 de 2021). Recuperado el 04 de Octubre de 2021 de El CSIRT y el trabajo de un BlueTeam: https://codespaceacademy.com/blog/csirt-trabajo-blueteam/

Concepto. (s.f). Recuperado el 10 de Octubre de 2021 de: https://concepto.de/codigo-de-etica/

Copnia. (2015). Recuperado el 11 de Septiembre de 2021 de Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-20): https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Deloitte. (2021). Recuperado el 05 de Octubre de 2021 de Pasos a seguir ante un ataque informático. Los planes de acción para prevenir y gestionar un tienen que tener cuatro fases: la prevención, la detección, la recuperación y la respuesta: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

Dirección nacional de Inteligencia (2013). Recuperado el 11 de Septiembre de 2021 de Ley Estatutaria 1621 del 17 abril de 2013: http://www.dni.gov.co/wp-content/uploads/2018/10/Ley-1621-del-17-de-Abril-de-2013.-Ley-de-Inteligencia-y-Contrainteligencia.pdf

Ecured. (s.f.). Recuperado el 10 de Octubre de 2021 de Kali linux: https://www.ecured.cu/Kali_linux

eltiempo.com. (2015). Recuperado el 11 de Septiembre de 2021 de Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue: https://www.eltiempo.com/archivo/documento/CMS-15141236

eltiempo.com. (2015). Caso Andrómeda: 8 uniformados no pasaron la prueba de polígrafo. Recuperado de: https://www.eltiempo.com/archivo/documento/CMS-15137795

Emagined. (s.f.). Recuperado el de Red Team vs blue team Penetration Testing: https://www.emagined.com/red-team-and-blue-team

Enter.co. (2015). Detrás de Buggly: la historia de la fachada Andrómeda. Recuperado de: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Fail2ban. (Mayo de 2016). Recuperado el 05 de Octubre de 2021 de Fail2ban: https://www.fail2ban.org/wiki/index.php/Main_Page

Fases de una auditoría (pentesting). (2017). Recuperado de: https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/

Fases de un pentesting. (2019). Recuperado de: https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/

Floridauniversitaria. (23 de Enero de 2014). Recuperado el 11 de Septiembre de 2021 de Adela Cortina en la Jornada de Desarrollo Profesional de Florida Universitaria, Adela Cortina: “Para ser un buen profesional se necesita vocación y excelencia”: https://www.floridauniversitaria.es/es-ES/noticias/Paginas/adela-cortina-etica-profesiona-floridaorienta.aspx

Gestión de eventos e información de seguridad (SIEM). (Agosto 14 de 2017). Recuperado de: https://www.computerweekly.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM?amp=1

Hardening. (Mayo 28 de 2020). Recuperado el 5 de Octubre de 2021 de: https://www.ciset.es/publicaciones/blog/746-hardening?dt=1633387962449

Incibe. (2019). Recuperado el 22 de Septiembre de 2021 de ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Incibe. (s.f). Recuperado el 05 de Octubre de 2021 de OSSIM: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/ossim

Incibe-cert. (6 de Abril de 2021). Recuperado el 23 de Septiembre de 2021 de Vulnerabilidad en archivos o carpetas virtuales en rejetto HFS (CVE-2020-13432): https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-13432

ICM. (18 de Agosto de 2020). Recuperado el 04 de Octubre de 2021 de La tecnología SIEM para la seguridad informática: https://www.icm.es/2020/08/18/tecnologia-siem/

Kaspersky. (s.f.). Recuperado el 09 de Octubre de 2021 de ¿Qué es Ciberseguridad?: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Mcafee. (s.f). Recuperado el 5 de Octubre de 2021 de ¿Qué es un firewall?: https://www.mcafee.com/es-co/antivirus/firewall.html

Open Source Security Information Management. Recuperado de: https://es.wikipedia.org/wiki/Open_Source_Security_Information_Management

Openwebinars. (22 de Octubre de 2018). Recuperado el 22 de Septiembre de 2021 de Qué es Metasploit framework: https://openwebinars.net/blog/que-es-metasploit/

Oracle.(s.f.). Recuperado el 05 de Octubre de 2021 de ¿Qué es un WAF?: https://www.oracle.com/es/database/security/que-es-un-waf.html

Oreamuno. (s.f.). Recuperado el 10 de Octubre de 2021 de LEYES Y REGLAMENTOS: https://www.oreamuno.go.cr/archivo-municipal/leyesyreglamentos/#:~:text=Ley,aspecto%20de%20las%20relaciones%20sociales.

Organización de Estados Americanos (2000). Recuperado el 12 de Septiembre de 2021 de Ley 599 de 2000 (Codigo Penal Colombiano): https://www.oas.org/dil/esp/codigo_penal_colombia.pdf

Pandasecurity. (s.f.). Recuperado el 22 de Septiembre de 2021 de Exploit: https://www.pandasecurity.com/en/security-info/exploit/

PandaSecurity. (2018). Recuperado 22 de Septiembre de 2021 de Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

PRIETO BRITO, ALEXIA, ¡Qué! (27 Noviembre de 2020). Recuperado el 22 de Septiembre de 2021 de QUÉ ES PAYLOAD: https://www.que.es/2020/11/27/que-es-payload/

Policia.(s.f.). Recuperado el 11 de Septiembre de 2021 de Normatividad sobre delitos informáticos. LEY 1273 DE 2009: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

¿Qué hacer antes, durante y después de un ataque informático?. Recuperado de: https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/.

Redeszone. (29 de Marzo de 2020). Recuperado el 10 de Octubre de 2021 de Escalada de Privilegios: cómo funcionan y cómo protegernos: https://www.redeszone.net/tutoriales/seguridad/escalada-privilegios-que-es-funcionamiento/

Redeszone. (10 de Junio de 2021). Recuperado el 22 de Septiembre de 2021 de Realiza escaneos de puertos con Nmap a cualquier servidor o sistema: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

Realiza escaneos de puertos con Nmap a cualquier servidor o sistema. (Actualizado el 10 de Junio de 2021). Recuperado de: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

RED TEAM Y BLUE TEAM - FUNCIONES Y DIFERENCIAS EN CIBERSEGURIDAD. (2021). Recuperado de: https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad.

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

Seagate. (s.f.). Recuperado el 4 de Octubre de 2021 de What is NAS (Network Attached Storage) and Why is NAS Important for Small Businesses?: https://www.seagate.com/tech-insights/what-is-nas-master-ti/

Searchdatacenter. (Noviembre de 2012). Recuperado el 05 Octubre de 2021 de Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT): https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT

SIEM open source vs. SIEM empresarial: ¿cuál es el adecuado para su empresa?. (Julio 16 de 2020). Recuperado de: https://www.helpsystems.com/es/blog/siem-open-source-vs-siem-empresarial

SOFECOM. (s.f.). Recuperado el 04 de Octubre de 2021, de SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran: https://sofecom.com/que-es-un-siem/amp/

UDistrital. (2017). Recuperado el 5 de Octubre de 2021 de POLITICAS DE SEGURIDAD: https://repository.udistrital.edu.co/bitstream/handle/11349/8322/Anexo%20C%20-%20Politicas%20de%20seguridad.pdf?sequence=4

Wazuh. (s.f.). Recuperado el 05 de Octubre de 2021 de Welcome to Wazuh: https://documentation.wazuh.com/current/index.html

Welivesecurity (20 de Septiembre de 2016). Recuperado el 11 de Septiembre de 2021 de Ética, el factor humano más importante en el ámbito de la ciberseguridad: https://www.welivesecurity.com/la-es/2016/09/20/etica-en-ciberseguridad-factor-humano/

ANEXOS

Acuerdo de confidencialidad de la organización “The WhiteHouse Security”.

Enlace que permite acceder al video de la sustentación: https://youtu.be/lJ-XD3CULcQ

Anexo 3 – Acuerdo

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas éticos y legales.

Situación problema: Análisis legal

ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y WHITEHOUSE SECURITY

Por la **parte reveladora**

Nombre: The WhiteHouse Security

Dirección: EE.UU

Teléfono: 1100011100

E-mail: Info@Thewhitehousesecurity.com

Por la parte **receptora de la información**

Nombre: Nombre estudiante

Dirección:

Teléfono:

E-mail:

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a Whitehouse Security**,** y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del proceso de selección de personal*.*

2. Que la información de propiedad de Whitehouse Security Whitehouse Security ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

   único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal*, nombre estudiante* que para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de Whitehouse Security*.*

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

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.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.

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".

   parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Whitehouse Security**,** restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

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

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

5. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

6. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

7. Responder por el mal uso que le den sus representantes a la **información confidencial.**

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

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**.**

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

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

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

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los (xxx) días del mes de (xxx) de 201_

Como Parte Receptora:	**Por la parte reveladora:**
_____	_____
Nombre del estudiante.	Nombre Gerente de la empresa
Estudiante UNAD.	Whitehouse Security
C.C. No. de	**C.C. No. de**