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

ROBERTO ANTONIO VALBUENA

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

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEA

ROBERTO ANTONIO VALBUENA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

ALEXANDER LARRAHONDO
TUTOR DEL CURSO

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

GLOSARIO

Amenaza: Estas son descritas como eventos que permiten aprovechar las debilidades de los sistemas informáticos y que permiten comprometer la seguridad de los mismos. Estas pueden venir de incidentes naturales como inundaciones, incendios, principalmente errores humanos y/o de ataques informáticos.

Ataque informático: Estas son acciones que se basan en las debilidades y en las fallas de un determinado sistema, y tienen como principal objetivo tener un beneficio, este puede ser, económico, pérdida de información o dañar el patrimonio informático de la entidad.

Endpoint: Teniendo en cuenta los aspectos de la seguridad informática estas plataformas brindan soluciones de seguridad que pueden permitir el alojamiento de servicios como firewall, antivirus, prevención de ingreso de intrusos y otras funciones que se instalan en computadores o celulares y que se encuentran conectados todos en la red.

GPL: (*General Public License*) Es una reconocida licencia que permite verificar y proteger los derechos de autor y que usualmente se usa en el software libre y le brinda a los usuarios la oportunidad de acceder a usar, estudiar y modificar un software

Impacto: De acuerdo con la norma ISO27001, es la consecuencia que se genera cuando se materializa una amenaza en un patrimonio informático.

Incidente de seguridad: Este consiste en una amenaza relativamente cercana que se puede producir por una o varias acciones de accesos no autorizados al sistema de la entidad, estas acciones maliciosas pueden violentar la política de seguridad de la información de la entidad.

Riesgo de seguridad. Este es un impacto en un patrimonio informático, que se presenta por la ausencia de controles en la seguridad para evitarlo.

Vulnerabilidad. Definiendo vulnerabilidad en el ámbito informático como una debilidad que se puede llegar a presentar en un sistema informático que compromete la seguridad de la información de una entidad. Esto se puede dar a la falta de actualización de algunos sistemas, a la falta de diseño a los errores de configuración.

RESUMEN

La principal función de implementar equipos especializados Blue team y red team estrategias que permitan a las empresas organizaciones establecer unos altos niveles de seguridad en cuanto a las amenazas actuales, el uso de estas técnicas y todo lo que conlleva la implementación de los equipos especializados nos permite mantener y defender la integridad de los activos informáticos incoherentes que buscan perjudicar a toda costa la organización.

Si tenemos en cuenta lo anteriormente mencionado, el mundo de la ciudad seguridad actualmente nos permite tener amplia de opciones de defensa un sinfín de software con características muy variadas para poder trazar perímetros de seguridad teniendo en cuenta la necesidad de la organización, pero no sólo basta con establecer una buena seguridad informática, sino que es necesario conocer las leyes y los decretos que nos pueden apoyar en la judicialización y en el proceder contra estos delincuentes cibernéticos, tener ambientes controlados y recrear sus formas de ataque nos permite hacernos una idea de cómo procederán, cómo prevenirlos y lo más importante cómo atraparlos.

El desarrollo del presente informe nos permite visualizar las capacidades en el marco de la gestión de los equipos Blue Team y red Team, y las posibles implicaciones legales y éticas que tienen los ataques informáticos y cómo nuestro proceder puede marcar el que se puedan juzgar o no estos ciber delincuentes, es muy importante para nosotros como especialistas en seguridad informática comprender a cabalidad todo lo que conlleva un proceso de ciberseguridad desde la parte legal, técnica y operativa.

Palabras claves: Blue team, Red team, pentesters, vulnerabilidades, ataques informáticos, amenazas, activos críticos, riesgos.

ABSTRACT

The main function of implementing specialized teams Blue team and red team strategies that allow companies organizations to establish high levels of security in terms of current threats, the use of these techniques and everything that involves the implementation of specialized teams allows us maintain and defend the integrity of inconsistent computing assets that seek to harm the organization at all costs.

If we take into account the aforementioned, the world of city security currently allows us to have a wide range of defense options, an endless number of software with very varied characteristics to be able to draw security perimeters taking into account the need of the organization, but not only enough with establishing good computer security, but it is necessary to know the laws and decrees that can support us in the prosecution and in proceeding against these cyber criminals, having controlled environments and recreating their forms of attack allow us an idea of how they will proceed , how to prevent them and most importantly how to catch them.

The development of this report allows us to visualize the capacities in the framework of the management of the Blue Team and Red Team teams, and the possible legal and ethical implications that computer attacks have and how our procedure can mark what can be judged or not these cyber criminals, it is very important for us as computer security specialists to fully understand everything that a cybersecurity process entails from the legal, technical and operational aspects.

Keywords: Blue team, Red team, pentesters, vulnerabilities, computer attacks, threats, critical assets, risks.

TABLA DE CONTENIDO

pág.

LISTA DE FIGURAS.

Pág.

INTRODUCCION

El mundo actual vive un constante cambio tecnológico y con él una constante de necesidades que deben ser cubiertas, eso aplica para todo y para todos actualmente, y las organizaciones no se quedan de lado es por esta razón que muchas de ellas ya ven como un activo de gran valor su información, y es que este patrimonio el cual poseen dichas empresas necesita una defensa en ciberseguridad, los grandes volúmenes de información y las tecnologías que hoy en día nos permiten almacenar, procesar y transmitir a grandes velocidades enormes volúmenes de información ameritan ser protegidas.

Pese al gran esfuerzo que realizan muchas empresas en velar por la integridad de su información, y protegerse de las innumerables amenazas que surgen diariamente, no es fácil y es que estas medidas no llegan a hacer lo suficientemente eficaces, la ineficiencia de los mecanismos utilizados para defender la información y la infraestructura tecnológica se debe al constante cambio de los mecanismos y de las herramientas utilizadas por los delincuentes, entonces cuáles innova constantemente cómo vulnerar los sistemas cómo aprovechar estas vulnerabilidades, de ahí la importancia de contar con equipos especializados en la protección y prevención de los ataques cibernéticos, el apoyo a estas actividades de seguridad en las organizaciones se hace mediante los equipos Blue Team los cuales nos permiten tener una defensa activa y constante de toda la red, Por otro lado si implementan equipos red Team los cuales junto al anterior equipo nombrado permiten la comprobación del nivel de seguridad actual del sistema, mediante el uso de herramientas similares a las utilizadas por los delincuentes informáticos, y finalmente esta manera tener una protección integralm activa y constante y esta manera lograr mantener nuestro sistema seguro.

Es por eso que el presente documento dará a conocer un informe técnico en donde plasmaremos las diferentes fases desarrolladas para la protección, prevención y contención de un escenario propuesto para la puesta en marcha tanto de un equipo Blue Team como de un equipo red tema, al igual se tendrá en cuenta los aspectos legales y éticos que se presenten durante el desarrollo de la actividad.

1. DEFINICIÓN DEL PROBLEMA

La relevancia de la ciberseguridad hoy en día aumentado tanto en las empresas como a nivel personal, esto se debe a que cada vez más se depende de la tecnología y de las herramientas que están nos ofrece para almacenar y gestionar información, procesarla y realizar automatización de algunos procesos particulares de cada empresa o persona.

Y es que cada sistema existente es vulnerable de una u otra manera, esto se debe a la gran variedad de amenazas que existen y la velocidad a la que aumenta, lo que Lo que no permite a los sistemas protegerse de una manera íntegra, por estas razones la toma de decisiones para la protección del sistema debe ser óptima y eficaz para evitar la explotación y aprovechamiento de dichas vulnerabilidades.

De ahí la necesidad de establecer equipos especializados en seguridad informática que trabajen de manera dinámica y articulada en la protección eficaz de los sistemas de tecnología e información, este tipo de equipo son denominados Blue Team y red Team, los cuales ponen en práctica habilidades específicas para la defensa del patrimonio tecnológico mediante el análisis y puesta a prueba de los controles de defensa, y es que como lo dice Lescay Arias “No basta reconocer y comprender algunas amenazas conocidas del medio, sino que se debe configurar las propuestas que se actualizan o que son novedosas y que permiten, no solo desde la protección sino asegurar que los activos de esta información se defiendan y anticipen los aspectos desconocidos o inciertos.”[1]

Pero aunque el planteamiento de dichos equipos sea una idea estupenda en cuanto a la protección y prevención de vulnerabilidades en los sistemas informáticos, se crea la necesidad de presentar esta información obtenida en cuanto a sucesos de seguridad a las diferentes directivas y personal solicitante de esta información, y es donde los informes técnicos toman vital importancia, los cuales deben ser claros y fáciles de entender, al igual debe presentar las estrategias, las consecuencias legales y el paso a paso de cómo se logra identificar, analizar y controlar un incidente de seguridad, mostrando así como los activos de la empresa se protegen mediante las acciones desarrolladas por los equipos Blue Team y red Team

[1] Arias, Michel. Estrategia de superación para la utilización de proxmox y pfsense en las instituciones de salud, Revista cubana de informática médica. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592019000200100#B13

2. JUSTIFICACIÓN

Los avances de la tecnología actual han creado un mundo más articulado con la virtualidad, y es que a menudo estamos conectados a la red, la cual nos permite desarrollar diferentes tareas, y es ahí donde toma fuerza el empezar a emplear la protección en el ámbito de la seguridad informática, y es que este concepto de seguridad en la red ha ido cambiando de manera constante con el pasar de los años, antes las empresas y las personas veían la seguridad informática como un lujo o algo innecesario, debido a que no percibían los peligros que acechan en la red, pero actualmente se ha convertido en una prioridad tanto para organizaciones como para las personas, y es que tanto a nivel particular como organizacional se manejan activos no sólo monetarios sino también de información, y este movimiento de activos es casi diario y de manera constante, lo cual obviamente nos lleva a pensar en implementar estrategias de prevención y mitigación de riesgos informáticos, lo primero que las personas piensan al igual que las organizaciones en implementar un antivirus y el uso de otros software de protección, al igual las organizaciones también toman como prioridad la creación de dependencias encargadas específicamente del tema de la seguridad de la información y la tecnología, empleando para dichas dependencias profesionales en el área con amplio conocimiento en este tema de protección y aseguramiento de información, otros que van más allá desarrollan equipos especializados para el apoyo y monitoreo constante de la seguridad y es donde aparecen los conceptos de red Team y Blue Team.

estos equipos anteriormente nombrados han tomado fuerza en los últimos años, y es que están confirmados de manera multidisciplinar por expertos en ciberseguridad, los cuales se encargan análisis del comportamiento de los diferentes sistemas de la empresa al igual que los usuarios que hacen parte de ella, en pocas palabras estos equipos hacen una defensa activa del sistema y de manera proactiva solucionan vulnerabilidades, previenen riesgos y controlan ataques. pero No obstante la seguridad informática no sólo compete a estos equipos sino que hace parte del diario vivir de una empresa y de sus integrantes, de ahí la importancia que estos equipos especializados brinden información concisa y eficaz de los sucesos de seguridad que ocurren en la organización, de tal forma que dichos informes contemplen diferentes aspectos a tratar con dicho incidente, como lo es los aspectos legales y éticos que están comprometidos con el desarrollo de un ataque, las estrategias utilizadas para la detección y control de dicha amenaza, y la prevención de los posibles riesgos detectados al igual que la creación de recomendaciones y pautas para evitar lo sucedido.

3. OBJETIVOS

3.1 OBJETIVOS GENERALES

Presentar de manera clara y precisa un informe técnico donde se relaciona los aspectos más relevantes de las actividades desarrolladas por los equipos especializados Blue Team y red Team en cuánto a un suceso de seguridad informática.

3.2 OBJETIVOS ESPECIFICOS

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

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

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

4. MARCO TEORICO

4.1 DENTRO DEL MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS

Las leyes y decretos colombianos sobre delitos informáticos y protección de datos personales existentes actualmente son:

4.1.1 Ley 1273 de 2009

Esta ley es una modificación al Código Penal, en la cual se crea un nuevo bien jurídico denominado “de la protección de la información y de los datos”, con el fin de preservar de manera integral los sistemas que usan las tecnologías de la información y las comunicaciones.

Como principales características de esta ley podemos encontrar:

- El abuso en el acceso a los sistemas de información.
- Cuando se infringe la confidencialidad, la integridad y la disponibilidad de los datos que se encuentran contenidos en sistemas informáticos.
- Procesos de intercepción de datos informáticos.
- Uso de software malicioso.
- Daños perpetuados a la información.
- Violación y uso indebido de datos personales.
- Realizar robos o estafas por medios informáticos.
- Realizar transferencias de activos sin el debido consentimiento.
- Obstaculizar sistemas informáticos o redes de comunicaciones mediante procedimientos ilegales.

Esta ley también contiene una gran cantidad de artículos dependiendo del delito informático y la violación en los derechos que se incurre mediante los mismos, y todos sus artículos regulan el desarrollo de nuevos especímenes penales que están vinculados con delitos informáticos y la Protección de Datos e información, esta ley específica penas de prisión de hasta 120 meses y multas hasta 1500 salarios mínimos legales mensuales vigentes, dependiendo el delito cometido y la gravedad de este.

4.1.2 Ley estatutaria 1581 de 2012

Esta ley contempla lo concerniente a la Protección de Datos personales, en donde las personas pueden corregir, actualizar y retractarse la información que ha sido obtenido respecto a dichas personas, que se encuentra almacenada en archivos o bases de datos.

De manera específica esta ley en su artículo número 2, nos da a conocer la manera cómo se aplicará las disposiciones de esta ley la cual aplicar a los datos personales que se encuentren registrados en cualquier base de datos susceptible a tratamiento de información por entidades ya sea de carácter público o privado.

4.1.3 Decreto 1377 de 2013

Este decreto establece la reglamentación parcial para la ley 1582 de 2012, se puede observar varias disposiciones referentes a la Protección de Datos personales.

4.1.4 ley 1712 de 2014

En dicha ley se establece la reglamentación acerca de la transparencia y los derechos que poseen los colombianos a tener acceso a la información pública de carácter nacional.

4.1.5 Decreto 103 de 2015

Mediante este decreto se procede a reglamentar de manera parcial la ley 1772 de 2014, en dicho decreto se relacionar el objeto, el ámbito de aplicación y los estándares que se deben utilizar para realizar la publicación de información.

4.2 ETAPAS DEL PENTESTING,

Una auditoría del tipo del pentesting, es una gran fuente de información, para cliente que contrata dicho servicio de auditoría, esto se debe a que el pentester realizará un ataque facilitando la información te cómo se comportará el sistema frente a este tipo de amenazas, es por eso que este tipo de test de intrusión seguían bajo unos pasos o etapas previamente definidas, para que finalmente los resultados sean los esperados, estas etapas son:

4.2.1 Etapa de contacto

En esta etapa inicial, es el momento en donde el pentester se contacta con el solicitante o cliente, y se establecen las finalidades y cuáles serían los puntos críticos para la empresa que va a ser analizada. en esta etapa también se establece de manera formal y escrita las condiciones del pentesting, se puede tener en cuenta condiciones como: el ambiente donde se ejecutará la prueba, los servicios y dispositivos que estarán dentro de la prueba, las direcciones IP a utilizar, los horarios de testeo, y se establecerá la persona responsable en el desarrollo de la labor, finalmente mediante la autorización de dicho test también se tendrán en cuenta las responsabilidades y los costos entre otros.

4.2.2 Etapa de planificación de las pruebas.

En esta etapa de la prueba se establece un espacio dedicado a la adquisición de información disponible, por lo cual se usarán scanners con el fin de contextualizarse respecto al sistema y programas que se ejecuten en los diferentes procesos de la empresa, de igual forma se revisan las diferentes actividades desarrolladas por los usuarios de tal forma que se pueda conocer qué sistemas utilizan, qué información relevante manipulan y que otros activos de información de la empresa se encuentran bajo su dominio.

es en esta etapa donde el pentester realiza el plan de pruebas, mediante el uso de plantillas que permitan la verificación y planeación de los requisitos de la prueba ya sea tanto en hardware como en software, al igual permite establecer un cronograma, los recursos tanto físicos como humanos a utilizar y las responsabilidades a cumplir.

Muy común en esta etapa utilizar herramientas de escáner como nmap, con el fin de monitorear el comportamiento de la red y de los equipos que componen la misma.

4.2.3 Etapa de diseño o modelado de las pruebas.

Esta etapa tiene como referencia la información recolectada anteriormente, y en base a ellas se procederá al diseño de la prueba para realizar el ataque a la máquina o máquinas víctimas.

en esta etapa es muy común el uso de listas de chequeo, que sirven como guía a las personas que realizan el ataque y de esta manera poder verificar que el modelo de prueba seleccionado cumple con los requerimientos. las listas de chequeo contienen una serie de ítems a evaluar, al igual que las descripciones, y herramientas a utilizar en la instrucción y finalmente los resultados reales y los esperados. Un ejemplo de ello sería el diseño de una prueba enmarcada en los niveles de acceso que puedan tener los atacantes, es decir sin acceso, con accesos limitados y con acceso ilimitado, de esta manera se podría establecer las posibles consecuencias de un ataque dependiendo su nivel de accesibilidad al sistema.

4.2.4 Etapa de ejecución de las pruebas o explotación de vulnerabilidades.

Con una estructura debidamente planeada y una base de información establecida, en esta etapa se procede acceder al sistema de la organización. esto se realiza mediante la ejecución de exploit hacia las vulnerabilidades encontradas o mediante el uso de privilegios adquiridos al ingresar al sistema. al finalizar dicha prueba se debe realizar una limpieza completa para evitar deja rastros falsos y que a futuro pueden llegar a confundir un nuevo análisis.

4.2.5 Etapa de Post-explotación o mantenimiento de acceso

La intención de esta etapa es lograr el mayor acceso posible en el sistema vulnerado, es decir lograr obtener credenciales o permisos de administrador, y de

esta manera lograr acceder a sistemas lo más importantes posibles para la empresa, mediante el uso de técnicas de pivoting entre otras.

Muchas de las veces esta etapa de mantenimiento de acceso se logra por vulnerabilidades por defecto es decir configuraciones no actualizadas o versiones de software antiguo los cuales son muy vulnerables, y son altamente conocidas sus debilidades.

4.2.6 Etapa de documentación e informe de los resultados

Finalmente al concluir con el desarrollo de las fases anteriores, se procede a realizar una documentación sobre el resultado del proceso de prueba realizado, al igual se documenta las herramientas y técnicas utilizadas y cuáles fueron las vulnerabilidades que se encontraron, esto se realiza con el fin que el cliente logre entender cuál es la gravedad de los riesgos que se descubrieron, también es importante resaltar los aspectos positivos en la seguridad del sistema y cuáles se deben corregir y cómo hacerlo. esta última fase es de vital importancia para ambas partes, lo cual da el conocimiento y comprensión al personal encargado del área de la tecnología en la empresa al igual que el ente administrativo, es por esto que se elaboran un informe de nivel Ejecutivo y otro de nivel técnico. estos informes deben incluir los registros detectados y las dificultades comprendidas al igual que las vulnerabilidades detectadas y la etapa donde se lograron encontrar, es muy importante y de gran utilidad el uso de bitácora de registro, y procesadores de texto que permitan la elaboración clara y legible de los informes para ambas partes.

4.3 HERRAMIENTAS DE CIBERSEGURIDAD

4.3.1 Herramientas

4.3.1.1 Metasploit

Esta es una herramienta de código abierto, la cual nos permite desarrollar auditorías de seguridad y pentesting, donde podemos determinar, explorar y delimitar el alcance que pueden llegar a tener las vulnerabilidades de seguridad presentes en el sistema, el metasploit más popular es el de framework donde podemos realizar acciones como.

- Instalación de puertas traseras.
- Aumento de privilegios y extracción de datos.
- Recolección y escaneo de toda la información de un equipo.
- Determinar y explotar vulnerabilidades.
- Realizar una búsqueda de errores presentes en el software de forma aleatoria.

- Eliminación del registro.
- Evasión de antivirus.

4.3.1.2 Nmap

Es un software libre y de código abierto, altamente usado para pruebas de intrusión y realización de auditorías de seguridad, mediante el uso de esta aplicación se puede realizar el escaneo de una red de datos y de esta manera lograr determinar cuántos equipos la integran, qué características técnicas contienen, entre éstas podemos encontrar las direcciones MAC, los servicios y puertos que se encuentran en uso, puertos abiertos y sistemas operativos utilizados por dichos equipos.

Sus principales características son:

- Identificar servidores, tales como computadores presentes en la red y los cuales puedan responder me mediante un mensaje ping.
- Determinar el sistema operativo y la versión que utiliza dicho equipo.
- Conocer características de hardware de red que posea el equipo analizado.
- Establecer qué servicios se está ejecutando el equipo analizado.
- Conocer características de hardware de red que posea el equipo analizado.
- Identificar qué puertos se encuentran abiertos en la máquina analizada.

4.3.1.3 OpenVas

Es un compendio de herramientas que se utilizan para analizar y explorar debilidades precedentes en los equipos de una red. su principal característica es el escaneo simultáneo de diferentes nodos, contener servicios de correo SSL, y lograr entregar reportes en varios formatos como el HTML y el XML.
un reporte entregado por esta aplicación nos muestra la descripción de las vulnerabilidades encontradas, qué puertos están abiertos y qué servicios están presentes en los mismos, al igual nos da una posible solución al problema detectado.

4.3.2 Servicios en línea

4.3.2.1 ExploitDB

Este servicio en línea es una base de datos que almacena diferentes vulnerabilidades que son compartidas por diferentes personas, las cuales dan a conocer cómo explotar dichas vulnerabilidades y de qué manera sacarles provecho.

4.3.2.2 CVE

Es una lista la cual contiene una serie de registros de las vulnerabilidades de seguridad conocidas, dichas vulnerabilidades tienen un número de identificación o ID, De igual forma contienen una descripción de dicha vulnerabilidad, las versiones de software que afectan, también se pueden encontrar posibles soluciones a la

vulnerabilidad detectada y en el caso de no tener solución mostrará configuraciones que permitan la mitigación de dicha vulnerabilidad, al igual se encontrarán diferentes fuentes bibliográficas ya sea de publicaciones en foros o blogs que hablen de dicho tema.

4.4 BANCO DE TRABAJO

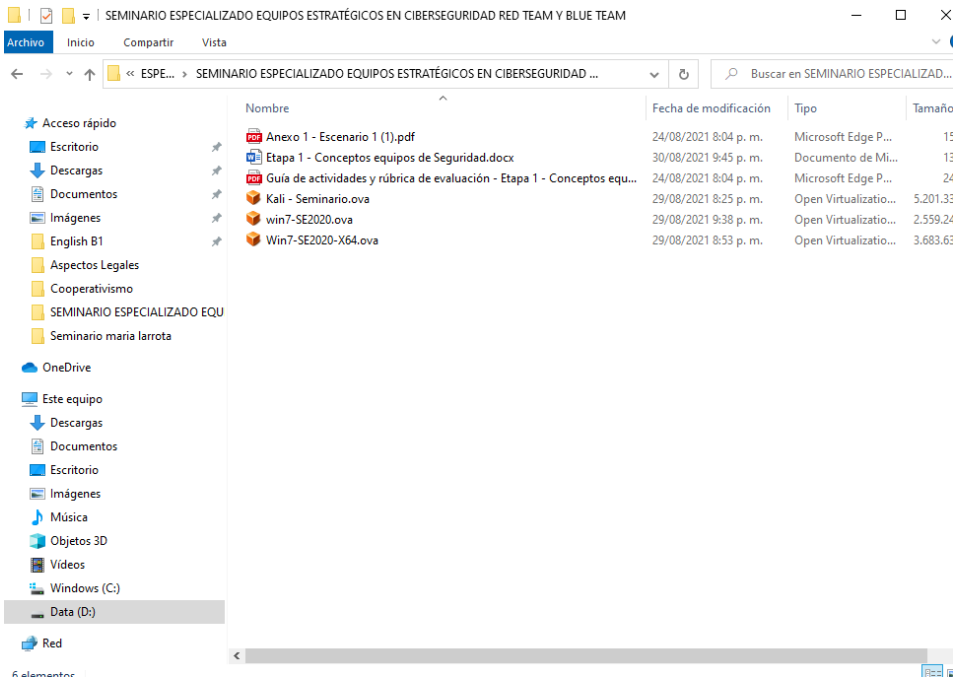
Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

Figura 1. Instalación de Virtualbox

Fuente 1: Propia del autor

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

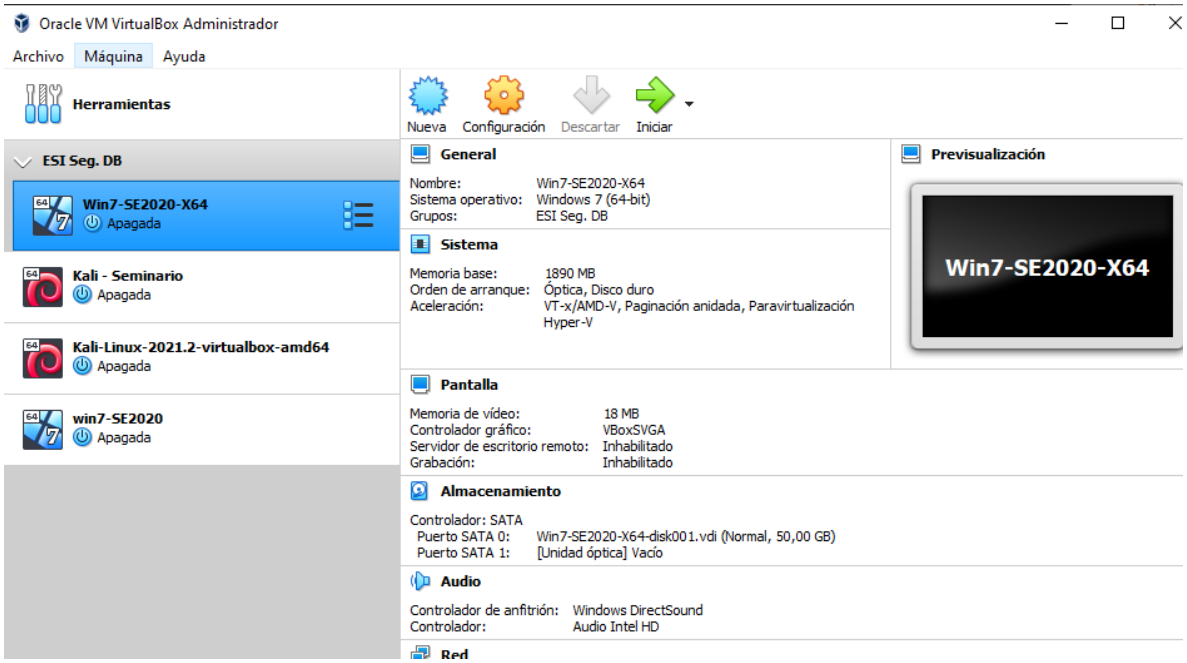
Figura 2. Descarga de las imágenes en formato OVA



Fuente 2. Propia del autor

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

Figura 3. Máquinas virtuales importadas

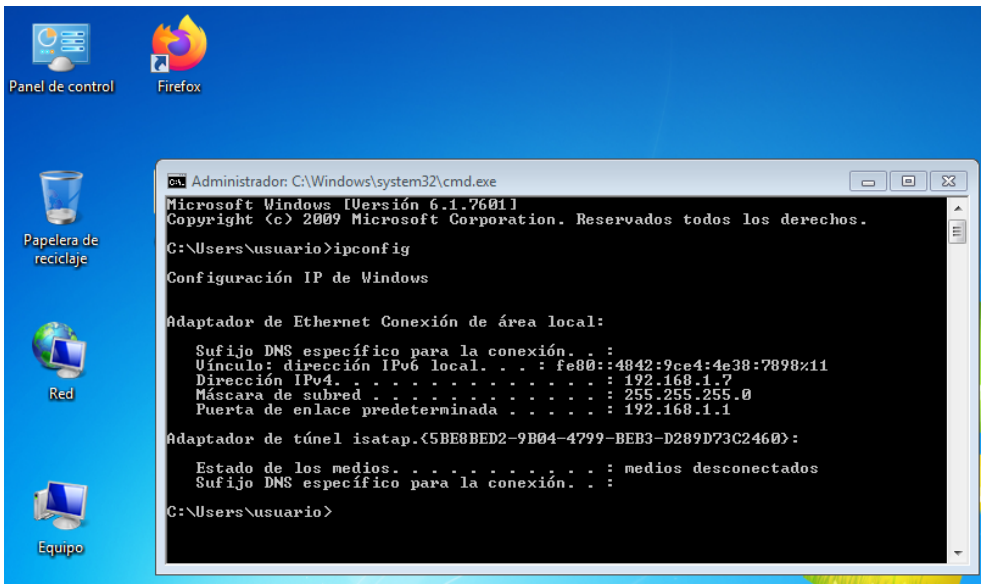


Fuente 3. Propia del autor

Prueba de conexión entre la maquina Windows 7-SE2020-X64 y la maquina Kali Linux.

Lo primero que debemos hacer es obtener la dirección IP de la maquina Windows 7-SE2020-X64, para ello usamos el comando ipconfig.

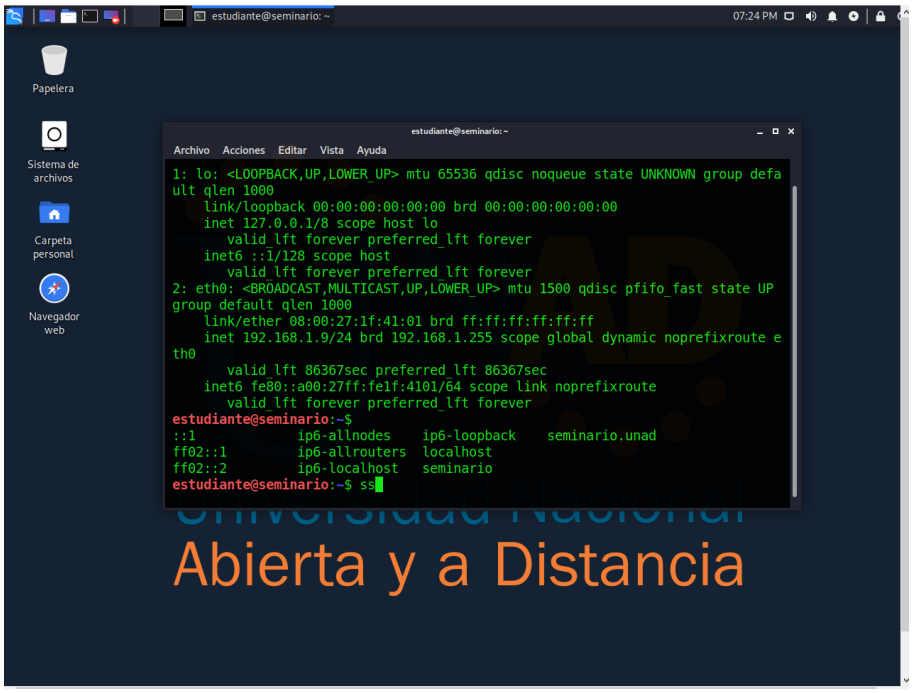
Figura 4. IP de la maquina Windows 7-SE2020-X64



Fuente 4. Propia del autor

Procedemos a obtener la dirección IP de la maquina Kali Linux, mediante el uso del comando ip a

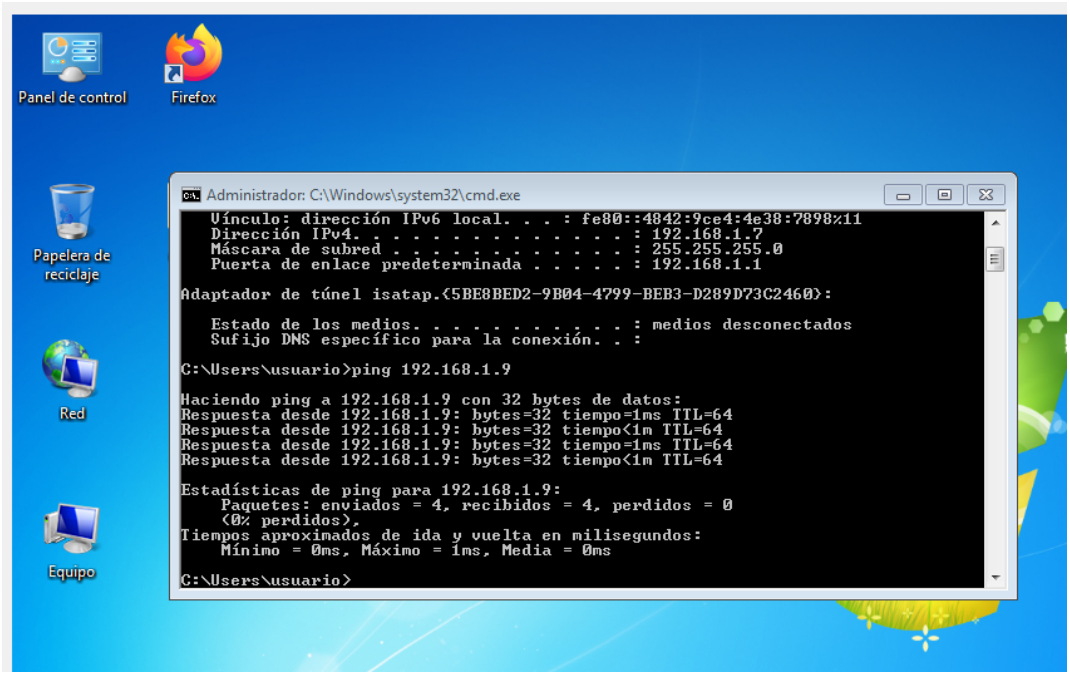
Figura 5. IP de la maquina Kali linux



Fuente 5. Propia del autor

Realizamos el envio del Ping hacia la maquina Windows don la dirección IP 192.168.1.9

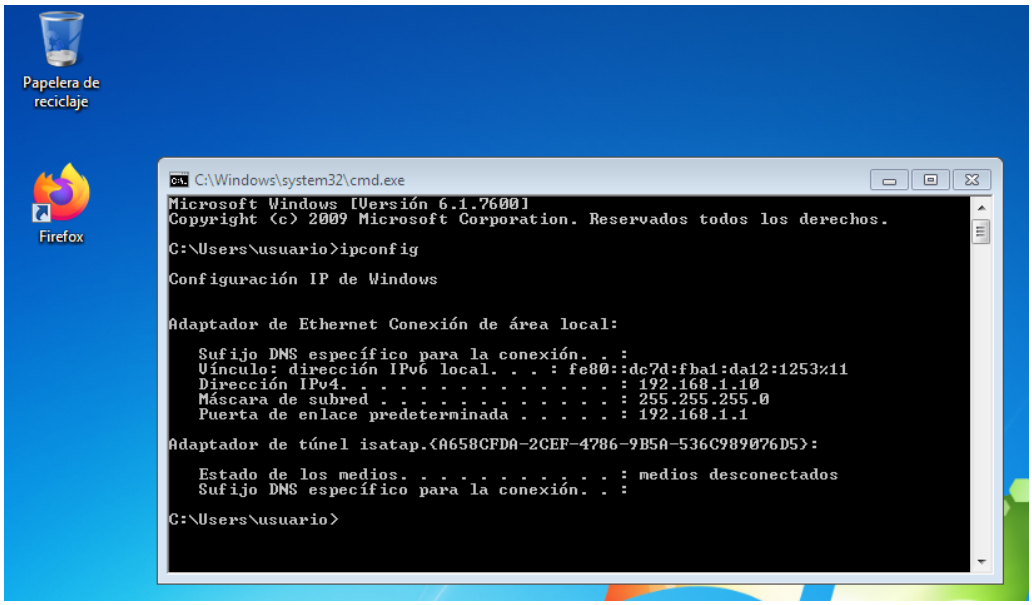
Figura 6: Ping desde la maquina Windows 64 a la maquina Kali Linux



Fuente 6. Propia del autor

Procedo a realizar la prueba con la maquina virtual Win7-SE2020, para ello hallamos la ip de dicha maquina

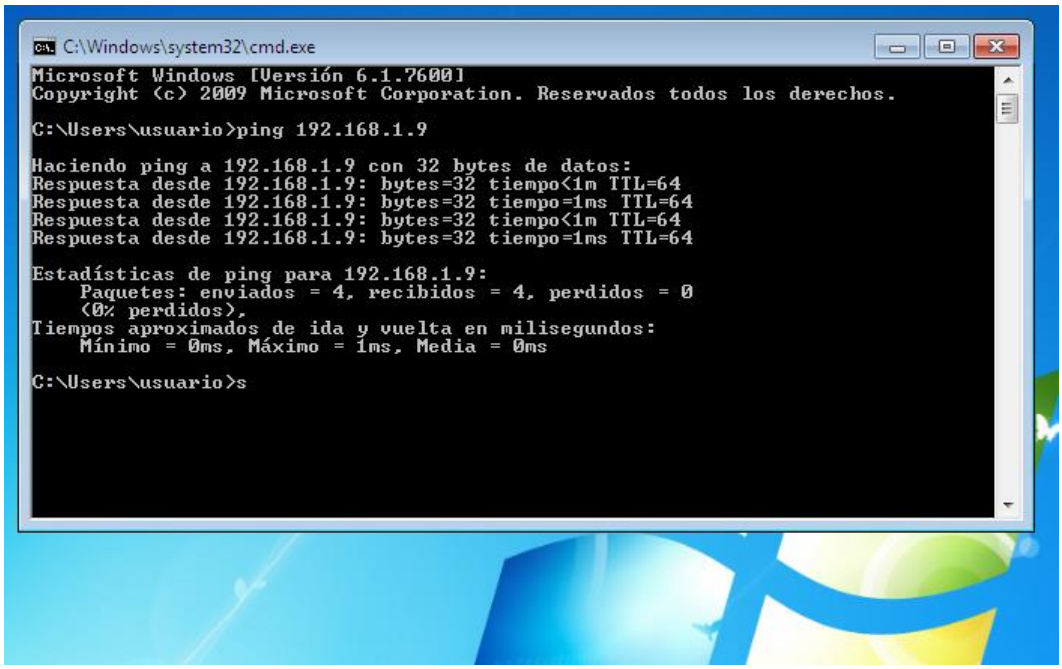
Figura 7. IP de la maquina Windows-SE2020



Fuente 7. Propia del autor

Realizamos el envió del Ping hacia la maquina Windows don la dirección IP 192.168.1.9

Figura 8. Ping de la maquina Windows se 2020 a la maquina Kali Linux



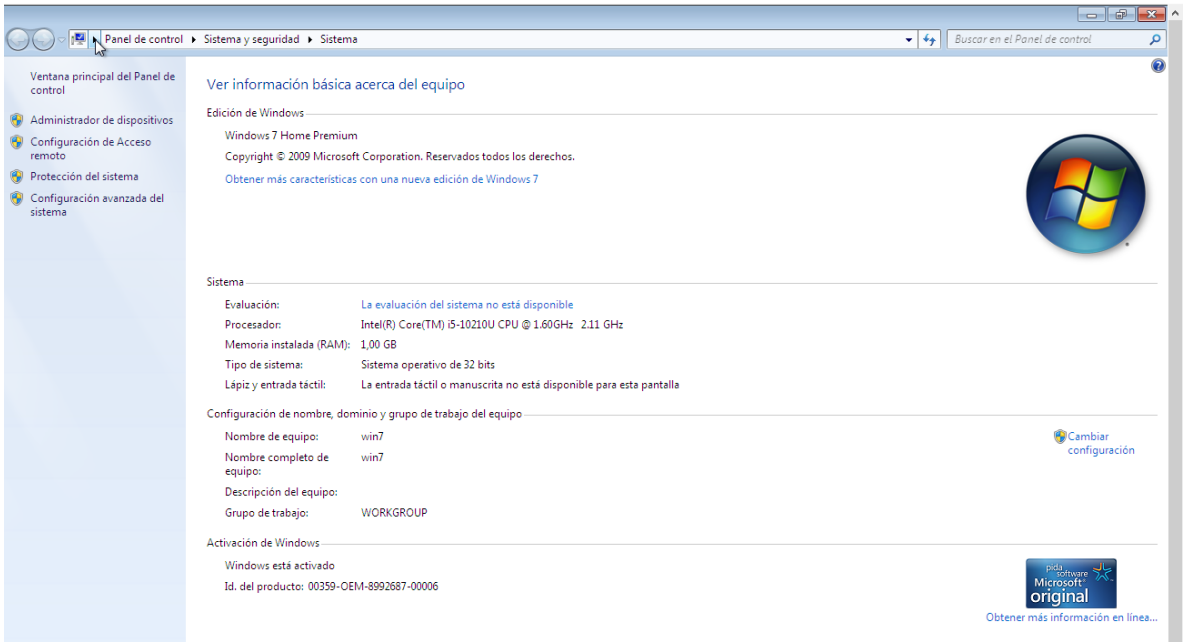
Fuente 8. Propia del autor

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

- Características de software y hardware de la máquina virtual Windows SE 2020

Esta maquina cuente con un procesador Intel Core i 5 de 10 generación con cuatro núcleos, una giga en RAM y un disco duro de 50Gb, posee un sistema operativo Windows 7 home premium original de 32 bits.

Figura 9. Características maquina Windows se 2020

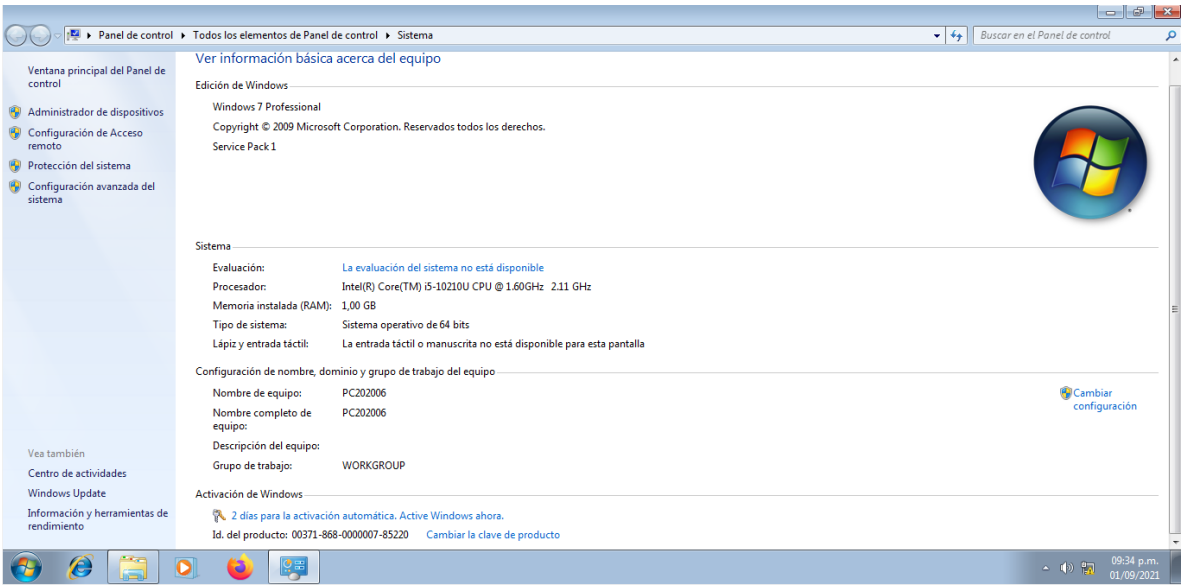


Fuente 9. Propia del autor

- Características de software y hardware de la máquina virtual Windows SE 2020 X64.

Esta máquina cuente con un procesador Intel Core i 5 de 10 generación con cuatro núcleos, una giga en RAM y un disco duro de 50Gb, posee un sistema operativo de 64 bits, Windows 7 Professional sin licencia.

Figura 10. Características maquina Windows se 2020 X64

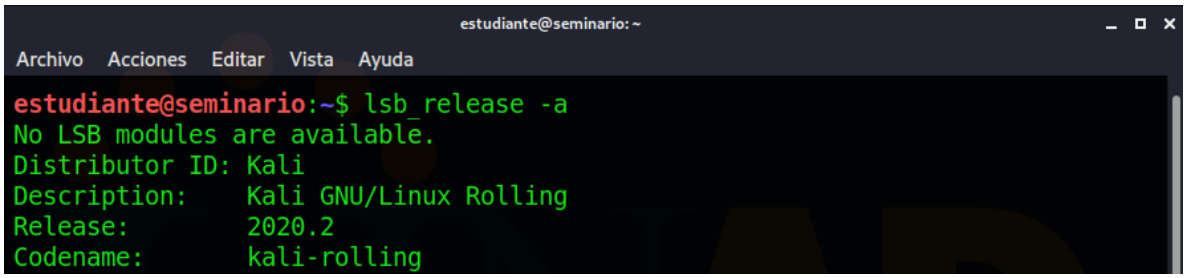


Fuente 10. Propia del autor

- Características de software y hardware de la máquina virtual Kali linux.

Esta máquina cuente con un procesador Intel Core i 5 de 10 generación con cuatro núcleos, una giga en RAM y un disco duro de 50Gb. Tiene un sistema operativo Kali Linux de 64 bits

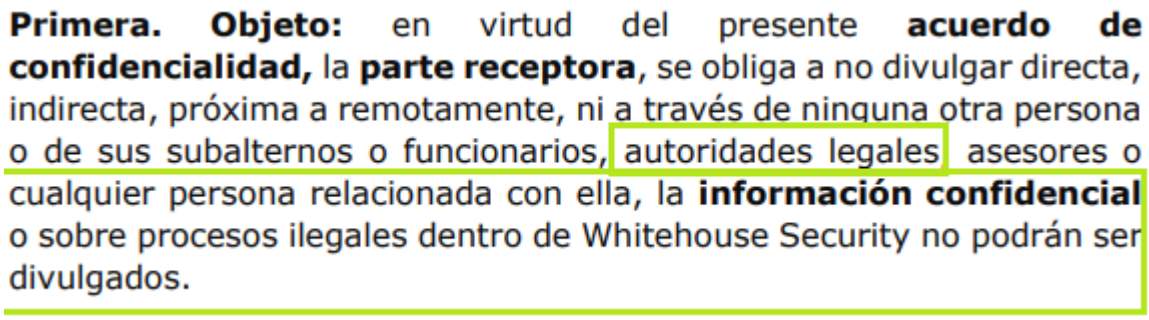
Figura 11. Características maquina Kali linux



Fuente 11. Propia del autor

4.5 ¿USTED LOGRA EVIDENCIAR ALGÚN PROCESO ILEGAL Y NO ÉTICO QUE SE ESTÉ ESTIPULANDO EN DICHO ACUERDO?

Figura 12. Fragmento ilegal primera cláusula

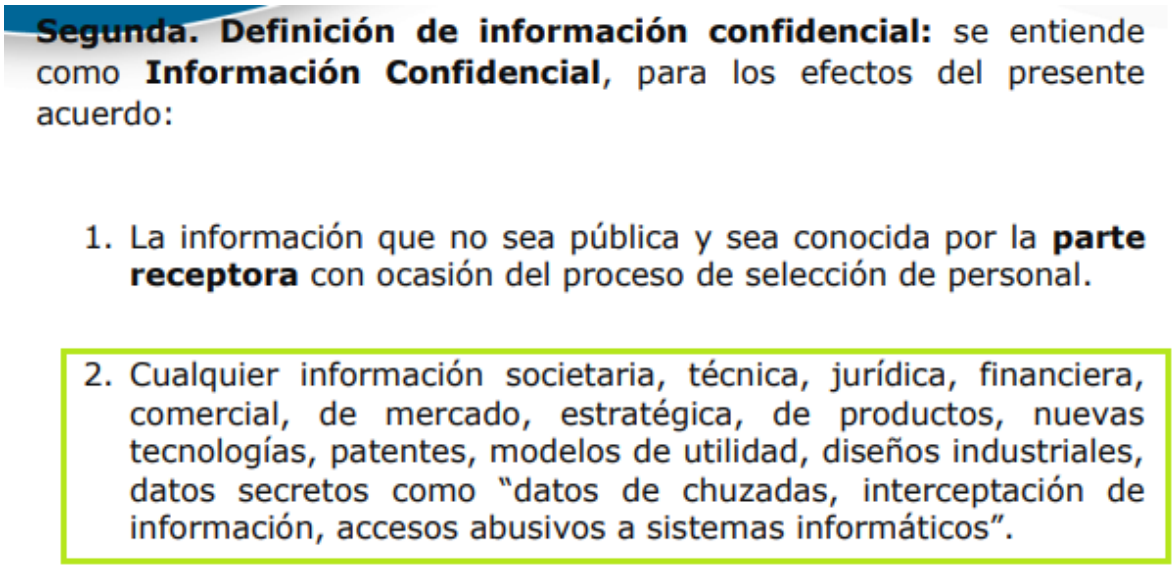

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales asesores o cualquier persona relacionada con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

Fuente 122. Propia del autor

Al momento de evaluar sí existe algún proceso ilegal en esta cláusula número uno, debemos tener en cuenta como primera medida que la empresa Whitehouse Security, es reconocida a nivel mundial por prestar asesoría a grandes gobiernos en procesos de ciberseguridad cierre de defensa, lo cual nos da a entender que manejan información muy sensible, que puede tener diferente índole y procedencia, por lo que es probable que se puedan encontrar información respecto a procesos ilegales, partimos de ahí para entender el porqué de esa cláusula, dándole a conocer a la parte receptora que no debe divulgar dicha información debido a su confidencialidad, y aclarando y haciendo énfasis en que cualquier tipo de proceso ilegal o información obtenida de los mismos no debe ser revelada por ningún tipo de comunicación ya sea física o remota, y tampoco se debe revelar autoridades, asesores y compañeros de trabajo.

Pero, aunque sea de alguna u otra forma lógica dicha cláusula, si la empresa procede hacer algún tipo de procedimiento ilegal o a manejar información de procesos o actividades ilícitas, no podemos ser ajenos a que estos van a ser desarrollados o informados a nosotros, y en este caso estamos regidos por las leyes colombianas, por lo cual al obviar o guardar información acerca de actividades ilícitas y procesos de la misma índole, estamos incurriendo en un delito y estamos faltando a la ética profesional, debido a la conducta ilegal que estamos tanto desarrollando como encubriendo y de esta manera las autoridades competentes estarían en todo el derecho a aplicarnos todo el peso de la ley.

Figura 13. Fragmento ilegal segunda cláusula, parágrafo 2

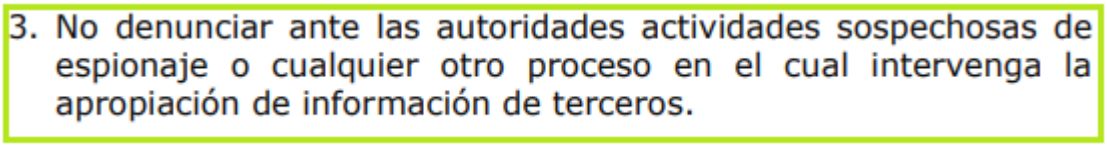


Fuente 13. Propia del autor

Leyendo detenidamente esta cláusula, podemos resaltar que la empresa aclara y define para ella que se considera información confidencial, dónde dicha información debe ser entendida y acatada por parte de nosotros y si se acepta dicho contrato, también estaríamos de acuerdo con la información confidencial proveniente de chuzadas, intercepciones de información y acceso abusivo a sistemas informáticos.

Teniendo en cuenta que algunas de las fuentes de información, son de carácter ilegal y que están penalizadas debidamente por la ley colombiana, además de llevarnos a incumplir la ética profesional, debemos tener en cuenta que al aceptar estamos incurriendo en un acto ilícito, sin importar que la empresa al manejar grandes volúmenes de información y al prestar el servicio de ciberseguridad ciudad defensa, muchas de las veces llega a estos procedimientos casi que por inercia, es necesario tener autorización legal por las autoridades colombianas o del país donde se esté realizando dichas actividades, sin importar el motivo por el cual se desarrolla debemos tener en cuenta que al no cumplir con la autorización podemos ser judicializados por dichos actos.

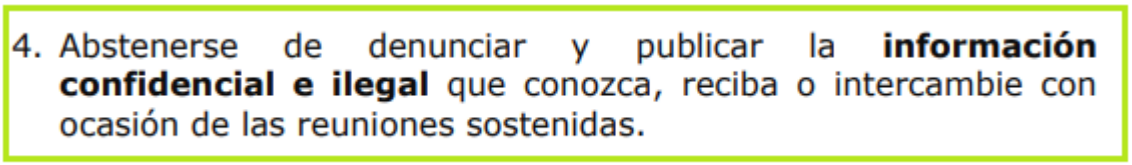
Figura 14. Fragmento ilegal cuarta cláusula, parágrafo 3


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

Fuente 14. Propia del autor

Muy claramente podemos observar en este parágrafo, la empresa le pide a su empleado parte receptora como en este caso se conoce, que no divulgue la información de actividades sospechosas de espionaje o cualquier otro proceso que se use para poder apropiarse de información de terceros, es decir se pide a la parte receptora sin cubrir los procesos ilegales que pueda desarrollar la empresa WhiteHouse Security, generando que el receptor incurre en un delito tipificado en la ley colombiana, rompiendo sus acuerdos de ética profesional mediante una conducta inapropiada y por omitir el debido proceso que deben desarrollar las autoridades competentes respecto a este tipo de actividades.

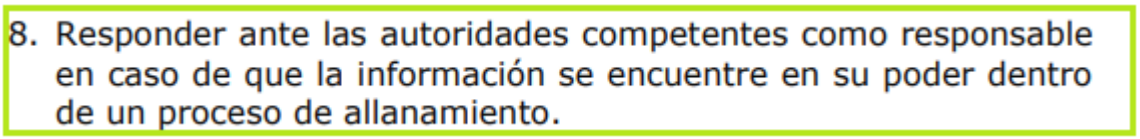
Figura 15. Fragmento ilegal cuarta cláusula, parágrafo 4


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

Fuente 15. Propia del autor

Este parágrafo nos establece claramente, que la parte receptora o el candidato al cargo, se debe comprometer con la no divulgación de la información confidencial ilegal que se llegue a conocer dentro de la empresa, mediante el desarrollo de sus actividades, es claro que se está incurriendo en un delito y en una falta grave en las normas de ética profesional, al omitir encubrir información ilegal que debe ser debidamente informada y presentada ante las autoridades pertinentes para que ellas tomen cartas en el asunto y procedan de acuerdo a la ley colombiana.

Figura 16. Fragmento ilegal cuarta cláusula, parágrafo 8

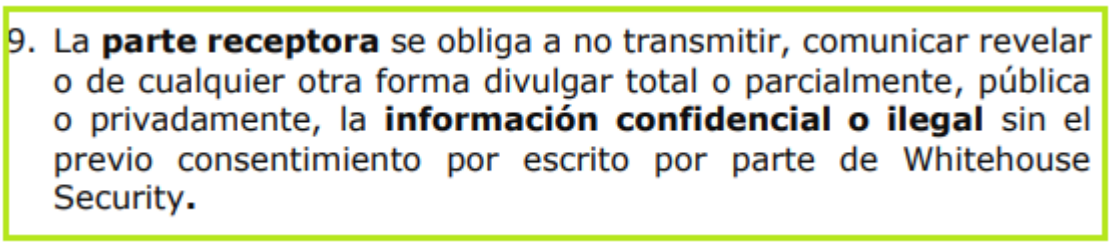

8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

Fuente 16. Propia del autor

Podemos observar en este parágrafo, la empresa le delega la responsabilidad absoluta, de la información encontrada al empleado o receptor, en el caso de que

haya una operación de allanamiento, lo cual me parece es completamente, canalla por parte de la empresa, debido a que esa información fue proporcionada por ella para que el receptor la utilice o la guarda y dependiendo de lo solicitado por la empresa, pero de Whitehouse Security Se limpia las manos con su empleado y digamos en palabras coloquiales lo pone de carne de cañón.

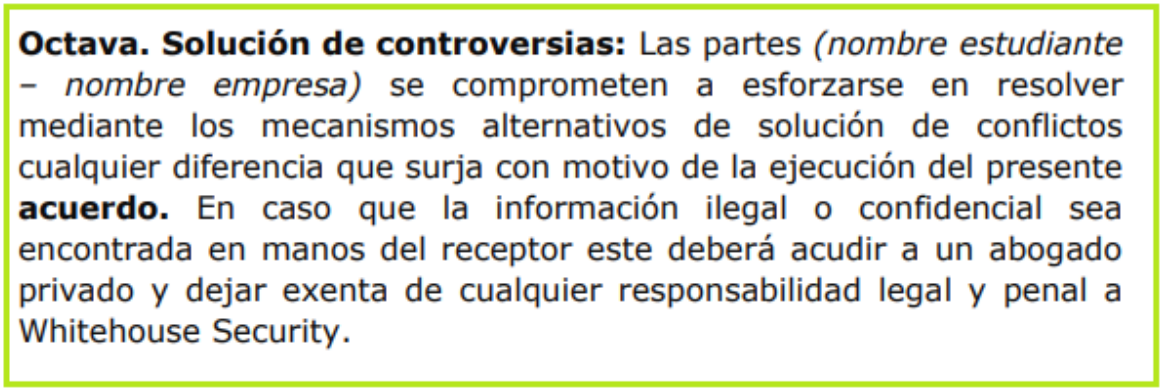
Figura 17. Fragmento ilegal cuarta cláusula, parágrafo 9


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**.**

Fuente 17. Propia del autor

Este parágrafo establece de manera clara y concisa que el empleado o receptor de la información no puede transmitir, comunicar o revelar de manera ni parcial o total la información confidencial o ilegal de la empresa, sin tener previo consentimiento por escrito de parte de Whitehouse Security, claramente este encubrimiento puede llevar al empleado o receptor a incurrir en un delito y a quebrantar las normas de ética profesional, debido a ser omisión de la divulgación a las autoridades pertinentes de conductas e información ilegal.

Figura 18.Fragmento ilegal octava cláusula.

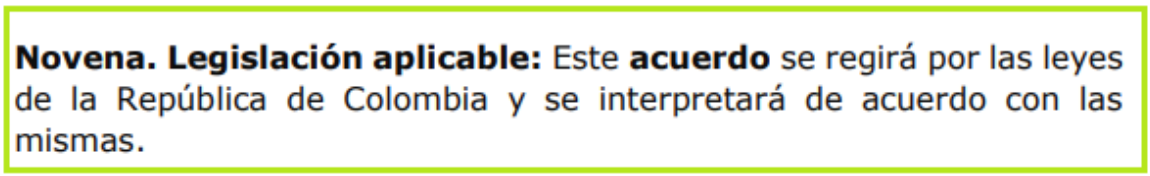

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso que la información ilegal 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.

Fuente 18. Propia del autor

Durante las diferentes cláusulas expresadas en el contrato es claro que la empresa Whitehouse Security, quiere a toda costa no hacerse cargo ni responsable de la información de carácter ilegal que pueda llegar a ella, esto se ve claramente en esta cláusula donde se expresa que el receptor debe hacerse cargo de las responsabilidades legales y penales de dicha información de procedencia ilegal, siendo también promotora de una defensa ex terna para dicho empleado receptor

que se ha encontrado con esta información, de ahí que el proceso ilegal que se esté desarrollando por el encubrimiento y posesión de dicha información recaerá solamente sobre el receptor de la misma.

Figura 19.Fragmento novena cláusula.


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

Fuente 19. Propia del autor

Dicho contrato aclara, que las anteriores cláusulas serán regidas por la ley colombiana, teniendo en cuenta esto en todas las cláusulas y parágrafos donde se habla de información ilegal o de procesos ilegales, estarían debidamente tipificados y sancionados por la ley colombiana, lo que quiere decir que incurren en una ambigüedad de términos, ya que no se puede hablar de que se rige en base a la ley de una país cuando en las demás cláusulas se habla de procesos ilegales, es como decir que robó pero estoy en desacuerdo con los ladrones, aun así no es clara la intención de esta cláusula debido a que se puede interpretar de muchas maneras y una de ellas es que lo que creamos concerniente se denuncia ante la autoridad colombiana en este caso, o por otro lado dar una falsa tranquilidad al futuro empleado debido a que va a regir por la ley colombiana.

4.6 ARTÍCULOS DE LA LEY 1273 SE PODRÍAN VULNERAR EN DICHO ACUERDO.

Teniendo en cuenta que en el anterior ítem logramos identificar varios procesos ilegales que se encontraban en el anexo 3, procederemos a mencionar los artículos de la ley 1273 que fueron vulnerados.

Las cláusulas primera y segunda al igual que la cláusula cuarta. vulnera los siguientes artículos:

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.
Este artículo es vulnerado en el momento en que la empresa WhiteHouse Security, nos da a conocer que al momento de obtener información utilizan procesos de acceso no autorizado mediante diferentes tipos de herramientas, sin consentimiento legal alguno.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.

La vulneración de este artículo se presenta debido a que mediante los procesos empleados por la empresa, se pueden causar variaciones en los sistemas informáticos y de telecomunicaciones pérdidas de acceso, a diferente información almacenada en las bases de datos y en la red intervenida.

La cláusula segunda vulnera los siguientes artículos:

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.
Se menciona la vulneración de este artículo en el momento en que la empresa informa y aclara, que una parte de su información obtenida se hace mediante medios ilícitos o ilegales, generando en ese momento el incumplimiento a este artículo que especifica que está prohibida la interceptación de datos informáticos ya sea tanto en el punto de origen como en el de destino, al igual también contempla las ondas electromagnéticas y su posible interceptación.

Artículo 269D. DAÑO INFORMÁTICO.
Según lo expresado en este artículo se genera su vulneración cuando sin previa autorización se dañe, destruya, borre, deterioro o altere los datos informáticos de un sistema de tratamiento de información. y esto lo vemos reflejado en el momento en que no se pide autorización para los procedimientos a realizar por la empresa, en cuanto a sistemas informáticos se refiere.

Por otro lado, algo otros artículos vulnerados de manera general por las anteriores cláusulas ya resaltadas e identificadas son:

Artículo 269E: USO DE SOFTWARE MALICIOSO.
La vulneración de este artículo se da cuando la empresa realiza procedimientos mediante el uso de malwar, para realizar los procesos de intercepción e intrusión en los diferentes sistemas para obtener la información qué necesitan.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES
Este artículo comprende la protección de los datos personales, los cuales incluyen información de bases de datos, ficheros y demás información que posea una persona, por lo cual se incurre en su vulneración al momento de realizar interceptación de información de cualquier persona sin previa autorización.

Articulo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. “El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.”

Como claramente se explica en el anterior artículo la empresa también incurre en la vulneración de este.

4.7 APLICARÍA A ESTE TRABAJO EN THE WHITEHOUSE

Teniendo en cuenta que anteriormente analizamos las diferentes cláusulas presentes en el contrato a firmar con la empresa The White House Security, podemos encontrar los diferentes aspectos ilícitos que éste contempla, y aunque la empresa de alguna manera justifica dichas cláusulas debido a su ocupación en el ámbito de la ciberseguridad, en mi caso considero que no amerita arriesgar mi carrera profesional y mi prestigio, por obtener dicho empleo es de tener en cuenta que al firmar el contrato tal y como está incurriríamos en varios delitos bajo la ley colombiana, Por otro lado si la empresa acepta obviar esas cláusulas y corregirlas debido a que también se especifica que estos contratos no han sido revisados debidamente, evaluaría el aceptar el trabajo, sólo si las cláusulas que fueron resaltadas en el punto anterior son eliminar del contrato.

las razones por las cuales no aceptar el contrato y que consideró ya están específicas en el código de ética establecido por COPNIA, específicamente este código de ética en su capítulo número 2 denominado “DE LOS DEBERES Y LAS OBLIGACIONES DE LOS PROFESIONALES”. Nos presentan los siguientes deberes generales de la profesión en el artículo número 31.

En este podemos articulo encontramos el literal F “Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder”[2], en donde claramente evidenciamos que es una obligación, que nosotros como profesionales denunciar los delitos y contravenciones que se puedan presentar en el ejercicio de nuestra profesión.

Posterior a este en el artículo 34 denominado “PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD”. El literal a encontramos lo siguiente: “Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación”[3], en donde como bien especifica el código de ética de COPNIA, se prohíbe a los profesionales aceptar trabajos en contra de las disposiciones

[2] COPNIA. (2015). COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

[3] COPNIA. (2015). COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

legales vigentes, y como bien sabemos analizando las cláusulas del debido contrato este incurre en faltas graves a las leyes colombianas.

También resaltamos el artículo 35 denominado "DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES", en el cual en su literal B no expresa lo siguiente: "Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones"[4], lo cual claramente se incumple al momento de aceptar el contrato con las condiciones que establece, debido a que no respetamos todas las disposiciones legales y reglamentarias con los actos que vamos a desarrollar en dicho empleo y también aceptamos no denunciar dichos ilícitos, llevando también estoy en cumplir el literal C del mismo artículo, donde no estamos velando por el buen prestigio de la profesión.

En el artículo número 39 denominado "DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL" en el literal a nos expresa lo siguiente: "Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo", donde claramente el llamado secreto profesional, se debe abolir en el caso que incumplamos con medidas legales del lugar donde nos encontramos y que sean requerido revelar información de nuestra actividad, el decir si cometemos actos ilegales y dicha información es necesaria en un proceso judicial debe ser revelada de manera oportuna.

El código de ética en su artículo 40 denominado " PROHIBICIONES A LOS PROFESIONALES RESPECTO DE SUS CLIENTES Y EL PÚBLICO EN GENERAL", es claro y conciso en expresar en su literal A lo siguiente: "Ofrecer la prestación de servicios cuyo objeto, por cualquier razón de orden técnico, jurídico, reglamentario, económico o social, sea de dudoso o imposible cumplimiento, o los que por circunstancias de idoneidad personal, no pudiere satisfacer"[5], de esta manera el código de ética nos dice que nos abstengamos de prestar servicios donde cuyo objetivo no se pueda desarrollar debido al carácter jurídico, que nuestro caso se debe a las acciones ilícitas que vamos a desarrollar, por lo cual si se acepta el contrato incurriríamos también en la falta a este artículo.

[4] COPNIA. (2015). COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

[5] COPNIA. (2015). COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

finalmente encontramos las faltas gravísimas que se encuentran expresadas en el artículo 53 de la ley 842 de 2003, en donde a mi modo de ver cabe resaltar el literal E el cual nos expresa lo siguiente: “Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares”[6], donde es claro que siempre debemos desarrollar nuestra profesión en el marco de las leyes de la República. Por otro lado el literal F hace alusión a lo siguiente ” Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente ley”, lo cual también aplica en el momento en que incurramos en las faltas anteriormente mencionadas, el incurrir en estas faltas gravísimas constituyen causa de cancelación de la matrícula profesional, lo cual significa que no podremos volver a ejercer nuestra profesión de manera legal en el país.

4.8 OPERACIÓN ANDROMEDA BUGGLY EN LA CIUDAD DE BOGOTÁ

Leyendo detenidamente cómo funcionó la operación Andrómeda, debemos resaltar que aunque fue dirigida y orquestada por un ente gubernamental como lo es el Ejército Nacional, y que se denominó una operación militar de inteligencia encubierta, no sé actuó de manera correcta, esto se debe a que todo se manejó de manera informal desde el sitio en donde se albergaban los hackers, hasta el modo como atraían a dichas personas que desarrollaban los procesos ilícitos, la búsqueda de información mediante medios abusivos y explotación de vulnerabilidades, hace notar la falta de ética y el mal proceder que se dio con dicha operación.

no resaltó que toda la culpa fuera del ente militar porque las personas que desarrollaban estos actos ilegales también sabían lo que hacían, pero es bastante contradictorio que una fuerza militar encargada de velar por el bienestar y las leyes de nuestro país, mediante el uso de artimañas y engaños como cualquier vil delincuente cree una treta, para obtener información que tenía explicaciones sociales y políticas de alto impacto en nuestro país, Por otro lado el hacer uso de población civil engañada para desarrollar el trabajo sucio, hace que la ética profesional tanto de los militares como de las personas que desarrollaban dicha actividad que por el suelo.

Los crímenes desarrollados en la acción de dicha operación mal llamada encubierta, deben ser tipificados bajo la ley 1273 de 2009, la cual ya daba las pautas para

[6] COPNIA. (2015). COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

judicial a los responsables de estas acciones, con el fin de que no quedaran impunes.

Por otro lado cabe resaltar que la información obtenida, fue tan relevante como para cambiar el posible resultado de una elección de dirigente nacional como el presidente de la República, lo que nos da a entender que se manejaba información altamente sensible, y de vital importancia en muchos aspectos de la sociedad colombiana, el manejo de dicha información no es fácil y Por otro lado se debía tener unos grandes estándares de ética profesional, y de esta manera darle el mejor trato a dicha información, aun así no era la manera de obtenerla y las personas civiles que desarrollaron dicha actividad eran plenamente conscientes de que estaban cometiendo delitos informáticos y aunque no tuvieran plenamente conocimiento de las normas estaban haciendo omisión y cometiendo un crimen independientemente de su ignorancia lo cual no borra los actos cometidos en contra de la ley colombiana.

4.9 DESCRIBA DE MANERA ESPECÍFICA LAS HERRAMIENTAS SOFTWARE USADAS EN EL REDTEAM.

- **Fase de recolección de la información.**

Teniendo en cuenta que, al realizar la solicitud para el análisis del problema, se nos facilita una serie de información muy importante, donde logramos evidenciar que existe una fuga de información al interior de la empresa, en uno de sus equipos de cómputo en la dependencia.

Debemos resaltar que la máquina comprometida tiene sistema operativo Windows 7 con una arquitectura de 64 bits, en donde dicho equipo también tiene instalada una aplicación denominada rejetto v. La cual tiene asociada un exploit que puede terminar en una Shell reversa, llegando a comprometer tanto el sistema que se han realizado procesos de escalamiento de privilegios hasta llegar a la creación de un usuario tipo administrador para el sistema.

Partiendo de esta información suministrada, debemos tener en cuenta que uno de los principales riesgos que se pueden ver de manera general es el sistema operativo utilizado, ya que Windows 7, actualmente no cuenta con actualizaciones de seguridad, esto se debe a que su creador en este caso Microsoft, a partir del mes de enero del año 2020 las dejó de emitir. y es que para su creador este sistema operativo cumplió con su vida útil y los usuarios debían migrar a su último sistema operativo denominado Windows 10. teniendo en cuenta esto el uso de dicho sistema operativo representa un alto riesgo, pues al no tener parches de seguridad las

vulnerabilidades a la fecha no tendrán un soporte, lo cual da pie a que sean aprovechadas para desarrollar ataques de diferentes tipos.

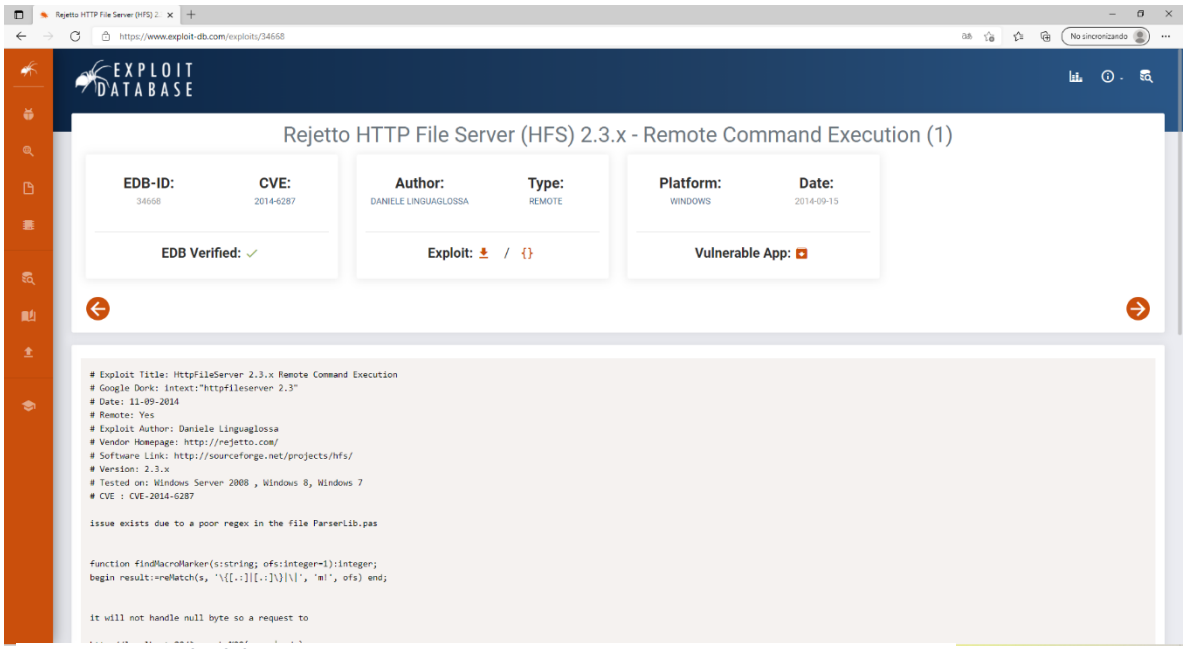
Es importante que definamos y conozcamos la herramienta que está permitiendo que el sistema sea comprometido. Rejetto v.2.3 Esta aplicación es un servidor de archivos http, este servidor web nos sirve para compartir archivos, estaba diseñado para ser libre de malware, y prestar una gran utilidad a sus usuarios, la versión que se encuentra instalada en nuestro sistema operativo Windows 7, fue lanzada en el año 2014, por lo cual debe contener versiones actualizadas pero para nuestro caso éstas no se han utilizado, Por otro lado también es importante hacer un pequeño análisis respecto a la posible instalación de dicha aplicación, lo más probable es que nunca se haya evaluado los riesgos y posibles vulnerabilidades que tenga esta versión que está usando.

- **Fase de búsqueda de vulnerabilidades**

Teniendo en cuenta que anteriormente definimos que la aplicación Rejetto v. 2.3, que se está usando en nuestro sistema Windows 7, fue publicada en el año 2014, no es raro que al digitar el solo nombre de la aplicación y su versión en la web en diferentes bases de datos de vulnerabilidades encontremos información acerca de la misma. y es que al ser una versión tan anterior las vulnerabilidades y contras los posibles ataques que se le ejecuten a las mismas también.

Mediante el uso de la aplicación web exploit database, buscamos las posibles vulnerabilidades para esta aplicación http file Server, y podemos encontrar varias vulnerabilidades certificadas es decir que fueron probadas y exitosas al momento de su desarrollo la primera de ellas la veremos en la siguiente imagen:

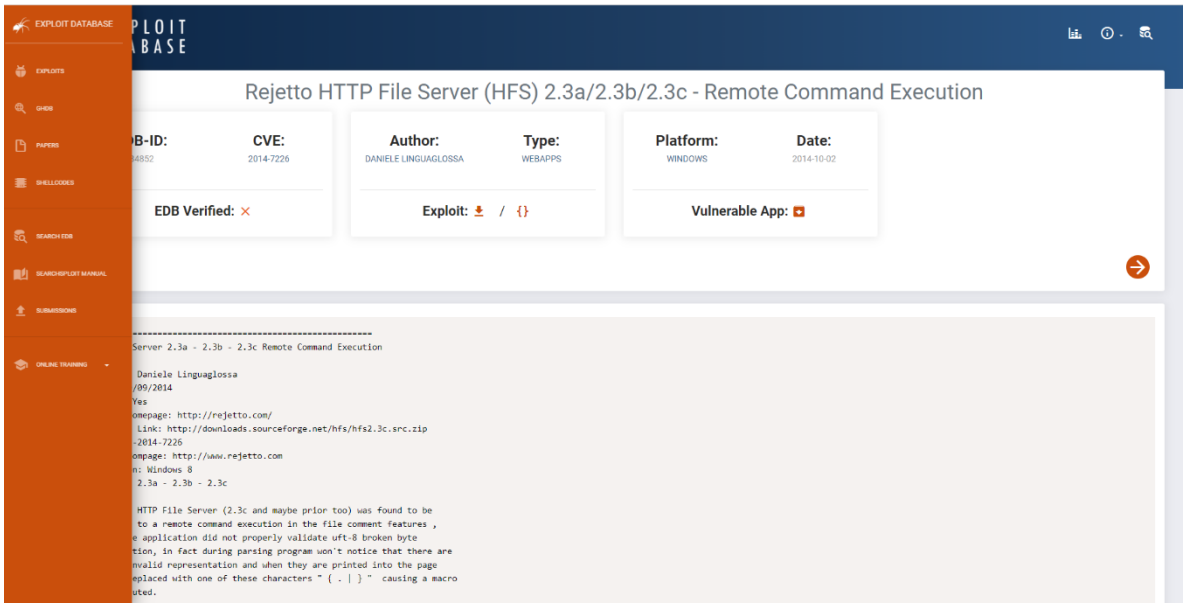
Figura 20. Vulnerabilidad 2014-6287



Fuente 20. Propia del autor

Como podemos observar la vulnerabilidad encontrada, fue publicada en el año 2014 y está verificada como exitosa, el exploit utilizado usa la función findmacromaker, la cual permite a atacantes remotos poder ejecutar o poner en marcha programas o aplicaciones que ellos desee esto mediante el uso de la secuencia %00, qué es una acción de búsqueda, que omite el filtrado. También es muy importante ver que en la descripción del exploit, nos muestra que ha sido probada o testeada En Windows 7 lo cual aplica para el caso que estamos analizando en este momento.
Pero esto no es la única vulnerabilidad existente para la aplicación Rejetto en su versión 2.3, como observaremos a continuación:

Figura 21. Vulnerabilidad 2014-7226.



Fuente 21. Propia del autor

Según lo expresado en la base de datos de vulnerabilidades, se descubrió que el último servidor de archivos HTTP (2.3c y tal vez anterior también) era vulnerable a una ejecución remota de comandos en las características de comentarios de archivos, porque la aplicación no validó correctamente el byte roto UFT-8 durante el programa de análisis no notará que hay representación múltiple no válida y cuándo se imprimen en la página será reemplazado por uno de estos caracteres " { . | } " provocar una macro a ejecutar.

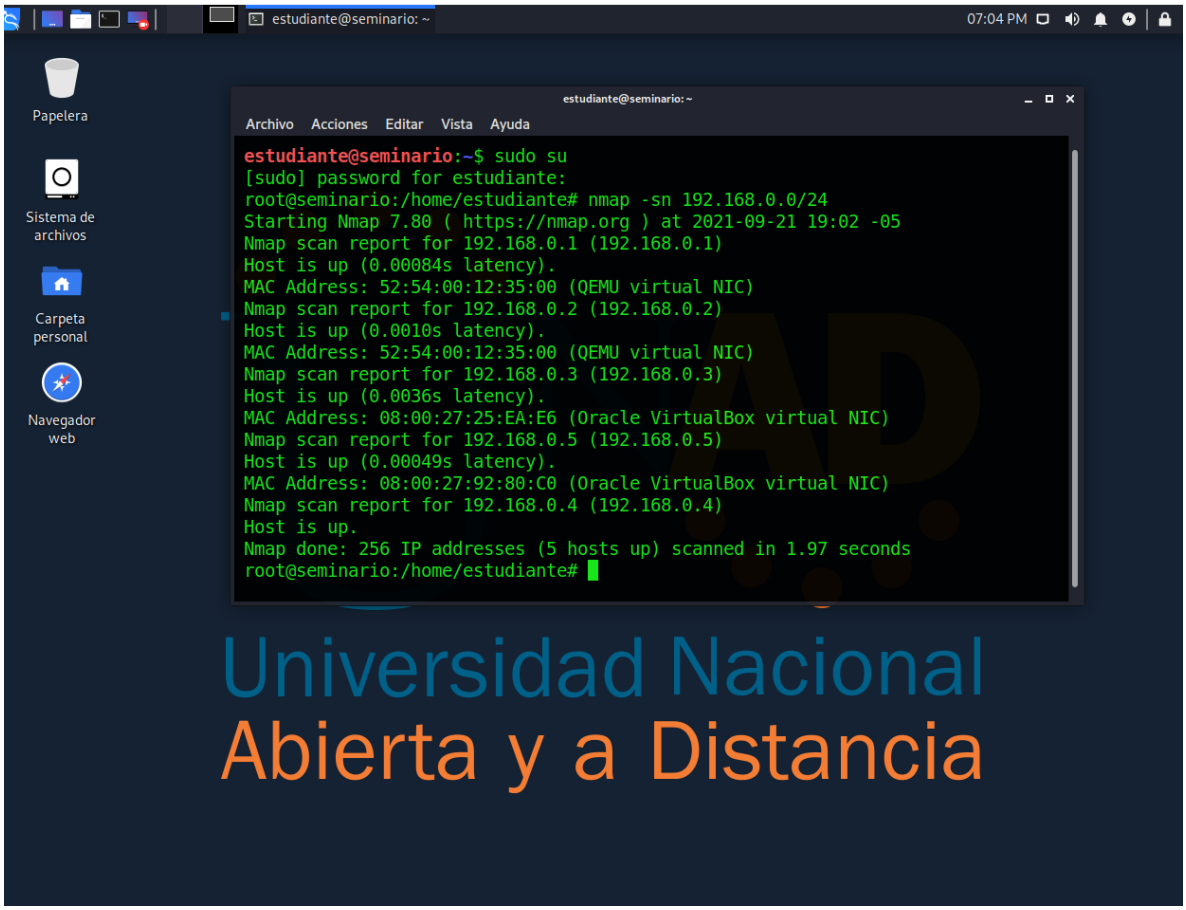
- **Fase de explotación de vulnerabilidades.**

Anteriormente se había establecido un entorno de trabajo por laboratorio de pruebas, como escenario para el posible análisis de las vulnerabilidades y ataques que puedan presentar las máquinas del entorno de trabajo, es por eso que tenemos una máquina virtual la cual cuenta con un sistema operativo Windows 7 de 64 bits., que en este caso es la máquina víctima, al igual está también cuenta con la aplicación Rejetto v. 2.3, para el análisis y explotación de vulnerabilidades usaremos como máquina atacante una distribución kali Linux, las 2 máquinas virtuales implementadas se encuentran en un mismo segmento de red, lo que nos permitirá no sólo encontrar las vulnerabilidades sino proceder a entender el procedimiento del fallo de seguridad mediante la simulación de un ataque a la máquina víctima.

para iniciar el análisis de la máquina víctima es decir nuestra máquina Windows 7, mediante la herramienta enema disponible en nuestra distribución kali Linux o máquina atacante, buscaremos identificar los puertos abiertos que nos permitan generar una vulnerabilidad y aprovechar de los mismos para lograr acceder a

nuestra máquina víctima de manera no autorizada, para esto necesitaremos la IP de la máquina Windows 7 para eso usaremos Nmap en nuestra maquina Kali Linux, donde haremos un escaneo de la red, para hallar los dispositivos activos.

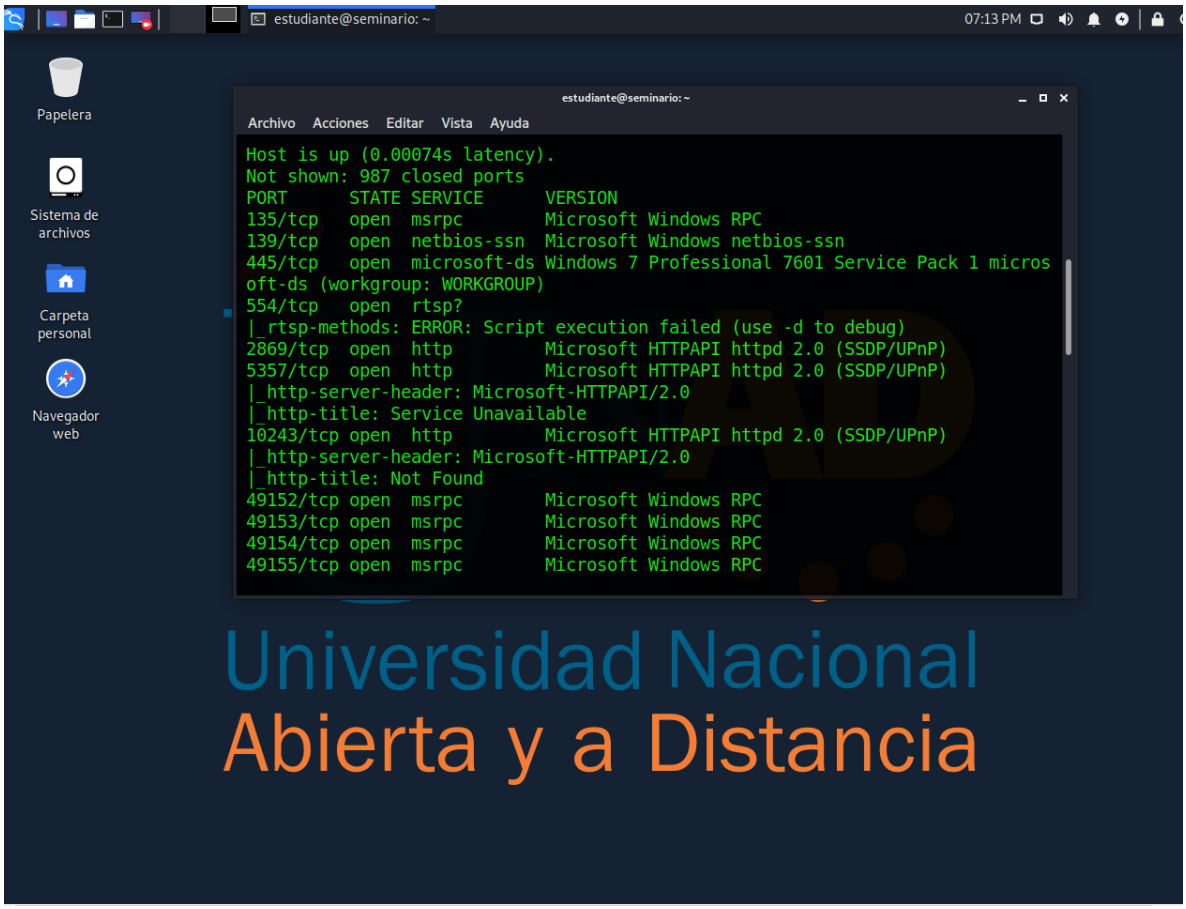
Figura 22. Hosts activos en la red



Fuente 22. Propia del autor

Como podemos observar encontramos 5 host activos, pero al realizar un pequeño análisis existen dos maquinas virtuales activas las cuales son las que estamos usando, al descartar nuestra ip de Kali Linux obtenemos que la ip que pertenece a el equipo víctima es la 192.168. 0.5, y posterior procederemos a escanear que puertos de esta maquina nos pueden presentar una vulnerabilidad y de esta manera poder atacar el equipo. Para esto usaremos el comando nmap -sS 192.168.0.5 -A

Figura 23. Puertos abiertos en la maquina victima



Fuente 23. Propia del autor

El resultado obtenido en el escaneo, en primera medida nos confirma que es la máquina que deseamos atacar por otro lado, también nos muestra los puertos abiertos y los servicios activos. En este caso identificaremos el puerto usado por el servidor de archivo http y se procederá a la ejecución del ataque pertinente para el acceso a la maquina víctima y el escalamiento de privilegios.

4.10 DATOS E INFORMACIÓN QUE LE FUERON DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD

- La información suministrada para el análisis del caso es muy valiosa, pero debemos partir de la fuga de información que está sufriendo la empresa y que proviene de uno de sus equipos de cómputo en la dependencia.

- Como segunda medida se nos informa la máquina que fue víctima del ataque con qué sistema operativo cuenta y cuál es la aplicación que está presentando la vulnerabilidad, que en este caso tenemos un sistema operativo Windows 7 de 64 bits y la aplicación Rejetto v.2.3

- El anexo también nos da a conocer que la explotación de la vulnerabilidad se debe a un exploit que puede terminar en una shell reversa y una sesión abierta de meterpreter, lo que ya nos da un indicio claro de qué vulnerabilidad debemos buscar en la aplicación, prácticamente no la describe lo que realmente necesitamos es saber que explotó, como se utiliza y cómo se hace el escalamiento de privilegios.

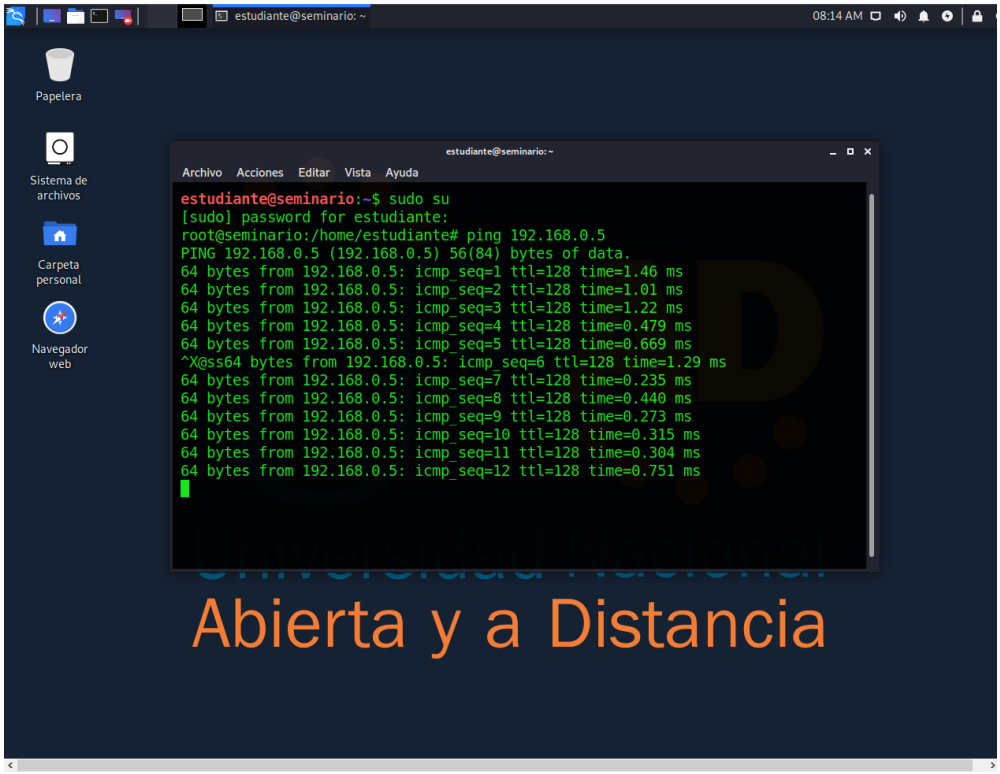
- El anexo también es muy claro hasta qué punto escalamiento de privilegios pudo llegar el ataque en este caso vemos que se llega hasta el punto de tener un usuario de tipo administrador, lo cual no se estructura el caso por completo teniendo en cuenta que debemos buscar el cómo se identifica la vulnerabilidad y cómo se aplica el exploit.

4.11 HERRAMIENTAAS UTILIZADAS PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA MÁQUINA WINDOWS 7

Mediante Kali Linux, usamos la herramienta **nmap** para conocer la ip de la maquina víctima. Identificamos si la maquina atacante tiene conexión con la maquina víctima, esto lo realizamos mediante un ping entre las maquinas.

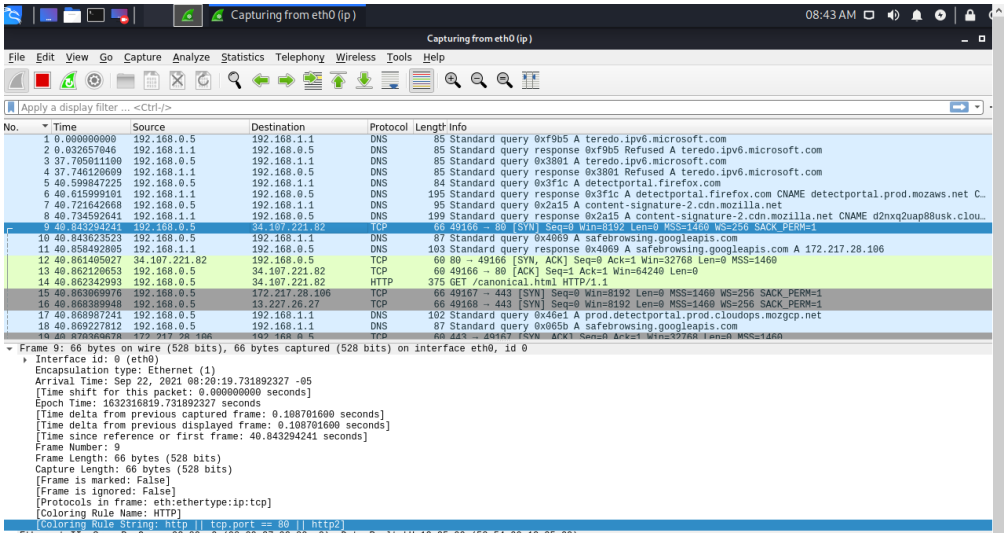
Corroborando la conexión procedemos a analizar el tráfico de la maquina victima con el fin de identificar el puerto que está usando la aplicación Rejetto v. 2.3, y de esta manera determinar el puerto y tipo de servicio que usa esta aplicación, para esto usamos la aplicación **Wireshark**.

Figura 24.Ping entre las dos maquinas



Fuente 24. Propia del autor

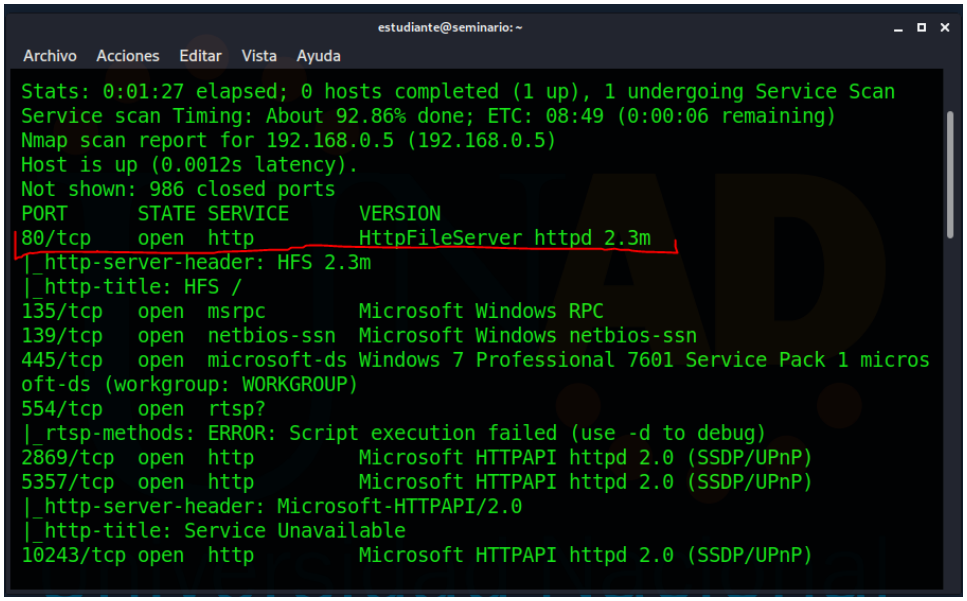
Figura 25. Análisis del tráfico de la red



Fuente 25. Propia del autor

Reconociendo que esta haciendo la maquina victima se detecta el alto trafico que genera la aplicación Rejetto v. 2.3, identificamos el puerto que hace estas peticiones tcp y la posterior conexión http, y posterior a esto usamos de nuevo la herramienta **Nmap** para analizar el estado de los puertos de la maquina víctima, donde detectamos precisamente el puerto 80 abierto y confirmamos el servicio de la aplicación.

Figura 26. Identificación de la vulnerabilidad en el puerto 80



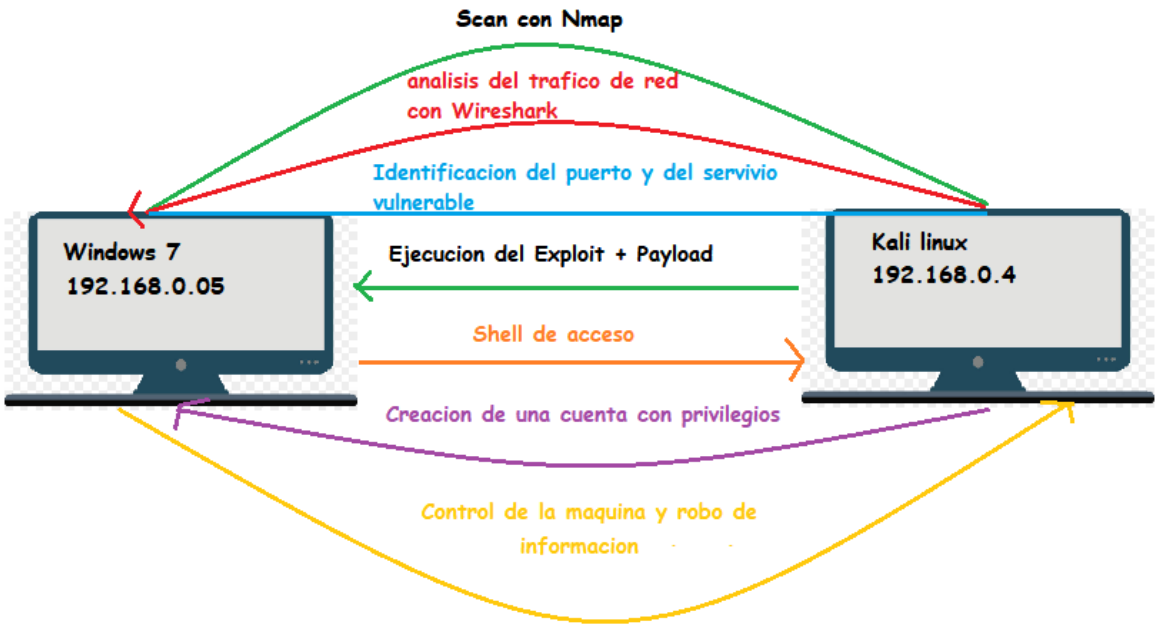
Fuente 26. Propia del autor

Indagamos en una base de datos de vulnerabilidades para la aplicación Rejetto versión 2.3, en este caso utilizamos la aplicación web **exploit database**, en donde logramos encontrar diferentes vulnerabilidades, donde según las características de la vulnerabilidad que nos da el anexo hace referencia a la 2014-6287.

4.12 CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64)

Después de tener identificado de manera especifica y clara la vulnerabilidad de la máquina, mediante el puerto 80, se emplea un exploit el cual aprovechara que este puerto está abierto por el uso de la aplicación vulnerable que en este caso es Rejetto v. 2.3, al ejecutar el exploit este nos permite como atacantes remotos realizar la ejecución de un código arbitrario, mediante la carga de un archivo con ciertas secuencias de bytes UTF-8, las cuales son interpretadas como un macro símbolo ejecutable.

Figura 27.Método empleado

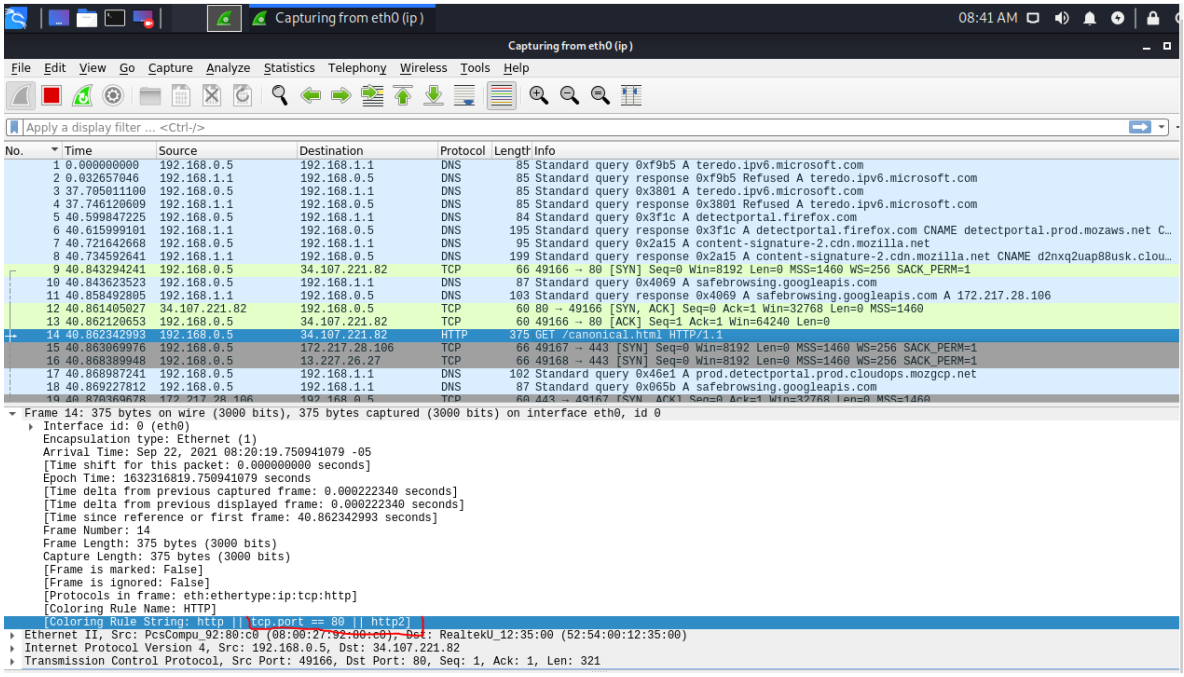


Fuente 27. Propia del autor

4.12 EXPLOTARCION DE LA VULNERABILIDAD EN LA MÁQUINA WINDOWS 7.

Identificamos el puerto y el servicio vulnerable como vemos a continuación.

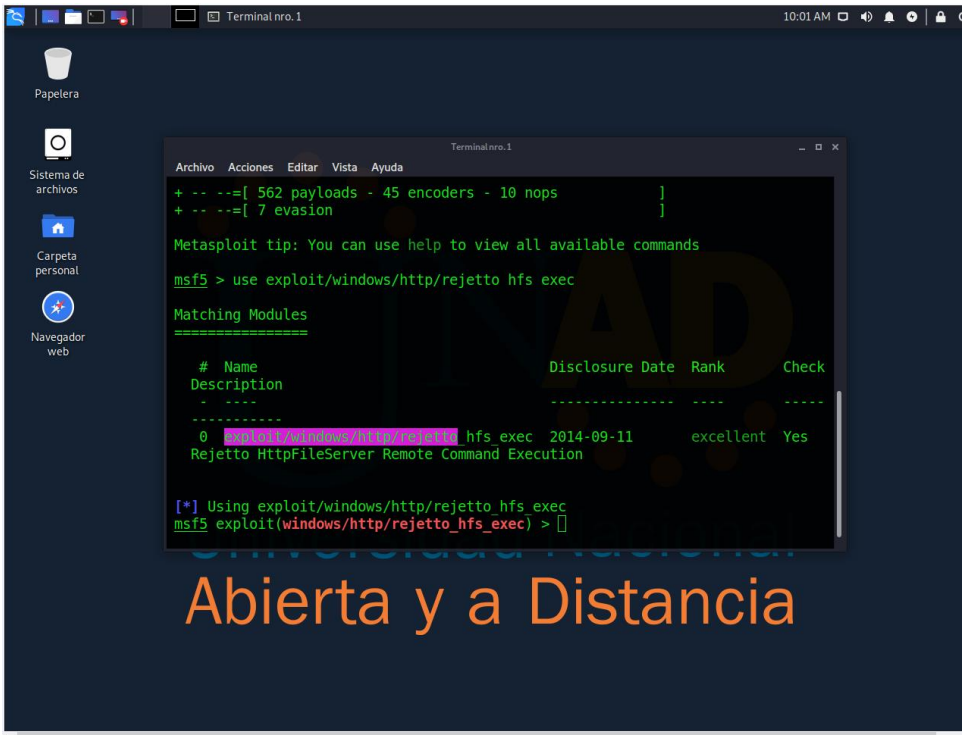
Figura 28. Identificación del puerto y servicio vulnerable



Fuente 28. Propia del autor

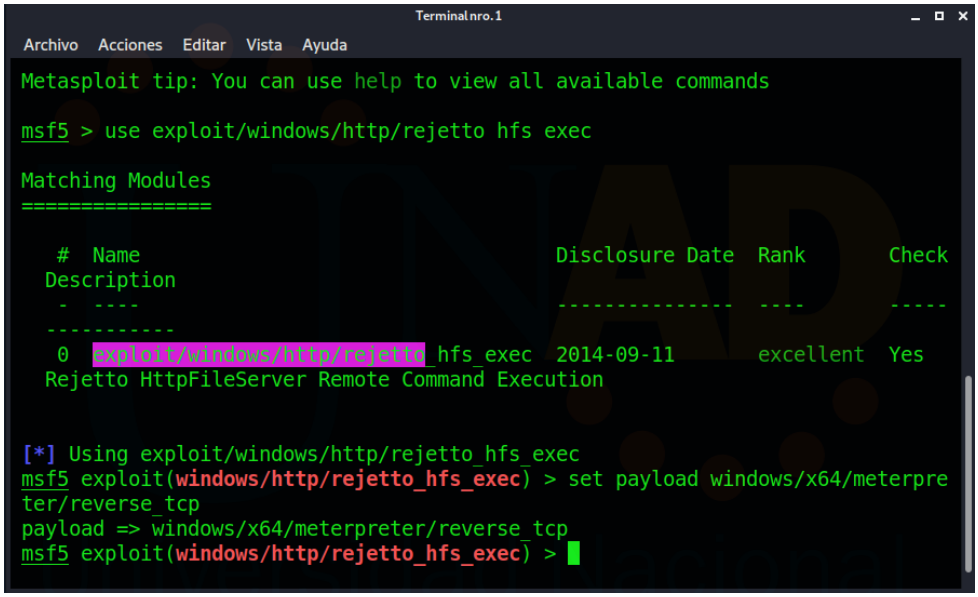
Posterior a esto procedemos a explotar la vulnerabilidad y ganar el acceso a un Shell (cmd) con el fin de tomar control del servidor, para esto usamos la herramienta Metasploit, ingresamos a la base de datos para que identificar los exploits de las vulnerabilidades que ya se conocen, después de carga el payload con el fin de que el equipo servidor realice una conexión reversa con el equipo atacante. También debemos especificar el target (RHOST), el cual es la terminal remota, que es este caso es el equipo víctima.

Figura 29. Comandos para la identificación del exploit a utilizar



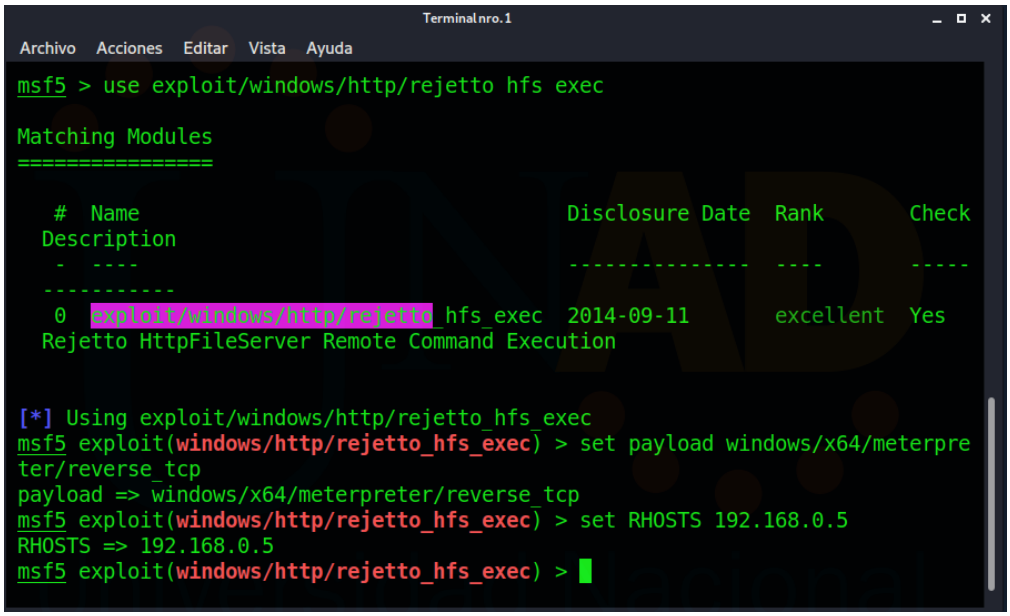
Fuente 29. Propia del autor

Figura 30. Carga del payload



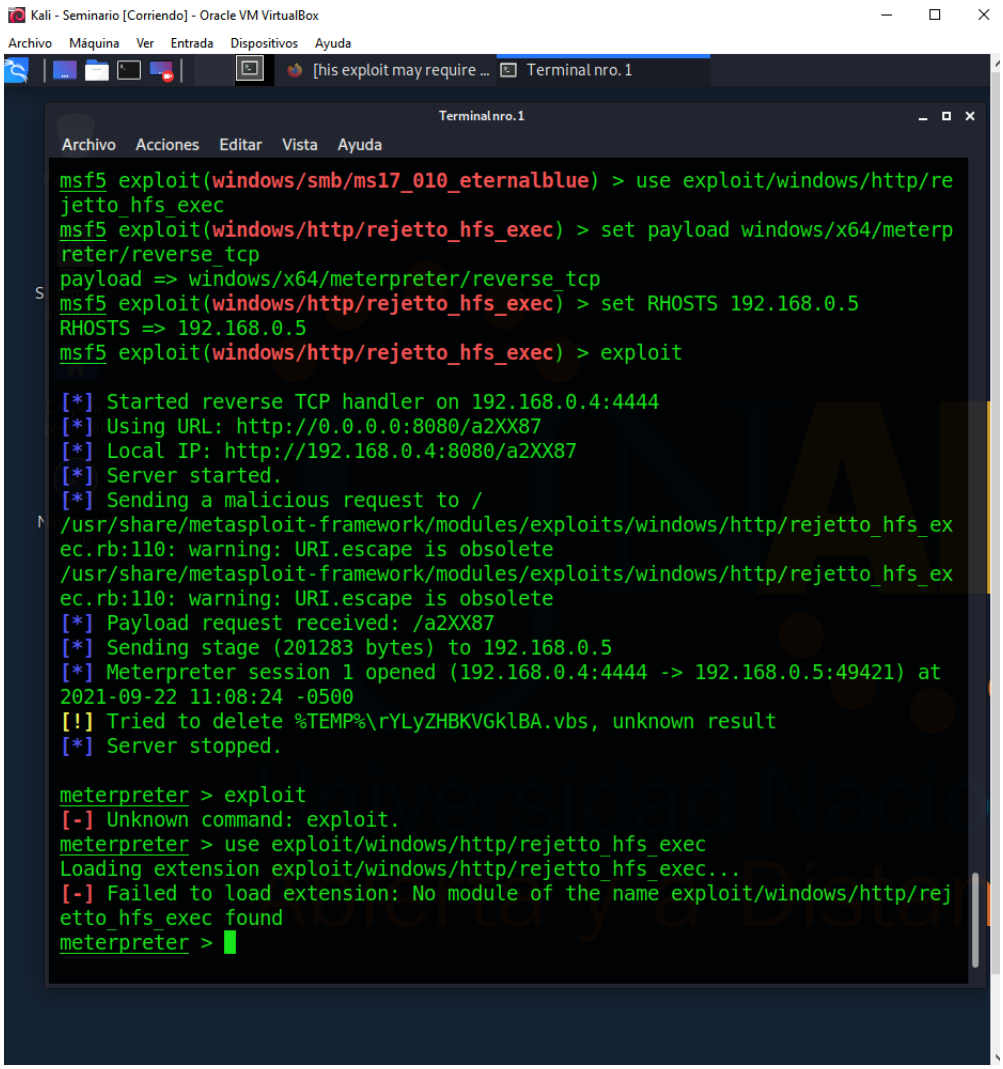
Fuente 30. Propia del autor

Figura 31. definición del target



Fuente 31. Propia del autor

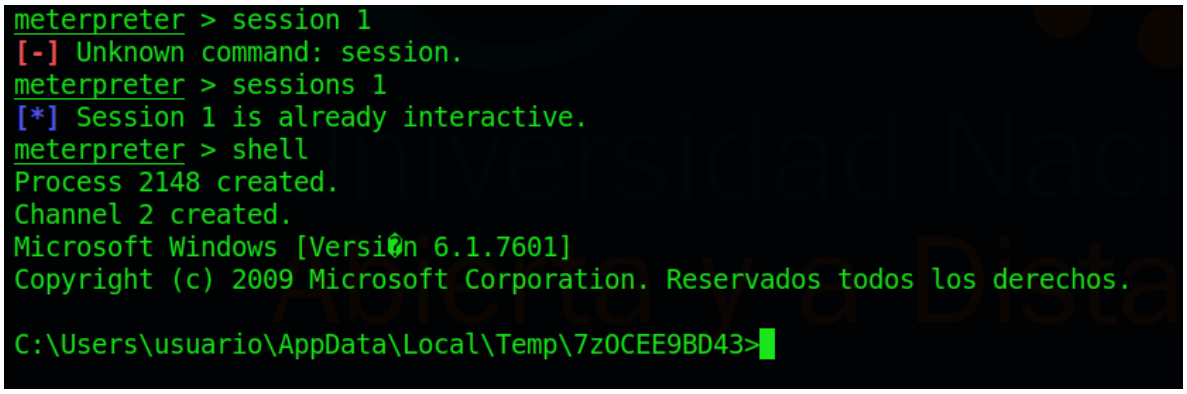
Figura 32. Ejecución del exploit y creación de una sesión



Fuente 32. Propia del autor

Iniciamos la sesión creada por el exploit y procedemos a ingresar al Shell de la maquina víctima.

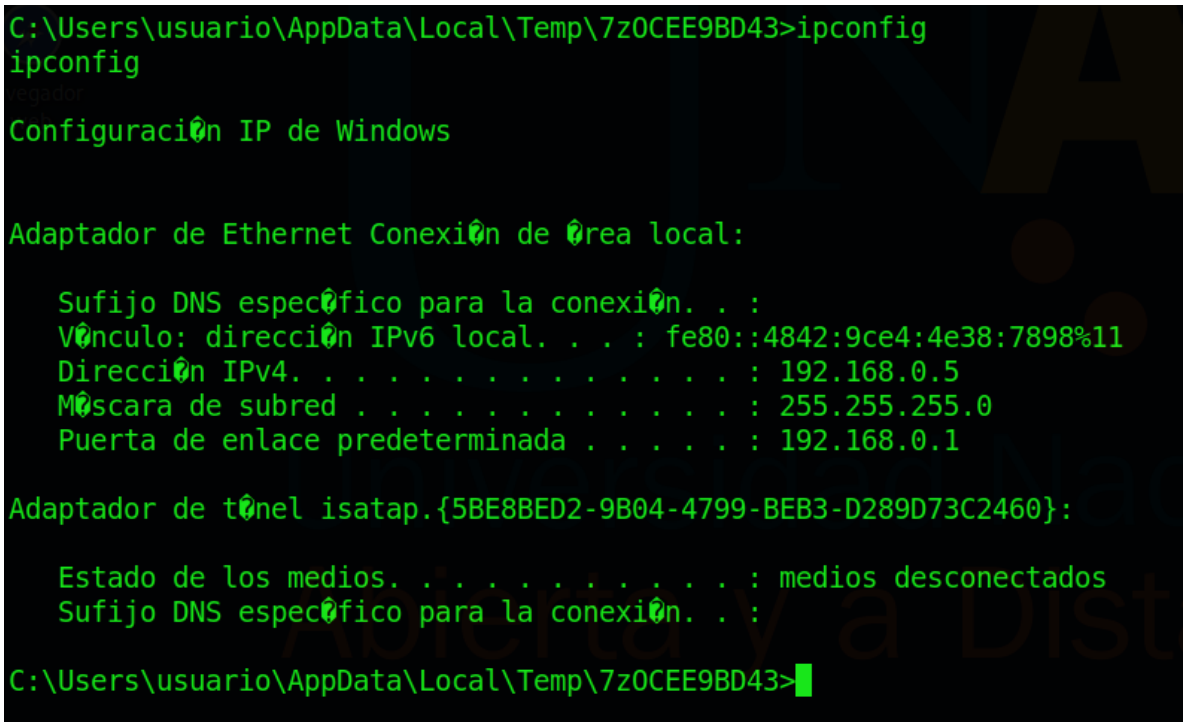
Figura 33. Acceso a la maquina victima



Fuente 33. Propia del autor

Corroboramos que ingresamos a la Shell de la maquina victima mediante el comando ipconfig

Figura 34. Ip de la maquina victima

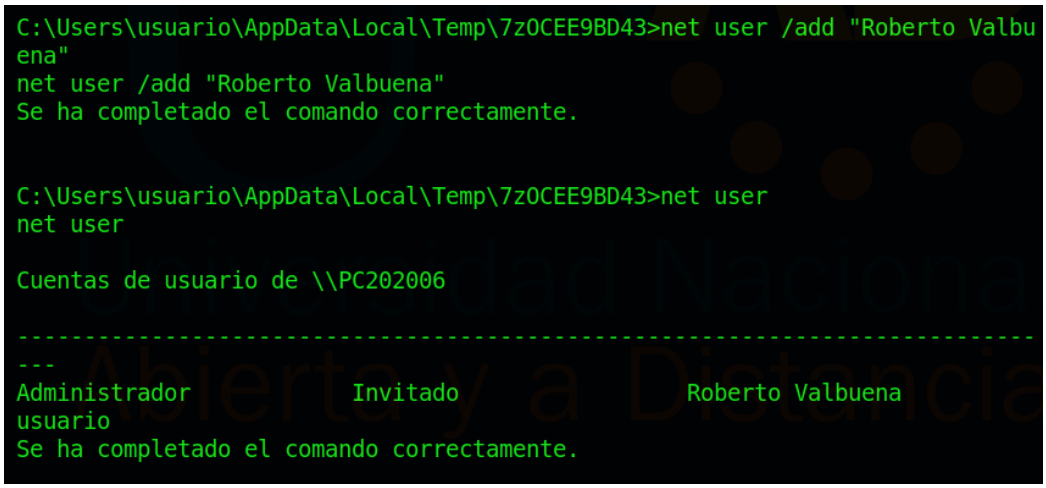


Fuente 34. Propia del autor

Por lo cual comprobamos el acceso a la maquina victima mediante el uso de la vulnerabilidad presente en el programa Rejetto v. 2.3 el cual deja siempre abierto el puerto 80 y de esta forma pudimos llevar a cabo el ataque. Procederemos a realizare el escalamiento de privilegios y la creación de un usuario con rol de administrador.

Primero creamos un usuario estándar para ver si es posible mediante los comandos que vemos a continuación:

Figura 35. creación de usuario estándar



Fuente 35. Propia del autor

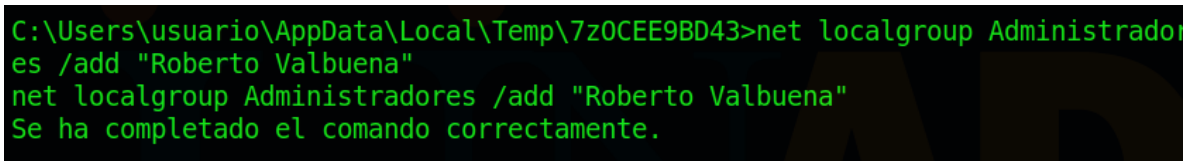
Posterior a esto revisamos los grupos de usuarios existentes en la maquina victima y obtenemos los siguientes:

Figura 36. Grupos de usuarios existentes en la maquina victima

Fuente 36. Propia del autor

Realizamos el escalamiento de privilegios al punto de crear un usuario con rol de administrador mediante los siguientes comandos:

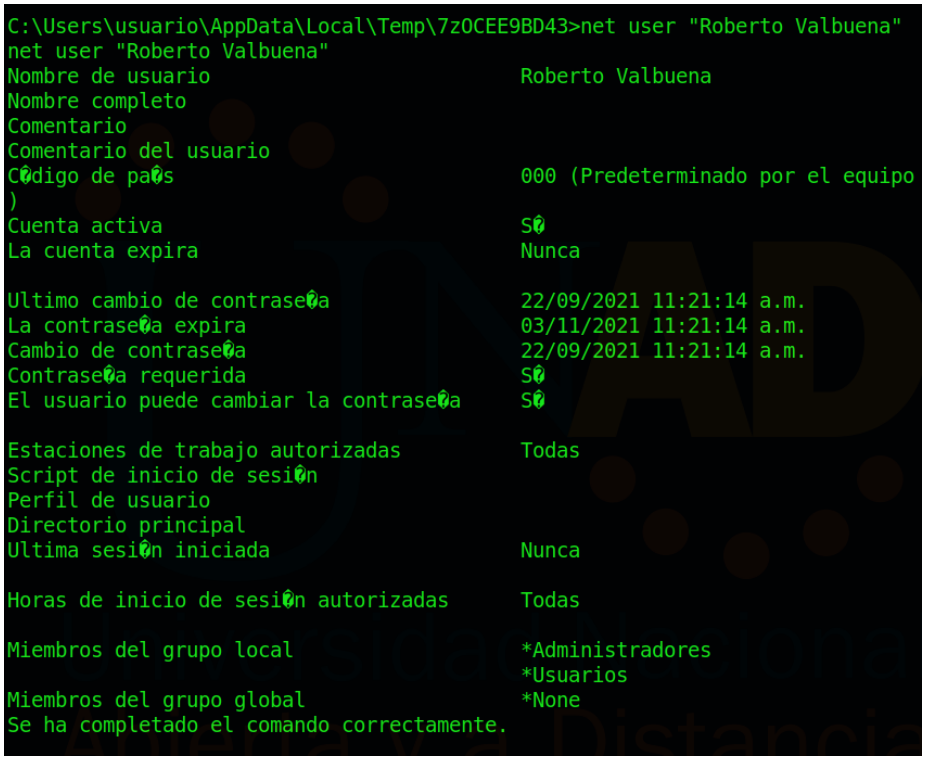
Figura 37. creación del usuario con rol de administrador.



Fuente 37. Propia del autor

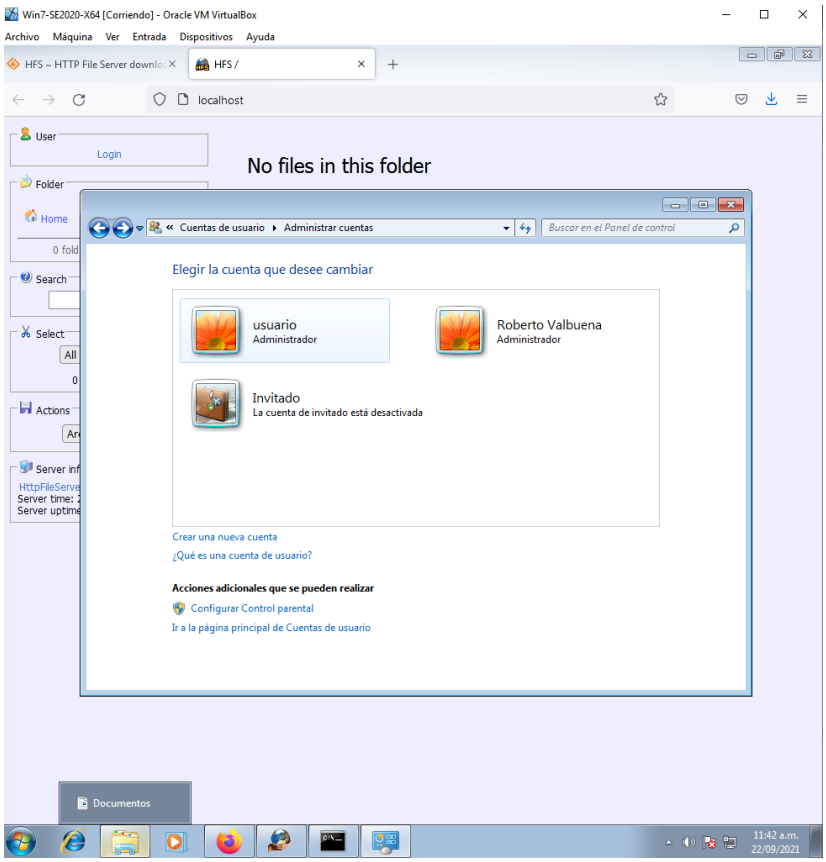
Final mente corroboramos que el usuario realmente fue agregado y tiene estos privilegios, con el siguiente comando en la maquina atacante e ingresando al administrador de cuentas de Windows 7.

Figura 38. Comprobación en Kali Linux de los privilegios de administrador de la cuenta creada



Fuente 38. Propia del autor

Figura 39: comprobación de la cuenta de administrador existente en Windows 7



Fuente 39. Propia del autor

4.13 ¿QUÉ SERÍA LO PRIMERO QUE INDAGARÍA Y HARÍA SI LLEGARA A ENCONTRARSE UN ATAQUE EN TIEMPO REAL?

Como primera medida consultaría a la empresa sí cuenta con un documento modelo para la gestión de incidentes de seguridad de la información, si la empresa cuenta con dicho documento, se procederá a establecer una estrategia la cual nos permitirá realizar la toma de cualquier decisión de manera oportuna y de esta manera lograr evitar que el incidente se siga propagando por la red, de tal forma que podamos minimizar los daños en los recursos de la tecnología de la información y las comunicaciones, al igual que minimizar la pérdida de información sensible para la empresa, la integridad de la misma y la posible eliminación de dicha información. Para esto debemos tener en cuenta las siguientes fases:

Monitoreo: en esta fase haremos uso de los elementos de hardware software presentes en la empresa y que están encargados o tienen como función el monitoreo de la red, esto con el fin de poder detectar el incidente, Y también

establecer el funcionamiento en el que se encuentra nuestra red o dado el caso sí dejó de funcionar.

Señales de alerta: Por otro lado, se debe tener en cuenta que la gran mayoría de los sistemas de monitoreo cuenta con señales de alerta o alarmas las cuales informan al personal encargado de la supervisión y mantenimiento de la seguridad informática, de la posible alteración del funcionamiento normal o intención de ataque externó o interno en la red.

Identificación: esta función está a cargo tanto de los equipos de monitoreo como de los funcionarios encargado de la seguridad informática, y es que la identificación se define mediante filtros y políticas de seguridad, todo esto se basa en el procedimiento establecido para la identificación y prevención de ataques, teniendo en cuenta que en las 2 fases anteriores se hizo un monitoreo y se puso en alerta al personal pertinente, se cuenta con información preliminar que permite proceder a realizar análisis de logs de los equipos afectados y según lo comprometidos que estén proceder de una u otra manera.

Contención: está fácil será el encargado de contener de manera completa las acciones que se están desarrollando en el ataque perpetrado, de esta manera mitigar y controlar dicho ataque, con la previa identificación y monitoreo de la situación que se está presentando en el sistema, se buscará evitar que se continúe desarrollando el ataque y que en el peor de los casos se propague por toda la red, y en primera medida se evitará a toda costa que se generen daños en la seguridad de la información y en la estructura TI.

Para esto también se cuenta con una serie de Marcos de seguridad como el CSF (V1.1, 2018) del Instituto Nacional de estándares y tecnología o NIST. Dentro de este marco se encuentra un enfoque llamado framework core el cual nos determina 5 funciones que se desarrollarán de manera continua y simultánea al desarrollo del ataque, estas funciones son:

- Identificar: esta nos permite conocer qué activos, datos y competencias tiene la empresa dentro de su red, y con qué recursos y elementos se soportan o se determinan cuáles son funciones críticas, al igual se determina los riesgos de seguridad informática que puede generar la afectación en dichos elementos.
- Proteger: en esta función se desarrollará las técnicas en contra del ataque y se procurará salvaguardar, los activos críticos de la empresa y se procederá a mitigar y contener las posibles afectaciones en el sistema.
- Detectar: para esta función se implementarán las estrategias y métodos que permitirán de manera adecuada un monitoreo continuo y de esta manera tener en tiempo real los eventos que están afectando nuestra ciberseguridad.

- ❖ Responder: teniendo un adecuado diagnóstico del Estado de la red, se deben establecer las acciones y actividades que permitirán la contención y respuesta al evento de seguridad y su posible mitigación.
- ❖ Recuperar: finalizando el evento negativo para la red se procede a volver a la normalidad y restablecer los servicios que se prestan diariamente.

4.14 MEDIDAS DE HARDENIZACIÓN PROPUESTAS PARA QUE EL ATAQUE NO SE REPITA

Para el para el ataque desarrollado en el caso anterior debemos tener en cuenta las siguientes acciones con medidas:

- ❖ Realizar el parcheo de las posibles vulnerabilidades existentes.
- ❖ Desactivar las opciones de acceso remoto.
- ❖ Realizar las debidas actualizaciones a los sistemas operativos y mantenerlos actualizados constantemente.
- ❖ Establecer la ejecución de servicios para usuarios con privilegios de no administrador.
- ❖ Actualización y uso de software antivirus debidamente licenciados.
- ❖ Uso de herramientas para la implementación de seguridad perimetral.
- ❖ Actualización y uso de software antiransomware, dichas aplicaciones deben ser debidamente licenciadas…
- ❖ Uso de herramientas de alerta frente a actividades sospechosas como lo son las IPS y IDS.
- ❖ Uso de sistemas integrados IoC.
- ❖ Uso de cliente EDR.
- ❖ Realizar manejo de información encriptada.

El proceso de Hardening, si implementa en varias capas donde se inicia por la más superficial desarrollando un perímetro hasta la más profunda que en este caso sería el servidor.

Perímetro: este se establece con el fin de integrar soluciones que permitan la protección en nuestro caso de las aplicaciones web, para lo que se pueden implementar WAF, evitando así ataques de tipo exploitDB, inyecciones SQL, entre otros muchos tipos de ataques que existe, está así que se puede llegar a establecer una serie de políticas para el firewall en donde se pueden restringir las conexiones dependiendo el acceso de donde se solicitan, la dirección IP de donde provienen, y la posible reputación que tenga la misma.

Endpoint: el destino final de las conexiones que en este caso lo conocemos como endpoint, que para el caso de estudio es el servidor que está a cargo de la ejecución de la aplicación de servicio, debe tener una serie de medidas de protección de manera adicional como lo vimos en el punto anterior.,

Firewall: este elemento de protección perimetral permite que una red tenga establecida una serie de políticas de control en cuanto al tráfico red presente en la misma, la identificación del tipo de tráfico de red, así como tiene los criterios para permitir o negar este flujo de información dependiendo el puerto establecido.

Como bien vimos en el caso anterior los puertos pueden permitir una serie de vulnerabilidades en el sistema y un posible acceso no permitido a la información vulnerable y privada de una entidad, de ahí la importancia que se ha monitoreado por el Firewall.

Esta herramienta también cuenta con los denominados DMZ o también conoció como zona desmilitarizada, en dicha zona se establecen conexiones con redes externas las cuales necesitan hacer contacto con una parte de la red interna, esto se debe a que esta pequeña parte de la red debe ser visible al público, por eso se establece esta zona la cual se tiene debidamente controlada en temas de seguridad y en el caso de que sea vulnerada no comprometa el sistema completo.

Firewall UTM: este dispositivo de red nos ayuda a la gestión unificada de amenazas, este maneja un determinado proveedor para el servicio de seguridad, esto nos genera como ventaja una manera más sencilla al momento de realizar controles y establecer políticas para la gestión y manejo de la red de seguridad.

Este dispositivo es bastante popular en pequeñas y medianas empresas, esto se debe a que este tipo de dispositivos tienen una centralización de funcionalidades establecidas en una sola consola, lo cual ayuda a tener una vista única de todos los elementos que pertenecen a la gestión de seguridad y no discreparía entre uno y otro.

se resalta elementos de seguridad perimetral como los Firewall, permitiendo así establecer políticas de control en los puertos, al igual también nos ofrece IDS e IPS, junto con antivirus. las diferentes herramientas con las que cuenta este dispositivo varía dependiendo la versión que se tenga hay versiones mucho más avanzadas dependiendo de la necesidad de la persona o empresa que lo necesite.

IDS: este sistema de detección de instrucciones, ayuda hacer un seguimiento de la red y de host al igual que la red y el tráfico existente en ella, esto nos ayuda a prevenir posibles amenazas evitar intrusiones en el sistema y de esta manera mantener la integridad de la información y de la red.

IPS: tema que permite la prevención de intrusiones esto mediante la inspección de las terminales y el tráfico presente en la red, permitiéndonos de esta manera detectar y prevenir las posibles amenazas o intrusiones que pongan riesgo la integridad de la información y de la red.

EDR: este software se instala y dispone de los equipos finales, independientemente si son servidores o Host, mediante el uso de esta aplicación se combaten amenazas incidentes de tipo avanzado que se presenten en los puntos finales de la red, este software combina diferentes características presentes en retroalimentación de ataques a nivel mundial, I.A, monitoreo de la red, análisis del comportamiento, respuesta a incidentes, listas blancas de aplicaciones y control de las mismas.

Cómo podemos ver el funcionamiento de este software genera una proactividad en la gestión de la seguridad informática mediante un conjunto de dispositivos, que permiten la mejora en la visibilidad de los procesos y comportamientos presentes en los puntos finales, al igual que la administración de los activos de información y físicos y el apoyo para la adquisición de datos que serán enviados al análisis Ti de dispositivos.

Antivirus: esta herramienta nos permite brindar seguridad a la información, este software realiza la identificación de malware mediante la comparación con bases de datos de virus ya existentes y plenamente identificados, por eso es de vital importancia que estas aplicaciones vivan constantemente actualizadas y establecer un antivirus de acuerdo a las necesidades que se tengan en cuanto a protección, y nunca olvidar que ser debidamente licenciado con el fin de que cuente con todas las herramientas y soportes necesarios, muchas de estas aplicaciones también usan herramientas de protección como los EDR y los IDS.

WAF: si realizamos su traducción textual obtendríamos un firewall de aplicaciones web, el cual tiene como función la protección de páginas web y todo tipo de aplicaciones web, en donde se busca analizar el tráfico de tipo http presente en la misma, se aclara que se analiza tanto el tráfico entrante como el saliente, buscando de esta manera disminuir las vulnerabilidades y amenazas asociadas, estos WAF existente tanto a nivel de software como a nivel de hardware.

Firewall de base de datos: su es específico para la protección de las bases de datos, este firewall busca la restricción en el tráfico y la implementación de políticas más estrictas cuando se solicita acceso a la base de datos, lo cual da como resultado la posibilidad de evitar amenazas y prevenir ataques.

4.15 DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

En cuanto al equipo Blue Team este hace una inspección profunda, frente a las medidas de seguridad implementadas en la infraestructura de red de la empresa, esto quiere decir que el equipo Blue Team trabaja en una defensa de la seguridad de la información basa en los hallazgos del Red Team, esto buscando que se articule de manera proactiva el trabajo del Red Team con el Blue Team y nos

permita obtener unos resultados óptimos teniendo en cuenta varios aspectos de seguridad.

- Seguridad DMZ
  Aislamiento automático de servidores comprometidos
  Contención del atacante.

- Seguridad perimetral
  Políticas de seguridad
  Políticas de Prevención de intrusos (IPS)
  Políticas de WAF para protección de servicios web

- Seguridad de Endpoint
  Integración a herramientas de seguridad para la correlación de eventos.

Es por esto el equipo Blue Team, realiza una vigilancia constante y permanente sobre el sistema y su red y establece las posibles vulnerabilidades, antes de que estas representen una amenaza para el mismo sistema es decir se ha hecho una prevención del riesgo y una mitigación de ataque.

Por otro lado el equipo de respuesta a incidentes informáticos, hace parte como tal de la organización o empresa, su principal uso está en los sectores gubernamentales, militares y públicos, esto se debe a que se busca una mitigación de amenazas a la seguridad informática de esta forma establecemos las siguientes funciones:

- Realizar la alerta sobre las vulnerabilidades detectadas.
- Dar a conocer información acerca de los hallazgos
- Realizar la gestión de los incidentes de seguridad
- Dar a conocer pautas necesarias para la configuración pertinente de las herramientas de seguridad.
- Realizar la gestión de las vulnerabilidades cuando estás están presentes.

4.16 ¿SI DENTRO DE UN EQUIPO BLUETEAM LE INDICAN QUE DEBE TRABAJAR CON CIS “CENTER FOR INTERNET SECURITY” USTED LO UTILIZARÍA PARA QUÉ FIN?

El principal objetivo del CIS es preservar la seguridad de internet, esto mediante el desarrollo de actividades que permiten, identificar, desarrollar, determinar y generar soluciones para los diferentes procesos que se desarrollan en la ciberdefensa, éste cuenta con una variedad de controles y herramientas que permiten la configuración de seguridad en las máquinas o sistemas determinadas, para lograr cumplir con la normatividad vigente establecida.

Podemos definirlo también como un gran Banco con información útil y actualizada de manera constante que puede ser utilizado en los equipos Blue Team, con el fin de aplicar buenas prácticas de configuración al igual que la implementación de procedimientos para asegurar la información, de esta manera el CIS nos da a conocer documentación explicativa para el manejo de herramientas de ciberseguridad y prevención al igual que las aplicaciones para detección de amenazas, y diferentes sistemas operativos, dispositivos de red, software para servidores entre otros servicios presentes en una red organizacional.

en el momento de definir se utilizaría el CIS, me parecería pertinente su implementación debido a las diferentes alianzas que también existen entre empresas de ciberseguridad y las organizaciones con el fin de crear ambientes seguros y debidamente configurados, para evitar y prevenir riesgos existentes y que están en busca de sistemas poco seguros para realizar la explotación, lo cual nos ayudaría en el desarrollo de la evaluación de vulnerabilidades, el monitoreo constante y el análisis de la red de la empresa, todo esto enmarcado en información actualizada de las diferentes vulnerabilidades y riesgos presentes en el mundo.

4.17 FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LO QUE ES UN SIEM.

La definición de SIEM es Security information and event management, en donde encontramos una combinación de 2 conceptos el primero el de Security information management o SIM y Security evento management o SEM, basados en la Unión de estos 2 conceptos anteriormente mencionados el SIEM nos muestra unos plantea una vista completa de lo que es la seguridad informática mediante un software.
Una de las principales características de este tipo de software es que tiene en cuenta los requisitos específicos y características de las empresas donde interviene, siempre teniendo en cuenta cuáles de estos aspectos comprometen la seguridad informática de la organización, al igual realizó una clasificación de cómo y qué prioridad tienen ciertos eventos y como responder por reaccionar frente a estos. Por otro lado, también podemos comprender este concepto como una serie de normas para los diferentes estándares de seguridad existentes y directrices que permiten mantener la calidad de las actividades informática dentro de la organización.

Funciones:

- Agrupa la información sobre amenazas que pueden ser potenciales. Dónde está monitoreo y agrupación de información puede estar dado en tiempo real.

- Te limita cuáles amenazas deben ser solucionadas y cuáles otras son una falsa alarma o no tienen importancia.

- Realiza un escalamiento de temas a los analistas de seguridad encargados, esto se realiza mediante el sistema de alertas el cual permite que se tomen acciones en el menor tiempo posible y de la manera más acertada.

- Realiza la documentación pertinente de manera que la auditoría dar a conocer los eventos que fueron detectados y la solución que se le dieron a los mismos.

- se tiene en cuenta y se cumple la regulación de la industria mediante un formato de reporte sencillo PCI DSS.

Características:

- El SIEM tiene la capacidad de realizar la gestión de la información de seguridad, monitoreo de los eventos que se desarrollan en tiempo real y permite realizar notificaciones y presentar información de seguridad.

- Tiene la capacidad de almacenar los logs de los usuarios, con dicha acción se guarda la información acerca de los usuarios que ingresan a ciertas zonas. es decir que si un usuario entra a una zona no permitida se visualiza su actividad, al igual que si desarrolla un procedimiento normal o si altera las configuraciones, etc., también es de resaltar que se puede almacenar información del atacante, tal como su dirección IP entre otros.

- Realizar notificaciones a la par con el desarrollo del ataque permite a las personas que monitorean el comportamiento de la red estar actualizadas en cuanto a eventos de seguridad y proteger en tiempo real la información de la empresa mitigando los posibles daños.

- su gran capacidad de protección se extiende a todos los activos de la empresa o red, teniendo claro que estos activos hacen parte de las TI.

- Realiza la agrupación de la información y de los eventos ocurridos en la red en un solo lugar, lo que permite la automatizar tareas, mejorar los tiempos de respuesta y ahorrar costos, también presenta un historial de eventos de seguridad.

De esta manera podemos comprender que SIEM nos genera los medios necesarios para realizar la integración de las fuentes de información, las cuales al principio están separadas, pero que mediante su implementación estarán agrupadas y listas para observarse y analizarse en tiempo real y esta manera la respuesta efectiva rápida y acertada a los eventos de seguridad presentes en la organización.

Algo muy interesante de esto también es la capacidad que tiene para gestionar y realizar la presentación de información obtenida en el momento del monitoreo y

durante la prevención mitigación de la amenaza, permitiendo así realizar un registro detallado para la elaboración de la auditoría y presentarlo de manera eficaz a las personas interesadas, y de esta manera tomar decisiones respecto a las acciones pasadas y eventos presentados.

4.18 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS HARDWARE O SOFTWARE.

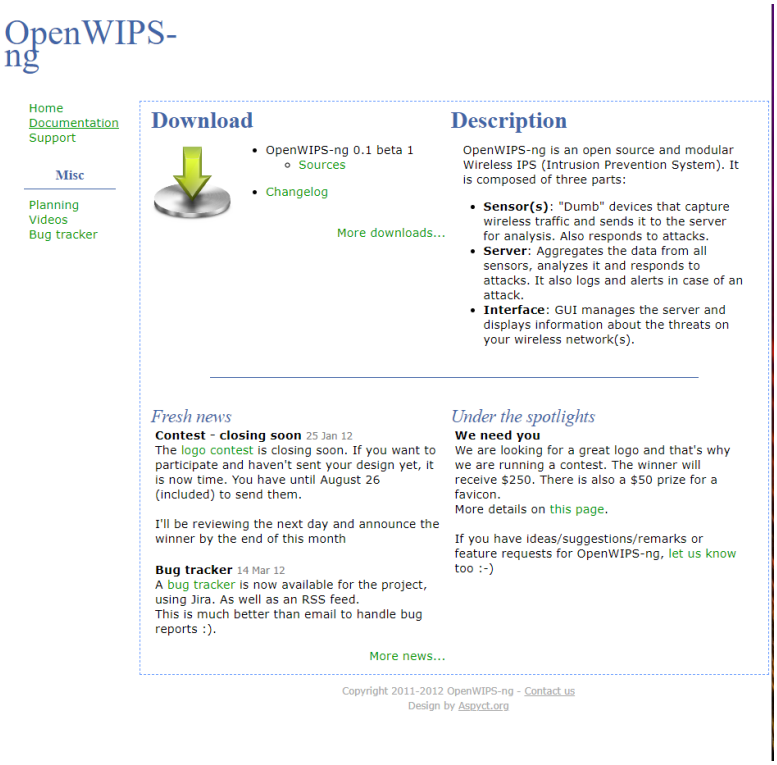
OPEN WIPS-NG: este sistema de detección y prevención de amenazas provenientes, por ataques inalámbricos se basa en 3 componentes:

- Sensores: son los encargados de hacer la respuesta a las amenazas, también monitorean el tráfico y lo guardan para realizar un análisis posterior.

- Servidores: son los encargados de alertar y da respuesta a dichas amenazas, esto lo hacen mediante el análisis de los datos obtenidos por los sensores.

- Interfaces: éste se encarga de presentar la información acerca de los ataques perpetrados a la red inalámbrica y si nos muestra de una manera amigable a los interesados.

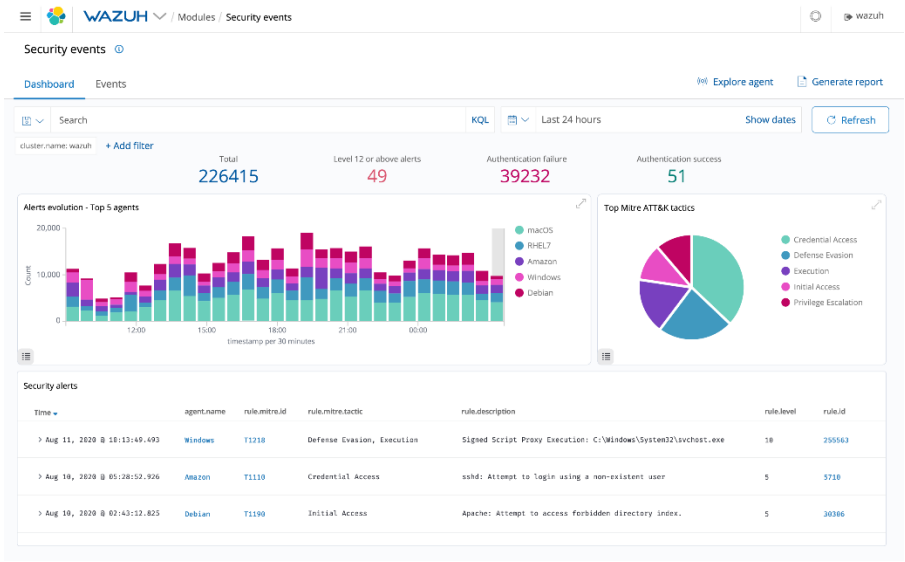
Figura 40. Página principal de OpenWIPS-ng



Fuente 40. OpenWIPS-ng, s.f.

WAZUH EDR: este punto final detección y respuesta, realiza la función de perímetro, donde se procede a establecer una serie de políticas de seguridad, pero estas acciones van un poco más internas en el sistema, para los nuevos sistemas informáticos las políticas de seguridad tienen una gran importancia, pero con redes cada vez más abiertas y sin límites o fronteras, los escenarios de exposición externa a la que se ve sometida a la red, como lo son los VPN, los proveedores de cloud, plantear una serie de retos para los diferentes administradores de seguridad informática y de la información. Donde herramientas como este de tipo EDR, que se enfocan en la respuesta automática basa en el punto de vista de los Endpoint, equipos finales de los usuarios o servidores, toman una gran relevancia.

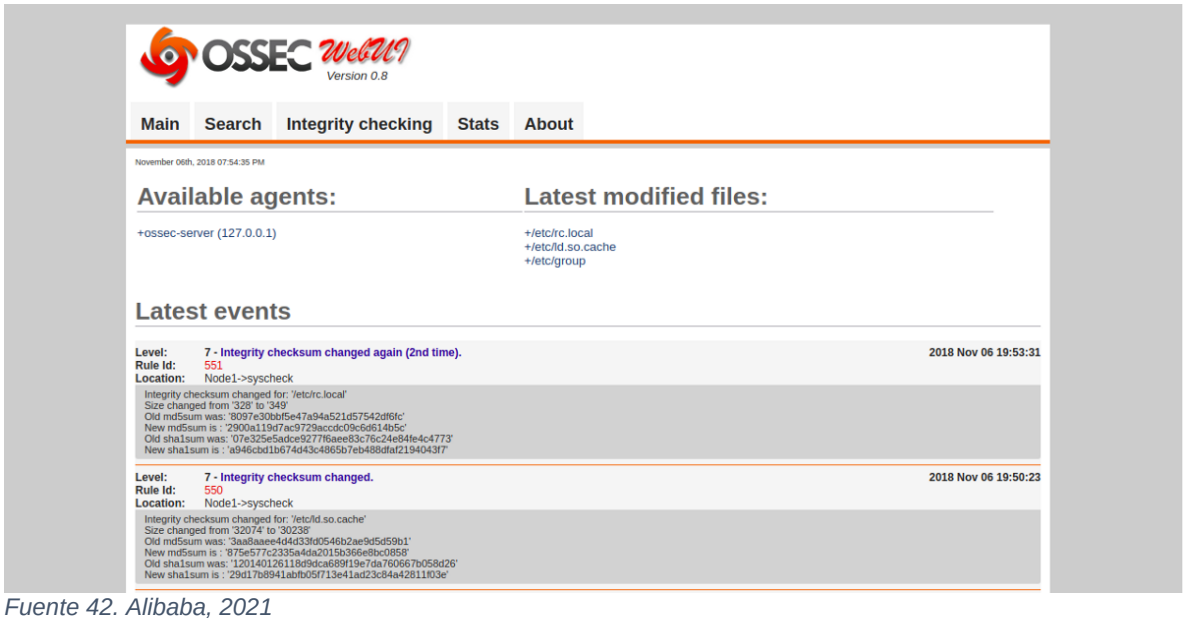
Figura 41. Panel principal Wazuh



Fuente 41. Wazuh, 2021

OSSEC (IDS): esta herramienta es altamente conocida por su popularidad, es de tipo Open Source, esta aplicación tiene consigo una serie de herramientas que permiten relacionar los eventos de seguridad, monitorearlos, realizar el análisis de vulnerabilidades y responder a dichas amenazas de forma automática y en tiempo real.

Figura 42. Panel frontal de OSSEC



Fuente 42. Alibaba, 2021

4.19 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM

Como primer aspecto y uno de vital importancia, se debe tener en cuenta unas adecuadas políticas de seguridad por parte de los administrativos de la organización, dichas políticas deben tener claramente establecido qué objetivo y que alcance se quiere obtener a nivel de ciberseguridad, esto con el fin de tener un plan operativo acorde a las necesidades y posibilidades que brindará la empresa al equipo de seguridad informática y evitar de esta manera posibles conflictos, entre la parte administrativa y el equipo de seguridad.

También es muy importante en base a estas políticas fomentar que el equipo creado para la protección cibernética se ha establecido de manera sólida y con bases claras y articuladas, de las necesidades y metas que se le plantarán al equipo, al igual de qué necesidades y qué materiales van a tener.

El adecuado manejo e implementación del equipo de ciberseguridad debe complementarse con una comunicación asertiva, tanto en el equipo red Team como el equipo Blue Team, en donde tanto al interior de cada equipo como en general la Unión de estos dos equipos, debe ser fuerte y clara en cuanto a sus objetivos y cómo se articulan las actividades del uno con el otro, y de esta manera lograr con su objetivo que es mantener la integridad de los activos de información y comunicaciones de la organización.

Al igual es muy importante mantener un registro constante y seguimiento de los sucesos de seguridad ocurridos desde la creación del Departamento de Seguridad hasta el día en donde se consulte, eso con el fin de proponer análisis y propuestas en base a los resultados de los mismos y mejorar la seguridad en el sistema, al igual de ser necesario ampliar o cambiar el equipo de seguridad. Se tendrá una evidencia consistente de las posibles actividades sospechosas y cómo abordarlas mediante las estrategias propuestas o la proposición de estas en base a las ya anteriormente ejecutadas y que posiblemente no tuvieron éxito.

Tener la proactividad en todo el equipo en cuanto a actualización información del mismo, a nivel de nuevas tecnologías y métodos de ataque, Por otro lado también se debe estar a la vanguardia con la protección y control de incidentes evitando así quedarse por fuera las nuevas tendencias y los nuevos tipos de ataques.

5. METODOLOGÍA

La metodología se desarrolló mediante cinco fases las cuales fueron:

- Fase número uno: se desarrolla la evaluación de las actividades de los equipos red Team y Blue Team, en marco de los criterios éticos y legales, también se realiza el acercamiento algunas herramientas de ciberseguridad de vital importancia para el desarrollo de las actividades de seguridad, finalmente se realiza el montaje del Banco de trabajo a utilizar en las siguientes fases para dar cumplimiento al objetivo planteado.
- Fase número dos: con los conceptos claros en cuanto a aspectos éticos y legales, se aborda de manera más profunda y clara las leyes y decretos que pueden ser vulnerados en el escenario tratado y como un uso acertado y eficiente de la legislación existente en cuanto a ciberseguridad comprende.
- Fase número tres: se ponen en marcha las actividades de un equipo red Team en donde se pretende la búsqueda análisis y explotación de una vulnerabilidad, mostrando así los mecanismos y los alcances de dicha vulnerabilidad y la posible escalación de privilegios, dando a entender lo vulnerable que es el sistema ante dichos ataques
- Fase número cuatro: se ponen en marcha las actividades de un equipo Blue Team, donde se pretende realizar el análisis del ataque desarrollado en la anterior fase y se propone unos métodos de aseguramiento me basado en medidas de Hardenizacion, con el fin de evitar que este tipo de ataques se repita y cómo complementar la seguridad que se tiene actualmente con diferentes mecanismos y herramientas existentes.
- Fase número cinco: como fase final se comprende la presentación de un informe técnico relacionando los aspectos más relevantes en el desarrollo de las anteriores fases y generando un planteamiento en cuanto a recomendaciones y conclusiones que aporten de manera significativa a las estrategias utilizadas por los equipos red Team y Blue Team.

6. RECOMENDACIONES

Al momento de implementar este tipo de estrategias de uso de equipos blue team y red team debemos tener en cuenta varios aspectos, uno de ellos y no menos importante es el factor humano que al igual que el factor tecnológico puede generar una serie de riesgos y vulnerabilidades que pueden comprometer el sistema, de ahí la importancia de contemplar en estas estrategias la concientización y sensibilización al personal acerca de la seguridad informática y la importancia de su aplicación y debido conocimiento en su labor diaria y que tengan debidamente presente los siguientes aspectos:

- Hay que confirmar siempre que los correos recibidos vienen de una fuente confiable, y posterior a ello constatar que el origen sea el deseado para evitar que ésta sea una vulnerabilidad aprovechar por los ciber delincuentes, cabe aclarar que si el origen es desconocido se debe procurar no abrir o utilizar la información contenida en el correo.
- Tener claro cuáles son las redes de navegación segura y cómo identificarlas para que en este caso cada vez que utilicen una red sepan si cumple con los debidos certificados que la hagan confiable y segura para cualquier tipo de actividad que vayan a desarrollar en la red.
- Dado el caso se deban utilizar dispositivos de almacenamiento extraíble, siempre se debe constatar su origen y deben ser analizados previamente por algún software antivirus o antimalware, y procurar pues el uso mínimo de este tipo de dispositivos debido a que el suelo una fuente de riesgo muy grande.

Por otro lado, uno de los factores te bastante importancia en el cual debemos hacer unas recomendaciones muy puntuales es el software:

- Todas las aplicaciones y sistemas operativos deben estar debidamente actualizados, con el fin de evitar tener vulnerabilidades a costa de explotar al igual que prevenir vulnerabilidades de día cero, por tal motivo las actualizaciones se hacen necesarias con el fin de obtener nuevos parches de seguridad evitando que estas vulnerabilidades sean explotables en el sistema.
- Poseer aplicaciones debidamente licenciadas y de origen seguro, esto con el fin de evitar vulnerabilidades por falta de licencias o por versiones incompletas.
- Corroborar que la empresa posea los servicios adecuados de antivirus, antimalware y firewall, y que éstos estén debidamente licenciados y actualizados y en óptimo funcionamiento.

7. CONCLUSIONES

Como expertos en seguridad informática debemos ser personas íntegras en cuanto al desarrollo y uso de nuestro conocimiento, esto se debe a la gran sensibilidad de datos e información que podemos obtener aplicando nuestro conocimiento, al igual de la importancia que tiene los activos de información con los que vamos a tratar, por tal motivo debemos conocer a cabalidad las leyes y decretos que nos rigen en nuestra actividad y que nos dan pautas éticas y Morales para el desempeño de estas.

En la actividad que se desempeña como especialistas en seguridad informática, no es sólo se deben tener conocimientos a nivel técnico sino que es muy importante saberlo expresar de manera formal mediante el uso de la legislación actual, debido a que no sólo basta con encontrar la vulnerabilidad y el culpable, sino que se debe tener en cuenta en que vulneraciones a la legalidad incurrió y cómo proceder para que deje su actuar delictivo, de ahí la importancia de conocer la ley 1273 de 2009, los diferentes decretos es pedidos respecto a seguridad informática y de la información, y el manual COPNIA el cual nos da pautas claras en muchos aspectos de nuestra actividad.

La debida ejecución de situaciones problemas aterrizadas a eventos reales, nos permiten desarrollar habilidades propicias para el desarrollo de la actividad como expertos en seguridad informática, donde tendremos la pericia para actuar frente a diferentes situaciones como las tratadas a lo largo de cada una de las fases de este proyecto, conocer diferentes herramientas y mecanismos para la detección y análisis de incidentes de seguridad, permitirá desempeñar de mejor manera el conocimiento adquirido y aplicarlo al campo laboral.

Es de tener en cuenta que estas actividades que se desarrollan en torno a la seguridad informática, y a las diferentes fases que esta misma comprende, deben estar debidamente documentadas, lo cual permite tanto a la persona que desarrolla el proceso como a los interesados en el tema, tener un conocimiento claro y conciso de que se desarrolló y cómo se hizo, para futuros incidentes tener una base clara de cómo se debe proceder y a qué se debe llegar.

8. BIBLIOGRAFIA

Arias, Michel. Estrategia de superación para la utilización de proxmox y pfsense en las instituciones de salud, Revista cubana de informática médica. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592019000200100#B13

Applebaum, A., Miller, D., Strom, B., Korban, C., & Wolf, R. (2016, December). Intelligent, automated red team emulation. In Proceedings of the 32nd Annual Conference on Computer Security Applications (pp. 363-373). https://ieeexplore.ieee.org/abstract/document/6081410

AS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26) Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Congreso de Colombia. Ley 1273 de 2009. [en línea]. [Consultado 14, junio, 2021]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

COPNIA. (2015). COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity??? Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing Ltd. https://books.google.es/books?hl=es&lr=&id=pyZKDwAAQBAJ&oi=fnd&pg=PP1&dq=+red+team&ots=VsElLTrv35&sig=JOPFdEb_afLizT8pyzxsN2QMGbM#v=onepage&q=red%20team&f=false

Exploit Database. (15 de 10 de 2020). Obtenido de Exploit Database: https://www.exploit-db.com/exploits/42031

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). Recuperado de: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

Heraldo, E. (s.f.). https://www.elheraldo.co/tecnologia/conozca-el-perfil-del-ciberdelincuente 258538

Hiberus. (13 de Mayo de 2016). Consecuencias legales de un ciberataque. Obtenido de: https://www.hiberus.com/legaltech/consecuencias-legales-de-un- ciberataque/

Incibe. (2014). OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. INCIBE-CERT. Recuperado de: https://www.incibe-cert.es/blog/owasp-4

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

Ley estatutaria 1581de octubre de 2012. (01 de Enero de 2014). Obtenido de

http://www.informatica-juridica.com/anexos/ley-estatutaria-1581-de-17-de-octubre-de-2012-por-la-cual-se-dictan-disposiciones-generales-para-la-proteccion-de-los-datos- personales-diario-oficial-48587-de-octubre-18-de-2012/

Ley_1273_2009. (s.f.). https://normograma.mintic.gov.co/mintic/docs/ley_1273_2009.htm

Luna, C. M. (2013). Derecho Usmp-centro de investigación criminológica. El Perfil Criminológico Del Delincuente Informático (pag. 1 – 6), Recuperado de: https://www.usmp.edu.pe/derecho/centro_estudios_criminologia/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf

Mirkovic, J., Reiher, P., Papadopoulos, C., Hussain, A., Shepard, M., Berg, M., & Jung, R. (2008). Testing a collaborative DDoS defense in a red team/blue team exercise. IEEE Transactions on Computers, 57(8), 1098-1112. https://ieeexplore.ieee.org/abstract/document/4479443

MINTIC. (2009). Ley 1273 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

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

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

Por violaciones de datos personales, Superindustria ha impuesto sanciones por más de $21 mil millones de pesos. (s.f.). Obtenido de: https://www.sic.gov.co/noticias/por-violaciones-de-datos-personalesuperindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-de- pesos

Rodríguez, J. C., Muñoz, F. M., & Cuevas, L. M. Perfil psicosociológico en el ciberdelincuente. RICSH Revista Iberoamericana de las Ciencias Sociales y Humanísticas, 8(16), 156-177. [en línea]. [Consultado 14, junio, 2021]. Disponible en: http://ricsh.org.mx/index.php/RICSH/article/view/179/879

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

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

Salellas Luciano. Ensayo sobre Seguridad Informática. [en línea]. [Consultado 14, junio, 2021]. Disponible en: www.sr-hadden-com.ar

What is a red Team. (15 de 10 de 2020). Obtenido de What is a red Team: https://redteams.net/redteaming/2013/what-is-a-red-team

Anexo 1

Link del video: https://www.youtube.com/watch?v=0w80aeXghk4