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

GLORIA YESENIA CAÑÓN ALVARADO

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

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

GLORIA YESENIA CAÑÓN ALVARADO

Proyecto de Grado – Seminario Especializado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

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

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

AMENAZAS: Tipo de incidente con el potencial de perjudicar a un sistema u organización.

BLUE TEAM: También llamado equipo azul, está conformado por un grupo de profesionales especializados en seguridad, que visualizan la organización de adentro hacia afuera. Su función es defender los activos más importantes de un sistema de información de la organización, buscando protegerlos de cualquier tipo de amenaza. Están fielmente conscientes de cuáles son los objetivos y estrategias en cuanto a seguridad refiere la organización. En otras palabras, busca fortalecer los muros de la información para que ningún atacante pueda sobrepasarlos.

RED TEAM: Contrario al equipo azul o blue team, el equipo rojo es un grupo de profesionales, pentesters o hackers éticos especializados en atacar las defensas de un sistema de información de la organización, buscando mejorar la eficiencia, disminuyendo o eliminando las vulnerabilidades encontradas, utilizando estrategias, definiendo el framework o la metodología de pruebas de penetración a implementar, creando un escenario real simulado para poder probar las defensas de la empresa. Deben crearse ataques reales que simulen a los que realizan los delincuentes cibernéticos, teniendo en cuenta que el entorno implementado debe ser controlado.

DATOS: Es la información que dentro de la organización busca ser analizada, cuyo propósito es la medición y control de los procesos que allí se establecen, además de ayudar a la toma de decisiones.

FRAMEWORK: Identificado también como marco e incluye una serie de pasos, prácticas y conceptos que se enfoca en una problema particular, el cual puede ayudar a resolver problemáticas similares.

HACKER ÉTICO: Persona con grandes habilidades y conocimientos en el área de sistemas que enfatiza su labor en detectar fallos y vulnerabilidades en cualquier sistema informático sin pensar en perjudicar al sistema en mención.

HERRAMIENTAS: Programas usados por los hackers para intervenir un sistema informático en busca de fallos o vulnerabilidades.

PENTEST: Se refiere a las pruebas de penetración autorizadas realizadas en un sistema, organización o empresa.

RIESGO: Es la probabilidad e impacto que tiene una amenaza en afectar de manera negativa los objetivos planteados por una organización.

SEGURIDAD: Estrategias, mecanismos, procesos, procedimientos mas todo lo relacionado con mantener la disponibilidad, integridad y confidencialidad de la información.

VULNERABILIDAD: Está relacionado con las debilidades o fallas que poseen los sistemas informáticos.

RESUMEN

Este documento tiene como fin realizar un informe técnico que contenga todas las actividades desarrolladas a lo largo del Seminario especializado, donde se evidencie tanto la parte teórica como la práctica de los aspectos más importantes que desempeñan los equipos Blue Team y Red Team, para con ello tener una visión más amplia de cómo garantizar la seguridad dentro de una organización y la forma de fortalecer la integridad, disponibilidad y confidencialidad de la información.

Se ejecutan cinco etapas, en donde se analiza un caso de estudio y bajo este se crea un banco de trabajo para realizar las diferentes pruebas tanto de Blue Team como de Red Team, resaltando sus aspectos éticos y legales, realizando un análisis de vulnerabilidades, socializando herramientas eficaces para ello, evidenciando técnicas de intrusión, así mismo formulando estrategias que permitan contener un ataque mediante el análisis de riesgos y las vulnerabilidades que se hayan encontrado durante el desarrollo de la práctica.

Por último, socializar las recomendaciones más relevantes y conclusiones de acuerdo con el trabajo realizado, expresando la importancia de ejecutar tareas que son implementadas por los equipos Blue Team y Red Team en la búsqueda del mejoramiento de la seguridad de la información.

Palabras Clave: Hacking ético, Metodología, Herramienta, Riesgo y Vulnerabilidad.

ABSTRACT

The purpose of this document is to produce a technical report that contains all the activities developed throughout the specialized Seminar, where both the theoretical and practical aspects of the most important aspects performed by the Blue Team and Red Team teams are evidenced. have a broader vision of how to ensure security within an organization and how to strengthen the integrity, availability and confidentiality of information.

Five stages are executed, where a case study is analyzed and under this a workbench is created to carry out the different tests of both Blue Team and Red Team, highlighting their ethical and legal aspects, carrying out a vulnerability analysis, socializing effective tools for this, evidencing intrusion techniques, as well as formulating strategies that allow containing an attack by analyzing risks and vulnerabilities that have been found during the development of the practice.

Finally, socialize the most relevant recommendations and conclusions according to the work carried out, expressing the importance of executing tasks that are implemented by the Blue Team and Red Team in the search to improve information security.

Keywords: Ethical Hacking, Methodology, Tool, Risk and Vulnerability.

INTRODUCCIÓN

La información es un recurso intangible de valor absoluto para las empresas y en general para cada uno de los usuarios que utiliza los medios informáticos, a menudo esta información que viaja en internet se ve seriamente comprometida y sometida a vulnerabilidades de tipo destructivos, por tal motivo la seguridad informática es muy importante como soporte y garantía de salvaguardar toda aquella transacción en internet.

De acuerdo con lo anteriormente señalado, se debe partir de buscar estrategias, herramientas, metodologías y todo aquello que contribuya a disminuir esas vulnerabilidades latentes en cualquier sistema de información, enfatizando en la mitigación de riesgos y creando pautas que conlleven a un mejoramiento continuo de la organización, todo lo que conlleve a la disponibilidad, integridad y confidencialidad de los datos, priorizando un beneficio colectivo y proporcionando niveles de seguridad adecuados.

La seguridad de cualquier sistema de información depende tanto de la responsabilidad y buen uso de los usuarios, así como de las organizaciones, por ende, es importante usar las herramientas que estén disponibles para proteger cualquier sistema, aplicado en cualquier contexto, además de capacitar a todo el personal involucrado en la búsqueda, exploración y hallazgo de vulnerabilidades, para que puedan ser mitigadas, a partir de estar siempre un paso delante de un atacante.

Pero para poder llevar a cabo lo anteriormente expuesto es indispensable conocer los equipos de seguridad Blue Team y Red Team que realizan tareas específicas en pro de la búsqueda de dichas vulnerabilidades, su mitigación y la forma de cómo defenderse frente a ataques que pueda recibir un sistema informático. Por tal razón, es importante que por medio del seminario especializado realizado, se evidencien las prácticas desarrolladas para resaltar las labores de los equipos Blue Team y Red Team, relacionando aspectos éticos, legales, así como técnicas y estrategias que permitan cumplir con los objetivos planteados, dando solución a las problemáticas vistas en cada uno de los anexos asociados a un caso de estudio que afecta a la organización WHiteHouse Security.

1 DEFINICIÓN DEL PROBLEMA

Según Quiroz[1], las tecnologías de la información y la comunicación (TIC) son el soporte principal de las organizaciones, puesto que a través de estas se respaldan todas las operaciones y transacciones que garantizan la continuidad del negocio. Implantar nuevas tecnologías y utilizar la informática en las organizaciones, hacen que los procesos fluyan de manera más ágil, eficaz y efectiva, lo que garantiza para cualquier cliente gran satisfacción y la prestación de servicios. Ésta es una razón por la cual la seguridad informática cobra importante relevancia puesto que ayuda a mantener dichos procesos y operaciones asegurados brindando confianza en los componentes que integran la infraestructura de tecnología en cada empresa.

De acuerdo con Voutssas[2], el crecimiento de Internet, la migración a las redes de las operaciones de las organizaciones, así como el aumento de las transacciones comerciales a nivel global gracias el comercio electrónico, creó la necesidad de diseñar sistemas informáticos más seguros ante la posibilidad latente de ataques informáticos que son una amenaza contra la estabilidad de las organizaciones y sus servicios prestados. Para prevenir dichos ataques es fundamental hacer un estudio de vulnerabilidades con el fin de controlarlas, empleando técnicas como el hacking ético, para Ramos[3], los hackers éticos se pueden definir como una red de computadores o personas encargadas de establecer cuáles son las debilidades de un sistema informático, teniendo en cuenta que los ataques en mención son autorizados por las directivas de una organización, con el fin de encontrar las fallas que los atacantes puedan utilizar a su favor.

Para que un hacker ético, pueda cumplir con su función es importante que realice pruebas de penetración[4], las cuáles son autorizadas por los propietarios de los sistemas informáticos, son legales y se usan con el fin de descubrir vulnerabilidades utilizando metodologías y herramientas que lleven al hallazgo de información sensible, vulneración de activos críticos para la organización y accesos no autorizados.

El realizar el hacking ético implica llevar a cabo pruebas que desarrollan los profesionales inmersos en los equipos Red Team, tratando de violar la seguridad de cualquier sistema informático, personas o procesos, desde un punto de vista

[1] QUIROZ, Silva y MACIAS, David. Seguridad en informática: Consideraciones. *Revista Científica Dominio de las Ciencias*. 2017, vol. 3, nro. 5, pp. 676-688. ISSN 2477-8818

[2] VOUTSSAS, Juan. Preservación documental digital y seguridad informática. *Investigación bibliotecológica.* 2010, vol. 24, nro. 50. ISSN 2448-8321

[3] RAMOS, Jorge. Pruebas de Penetración o Pent Test. *Revista de Información, Tecnología y Sociedad.* 2013, nro. 8. ISSN 1997-4044

[4] ALCALDÍA DE BOGOTÁ. [Sitio web]. Bogotá: Guardianes de la Información Penetration Testing

objetivo, para eso es importante conocer las herramientas que se pueden utilizar en esta labor con el fin de tomar las debilidades encontradas y realizar las mejoras correspondientes, identificando y documentando las vulnerabilidades y amenazas. En cuanto a los equipos Blue Team, se busca proteger los activos que son críticos en una organización, crear defensas sólidas ante cualquier ataque, evitar que cualquier intruso pueda infiltrar la organización.

Teniendo en cuenta lo anteriormente expuesto es importante conocer las actividades realizadas por los equipos Red Team y Blue Team, sus técnicas, herramientas y estrategias que se recomiendan para contribuir a que un sistema informático sea más seguro, desde el punto de vista ético y legal.

2 JUSTIFICACIÓN

Como lo afirma Solarte[5], la información es el activo de más valor en la organización, su manejo y control de forma eficiente y eficaz por intermedio de las tecnologías de la información se convierte en una parte fundamental dentro de la organización. Debido a esto se debe dar importancia a la seguridad según la prioridad de los procesos que se llevan a cabo, creando estrategias y convirtiendo las mismas en políticas de seguridad informática para avalar la infraestructura tecnológica y los sistemas de información de las organizaciones.

Las amenazas activas tienen una etapa inicial llamada riesgo que se define como el evento que trata de impedir el alcance de los objetivos en cualquier empresa, pueden generar serias consecuencias, como incluir pérdidas que en informática se interpretaría como un factor negativo que puede acaecer en sucesos inesperados. De acuerdo con Sena[6], un riesgo existe desde que se perciban o manifiesten vulnerabilidades en los activos de información y puede abordar diferentes elementos que lograrían causar un grave impacto en la organización.

Ahora, si bien es cierto, nuevas amenazas surgen cada día, el poder ejecutar acciones con cada uno de los Red Team y Blue Team, ayudará a crear sistemas informáticos más seguros, teniendo en cuenta que al crear un plan de actividades por cada equipo, que ayude a contrarrestar las vulnerabilidades y brechas de seguridad de cualquier organización, activará sus defensas y conducirá a un entorno de riesgo bajo. Se busca generar estrategias con la implementación de metodologías y herramientas que permitan trabajar en función de las vulnerabilidades y debilidades de la empresa[7], así como de las técnicas de ataque más recientes ejecutadas en el mundo real, en un ámbito no sólo regional o nacional, sino también internacional.

Luego de conocer las actividades y herramientas claves utilizadas en los equipos Red Team y Blue Team, realizar las prácticas implementadas en el seminario especializado, profundiza sobre la importancia de todas las labores por cada equipo, se trabaja sobre casos reales, aquellos más relevantes que se puedan encontrar en cualquier organización y se actúa como integrante de cada equipo, llevando ataques dirigidos para encontrar brechas de seguridad, luego se busca estar en el lado de la defensa, que conducirá a solucionar todas las falencias halladas con el desarrollo de la práctica y sugerir recomendaciones eficaces, así

[5] SOLARTE, Francisco; ENRIQUEZ, Edgar y BENAVIDES, Miriam. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL -RTE*. 2015, vol. 28, nro. 5, pp. 492-507.

[6] SENA, Leonardo y TENZER, Simón Mario. Introducción a riesgo informático. Facultad de Ciencias Económicas y de Administración. Universidad de la República de Montevideo. Uruguay, 2004. p.16.

[7] ROA BUENDÍA, José Fabián. Seguridad Informática. España: McGraw-Hill, 2013.

como conclusiones de todo lo que se debe implementar al momento de realizar medias de hardenización.

Con éste documento se pretende generar en la comunidad a quien interese, alertas que permitan priorizar la seguridad de la información, que brinde técnicas seguras y especifique las herramientas mínimas necesarias para mejorar cualquier brecha de seguridad, si bien es cierto, se evitarán bastantes dolores de cabeza, es importante también tener presente que la seguridad es un objetivo en movimiento, cualquier atacante cibernético se adapta al cambio, por tal motivo, es fundamental mantenerse actualizado y llevar a la práctica las recomendaciones sugeridas, con el fin de estar un paso adelante ante cualquier eventualidad que pueda perjudicar a la organización.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Construir informe técnico donde se evidencien todas las actividades realizadas en cada una de las etapas del seminario especializado.

3.2 OBJETIVOS ESPECÍFICOS

Recopilar los aspectos más importantes del desarrollo de la etapa 1 del seminario especializado, fundamentado en conceptos equipos de seguridad.

Socializar las actividades realizadas en la etapa 2 referentes a los aspectos éticos y legales de equipos Red Team y Blue Team.

Compilar el desarrollo de la etapa 3 donde se ejecutan y evidencian pruebas de intrusión.

Evidenciar la solución de la etapa 4 donde se formulan estrategias de contención para evitar ataques informáticos.

4 METODOLOGÍA

El desarrollo de todas las actividades propuestas en el seminario especializado se fundamentan bajo 5 etapas, que mediante el análisis de un caso propuesto busca llevar a la solución de las preguntas orientadoras planteadas, así mismo conocer estrategias que permitan cumplir con las actividades implementadas por los Red Team y Blue Team.

Las 5 etapas definidas fueron las siguientes:

Etapa 1. Conceptos equipos de seguridad, donde se crea el banco de trabajo para desarrollar las prácticas correspondientes en cuanto a análisis de vulnerabilidades, explotación, contención, así como relacionar conceptos importantes de seguridad y las leyes vigentes en Colombia.

Etapa 2. Actuación ética y legal, en la cual se evidencian los aspectos éticos y legales sobre los que debe trabajar cada uno de los equipos Red Team y Blue Team.

Etapa 3. Ejecución pruebas de intrusión, en esta etapa se busca hacer uso del banco de trabajo abordado en la etapa 1, permitiendo realizar un análisis de vulnerabilidades, explotar una de esas debilidades encontradas y documentar el correspondiente ataque.

Etapa 4. Contención de un ataque informático, medidas de hardenización y aspectos importantes relacionados con equipos de respuesta a incidentes informáticos, CIS y SIEM.

Etapa 5. Socialización de informe técnico, donde este se consolida recopilando las anteriores fases y anexando recomendaciones que permitan endurecer por medio de estrategias todos los aspectos de seguridad dentro de una organización, así como conclusiones basadas desde la perspectiva de ciberseguridad que permitan construir conocimiento.

5 DESARROLLO DEL INFORME TÉCNICO

5.1 ETAPA 1 CONCEPTOS EQUIPOS DE SEGURIDAD

5.1.1 **Legislación sobre protección de datos personales y delitos informáticos**.

A continuación, se relacionan las leyes y decretos colombianos vigentes sobre delitos informáticos y la protección de datos personales:

5.1.1.1 Ley 1273 de 2009. Establecida el 5 de enero de 2009, llamada "de la protección de la información y de los datos"[8], donde ya se empiezan a tipificar los delitos informáticos en Colombia. Cuenta con 2 capítulos, el capítulo 1 habla acerca de los atentados contra la confidencialidad, la integridad y la disponibilidad de datos, así como de todos los sistemas informáticos, se compone de 8 artículos que van desde 269A hasta el 269H, y se adicionan al artículo 1 del código penal.

El capítulo 1 se enfoca en penalizar la interceptación de información, acceder abusivamente a cualquier sistema informático, daño físico, digital, alteración, sustracción, venta, distribución de información, violación de datos personales y uso de software malicioso para interceptación de datos que puedan poner en riesgo el interior de un sistema informático. La situación es más grave y aumenta la pena si los delitos anteriores se realizan en sistemas informáticos oficiales o estatales, si los ejecuta cualquier servidor público ejerciendo su labor, aprovechando la confianza de cualquier persona con vinculo contractual, con la intención de perjudicar a otra persona, con fines terroristas o poniendo en riesgo la seguridad nacional, entre otros. Los delitos relacionados en este capítulo tienen una penalización de mínimo 36 meses y máximo 96 meses de cárcel dependiendo la categoría incurrida y multas entre 100 y 1000 salarios mínimos legales mensuales vigentes.

El capítulo 2 habla acerca de los atentados informáticos y otro tipo de infracciones, se compone de los artículos del 2 al 4 que son adiciones al código penal y 269I y 269J. Este capítulo se enfoca la violación y hurto de un sistema informático suplantando las credenciales con fines lucrativos con afectaciones de una organización o persona, este tipo de delitos incurrirá en prisión de 48 a 120 meses y multas de entre 200 a 1500 salarios mínimos legales mensuales vigentes.

[8] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). De la protección de la información y de los datos. En: Diario Oficial. Enero, 2009. Nro. 47223.

5.1.1.2 Ley 1581 de 2012. Esta ley resalta todo lo relacionado con la protección de datos personales[9], el derecho que tienen las personas a rectificar la información hallada en bases de datos, así como conocerla y actualizarla si es el caso, la importancia del manejo de datos sensibles, responsables del tratamiento de la información, las condiciones legales para el tratamiento de los datos, los derechos como ciudadanos frente a cada situación, así mismo se aclara que el tratamiento de las bases de datos pueden ser requeridas tanto por entidades públicas como privadas.

5.1.1.3 Decreto 1377 de 2013. Con este decreto la ley 1581 de 2012 se reglamenta parcialmente, constituyéndose en Colombia como el marco general para la protección de los datos personales, se socializa mediante seis capítulos las disposiciones generales, la autorización a quien es responsable del tratamiento de los datos, sus políticas, el ejercicio de los derechos de los titulares, la transmisión y transferencia internacional de los datos personales, las políticas efectivas internas que demuestran la responsabilidad frente al tratamiento de los datos personales.

5.1.1.4 Ley 599 de 2000. Del código penal[10], incorpora las sanciones por la interceptación y violación de comunicaciones, por ejemplo, el artículo 192 tipifica las penas que van desde los 16 hasta los 72 meses de prisión por violación ilícita de las comunicaciones, desde la sustracción ilícita, el ocultamiento, la destrucción, el extravío, la interceptación, impedir o controlar la comunicación privada que vaya hacia otra persona, aunque no especifica directamente sobre el delito informático si hace alusión de cualquier tipo de comunicación, en el artículo 197 especifica las sanciones por utilizar redes de comunicaciones ilícitamente, aclara que puede ser cualquier tipo de medio electrónico e incluye penas de 4 a 8 años de prisión. En el artículo 199 se especifica la pena por sabotaje en donde se resalta que, si con el ánimo de paralizar el trabajo desaparezca, destruya o dañe algún equipo, soporte lógico, base de datos, instalaciones, herramientas, entre otros, puede ir a prisión por mínimo 16 meses o hasta 108 meses además de pagar una multa.

[9] COLOMBIA. SENADO DE LA REPÚBLICA. Ley estatutaria 1581 de 2012. (17, octubre, 2012). Disposiciones generales para la protección de datos personales. En: Diario Oficial. Octubre, 2012. Nro. 48587.

[10] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 599 de 2000. (24, julio, 2000). De las Normas Rectoras de la Ley Penal en Colombia. En: Diario Oficial. Julio, 2000. Nro. 44097.

5.1.1.5 LEY 1928 DE 2018. Convenio sobre la ciberdelincuencia, es el primer tratado internacional cuyo propósito es proteger a la sociedad en general frente a cualquier tipo de delito informático, creando leyes pertinentes, trabajando en conjunto con entes internacionales y teniendo en cuenta óptimas técnicas de investigación. Enfatizan en el riesgo a las que están expuestas las redes informáticas, así como toda la información que se maneja de forma electrónica y que puede ser utilizada para cometer actos delictivos, como es el caso del problema en estudio[11].

5.1.2 **Etapas del pentesting y Herramientas a utilizar**

El Pentesting hace referencia a realizar detecciones minuciosas con técnicas empleadas por hackers éticos (especialistas contratados por las empresas para realizar ataques controlados a cualquier sistema informático o de información y el cual no busca perjudicar a las organizaciones, ni sus objetivos son criminales). El objetivo del pentest es buscar fragilidades y potenciales vulnerabilidades en la estructura de la red y todo el sistema informático, así como usar algunas herramientas específicas para realizar intrusiones que den señales sobre cuáles datos o información de la organización pueden ser hurtados por los atacantes, con el fin de reparar sus problemas de seguridad. Dentro del pentesting se encuentran las siguientes etapas[12]:

5.1.2.1 Recopilación de Información. En esta etapa de reconocimiento se recopila toda la información que sea posible sobre el objetivo, es una etapa fundamental, puesto que al ser el comienzo del pentesting se busca encontrar la mayor cantidad de vulnerabilidades de acuerdo con lo recopilado, puede optar por buscar información en fuentes públicas para darle veracidad a lo que realmente está expuesto frente a desconocidos, en redes sociales o empezar a hacer un reconocimiento de la red, verificando si existen puertos abiertos, averiguar sistemas operativos, entre otros. Herramienta a utilizar: Nmap es una herramienta eficaz para poder utilizarla en esta etapa de recolección de información, más adelante se explica en profundidad su función y lo que representa.

[11] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1928 de 2018. (24, julio, 2018). Convenio sobre la Ciberdelincuencia adoptado el 23 de noviembre de 2001 en Budapest. En: Diario Oficial. Julio, 2018. Nro. 50664.

[12] PILLAY, Rishalin. *Learn Penetration Testing: Understand the art of penetration testing and develop your white hat hacker skills*. Packt Publishing Ltd, 2019.

5.1.2.2 Búsqueda de Vulnerabilidades. Luego de recopilar toda la información necesaria, se procede a hallar las vulnerabilidades, encontrar aquellas brechas de seguridad del objetivo que se está estudiando, todo esto con el fin de explotarlas. Se pueden buscar herramientas eficaces que ayuden a encontrar la mayor cantidad de vulnerabilidades posibles.

Herramienta a utilizar: Openvas sería útil para realizar un escaneo de vulnerabilidades, más adelante se profundiza un poco más en ésta herramienta. Nessus también podría servir de mucha ayuda puesto que se considera como un estándar de la industria con soluciones de evaluación de vulnerabilidades puesto que ayuda a identificarlas, evidenciando parches faltantes, configuraciones erróneas, fallas de software, malware y lo mejor es que puede ser utilizado en diferentes aplicaciones, sistemas operativos y dispositivos. Tiene una licencia que se puede pagar para adquirir todas las funciones de esta herramienta en su totalidad. La larga lista de pluggins que maneja así como las pruebas de vulnerabilidad son escritas en lenguaje de Scripting de ataque de Nessus.

5.1.2.3 Explotación. Luego de haber hallado todas las vulnerabilidades posibles, es importante explotarlas, como su mismo nombre lo indica se pueden utilizar exploits de tipos cliente, locales o remotos. En esta fase puede hacerse uso de fuerza bruta o utilizar distintas herramientas que ayudarán con el objetivo principal, sacar provecho de todas las falencias encontradas. Herramienta a utilizar: Para esta fase se puede utilizar Metasploit, del cual se da un concepto más profundo en el ítem 4.

5.1.2.4 Post Explotación. Se busca en esta fase causar un gran impacto en el objetivo de acuerdo con las vulnerabilidades explotadas, para ello el punto clave es poder realizar una escalada de privilegios, acceder a información crítica, se busca actuar como una amenaza persistente avanzada, con el fin de descubrir brechas de seguridad, no solo en sistemas internos, sino que abarque seguridad perimetral, esto ayudará a detectar cualquier tipo de actividad sospechosa en la red. Herramienta a utilizar: CAIN, su licencia es de software libre y sirve como herramienta para recuperar contraseñas teniendo en cuenta diferentes métodos como criptoanálisis, diccionario de datos o fuerza bruta, cabe resaltar su crakeo web, calculadora de hashes, ARP spoofing y aceleración de captura de paquetes. También se puede encontrar como Cain y Abel.

5.1.2.5 Reporte o Informe de Resultados. Se genera un consolidado donde se especifique todas las vulnerabilidades y falencias halladas, se anexan imágenes o capturas de pantalla donde se evidencia todo el proceso realizado en las fases anteriores, aquí también deben ir todas las soluciones a los problemas hallados con el fin de que se eviten riesgos futuros y todas las vulnerabilidades queden resueltas o por lo menos en un nivel crítico bajo.

Herramienta a utilizar: Kali Linux, su distribución se basa en Debian, este sistema operativo tiene su principal enfoque en la auditoría y seguridad informática en general, tiene preinstaladas muchas herramientas que pueden realizar diferentes tipos de actividades, por ejemplo, crakeo de contraseñas, escaneo de puertos, pruebas de seguridad inalámbrica, sniffer, ingeniería inversa, forense, entre muchas otras más. El tipo de licencia que maneja es GPL, está financiado, desarrollado y mantenido por Offensive Security, esta organización es líder en capacitaciones en seguridad informática. Es importante resaltar las siguientes características: gratuito y libre, con más de 600 herramientas para pruebas de penetración, los dispositivos inalámbricos que soporta son de gran alcance, se fija al estándar de jerarquía del sistema de archivos, contiene un árbol de desarrollo cuyo código es abierto.[13]

5.1.3 **Herramientas de Ciberseguridad y servicios en línea**

5.1.3.1 Metasploit. Es un framework que permite crear y ejecutar exploits contra máquinas remotas de código abierto, ayuda en tests de penetración y en el desarrollo de firmas para IDS (Sistemas de detección de intrusos) inicialmente fue creado en lenguaje Perl y luego fue reescrito en Ruby, existe versión gratuita y premium, la gratuita tiene soporte de la comunidad y la premium que es llamada Metasploit pro es soportada por Rapid7.

Algunos subproyectos importantes de metasploit son las bases de datos de opcodes (códigos de operación) y archivos de shellcodes. Con este framework se pueden crear nuevos exploits o utilizar varios ya establecidos, con lo que se puede explotar vulnerabilidades, se puede integrar con otras herramientas como Nmap y existe también ya preinstalada en Kali Linux.

[13] KALI.ORG. [Sitio Web]. The Most Advanced Penetration Testing Distribution. [Consulta: 30 de agosto de 2021]. Disponible en: https://www.kali.org/

5.1.3.2 NMAP. Herramienta muy práctica que permite verificar puertos abiertos, cerrados y con ello se puede identificar las aplicaciones que la organización está utilizando, entre otros aspectos relevantes, con esta herramienta se pude inicial con la búsqueda de vulnerabilidades importantes que puede afectar a la organización. Muy utilizada para la fase de recopilación de información.

Es multiplataforma y de código abierto, su licencia es GNU y se puede utilizar para una auditoría de seguridad y descubrimiento de redes, servicios o servidores. La forma en que trabaja es que envía paquetes definidos hacia diferentes destinos en otros equipos y de acuerdo con su respuesta los analiza, cubre varias funciones que son extensibles utilizando scripts para proporcionar servicios de detección avanzados, detectar vulnerabilidades y variedad de aplicaciones. Cuando se ejecuta su escaneo tiene la facilidad de adaptarse a condiciones de latencia y congestión de la red. Dentro de sus funciones también se encuentra analizar los filtros del firewall y sus principales características son su portabilidad, flexibilidad, soporte brindado por una comunidad activa y maneja tanto una buena como amplia documentación[14].

5.1.3.3 OPENVAS. Con esta herramienta se puede escanear un equipo local o remoto en busca de vulnerabilidades y de acuerdo con los resultados se generan las posibles remediaciones, su base de datos de vulnerabilidades se actualiza diariamente, además de contar con una base de datos que contiene más de 50.000 de ellas. Esta herramienta es muy completa en cuanto a escaneo de vulnerabilidades, puesto que si se realizan pruebas a gran escala serán optimizadas, en sus aspectos más importantes cabe destacar que se pueden realizar pruebas autenticadas, así como no autenticadas, tiene su propio lenguaje con el que se puede implementar diferentes tipos de pruebas de vulnerabilidad. El tipo de licenciamiento que maneja es GNU GPL[15].

5.1.3.4 EXPLOIT DB. La base de datos de Exploit es una herramienta muy eficaz donde se recopilan todos los exploits que se pueden utilizar para explotar falencias o vulnerabilidades, esta base de datos es alimentada por expertos en hackeo, que además de explicar como se puede sacar provecho de las vulnerabilidades, dan instrucciones muy precisas de cómo hacerlo.

[14] LÓPEZ ARBOLEDA, Claudia, et al. Capacidades técnicas, legales y de gestión para equipos blue team y red team. [en línea]. Seminario Especializado. UNAD, 2021. [en línea]. Seminario Especializado. UNAD, 2021. p. 16

[15] OPENVAS.ORG. [Sitio Web]. OpenVAS - Open Vulnerability Assessment Scanner. [Consulta: 31 de agosto de 2021]. Disponible en: https://www.openvas.org/

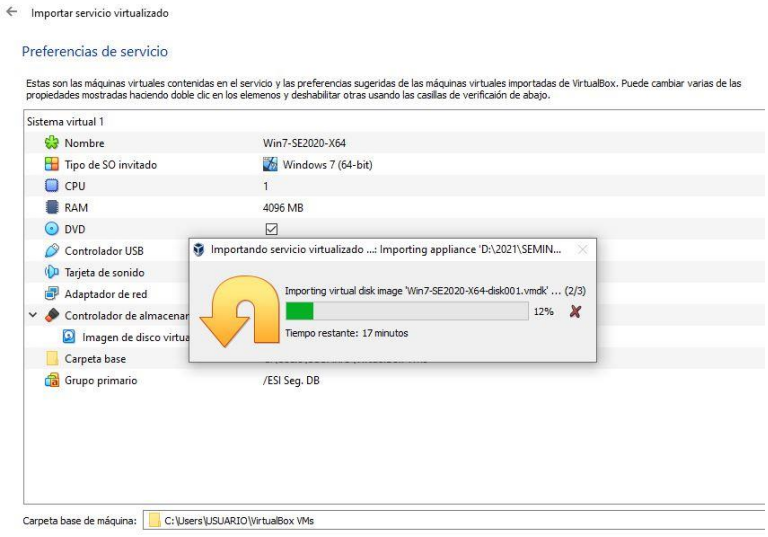
5.1.3.5 CVE. Es un estándar de nomenclatura de vulnerabilidades, encargado de reunir todas las fallas de seguridad halladas en un sistema informático, brindando prioridad y buscando solucionarlos en el menor tiempo posible, organiza las fallas de forma estándar y se almacenan con el fin de brindarle a las organizaciones y a quien interese una guía, así poder encontrar la información de manera rápida. Asigna a cada vulnerabilidad un número de identificación, junto con su descripción, la clasifica en una escala del 0 al 10

5.1.4 **Banco de trabajo**

Se procede a instalar las máquinas virtuales necesarias para realizar las prácticas correspondientes de acuerdo con lo solicitado en cada etapa.

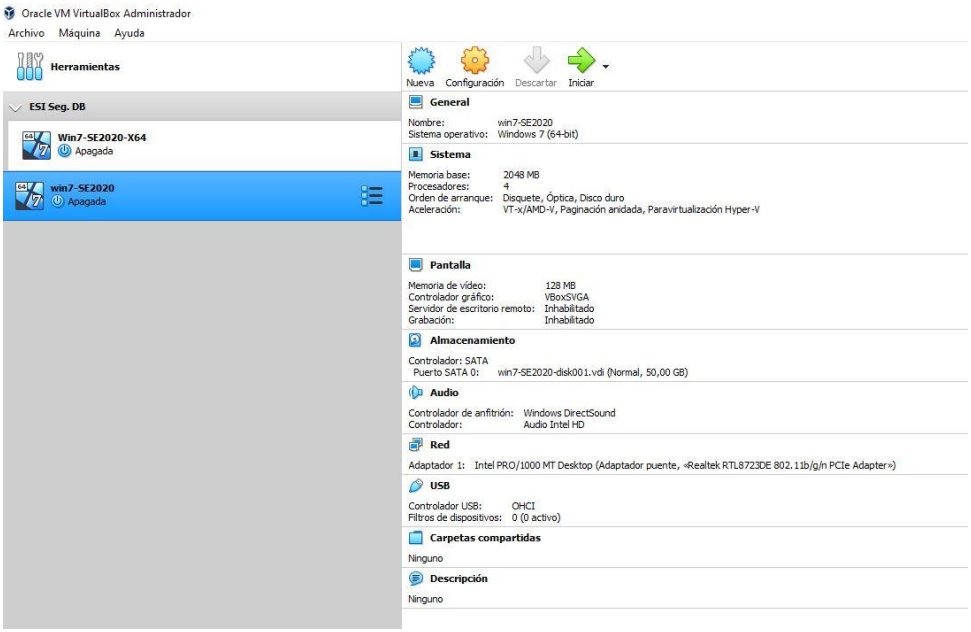
Se importan las OVAS correspondientes:

Figura 1. Windows 7 X64



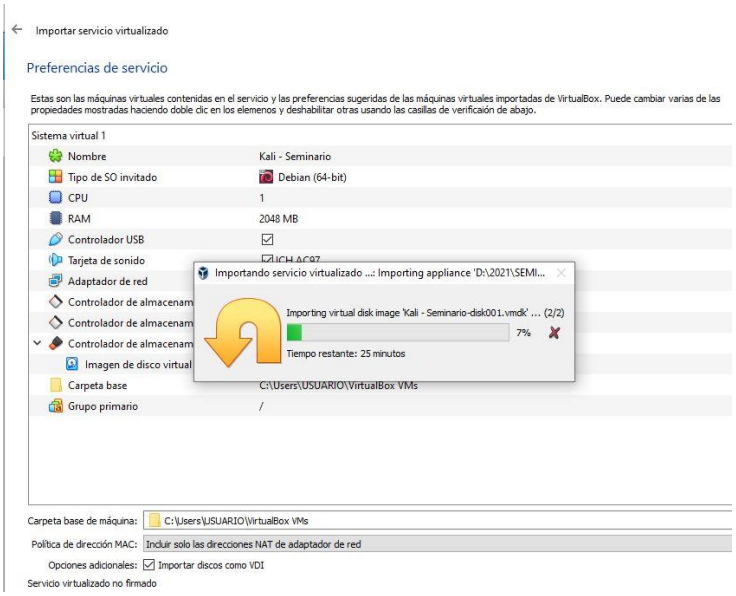
Fuente: Propia

Figura 2. Windows 7 X86



Fuente: Propia

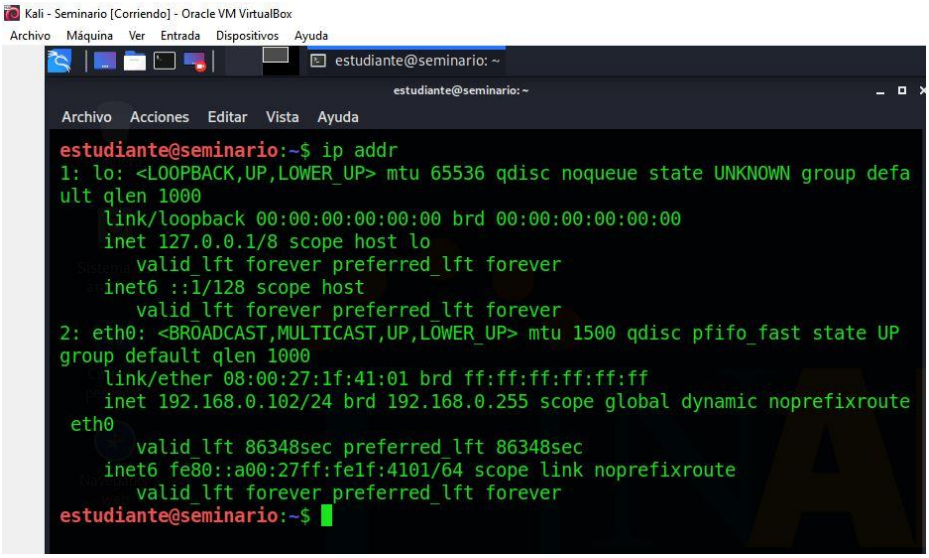
Figura 3. Kali



Fuente: Propia

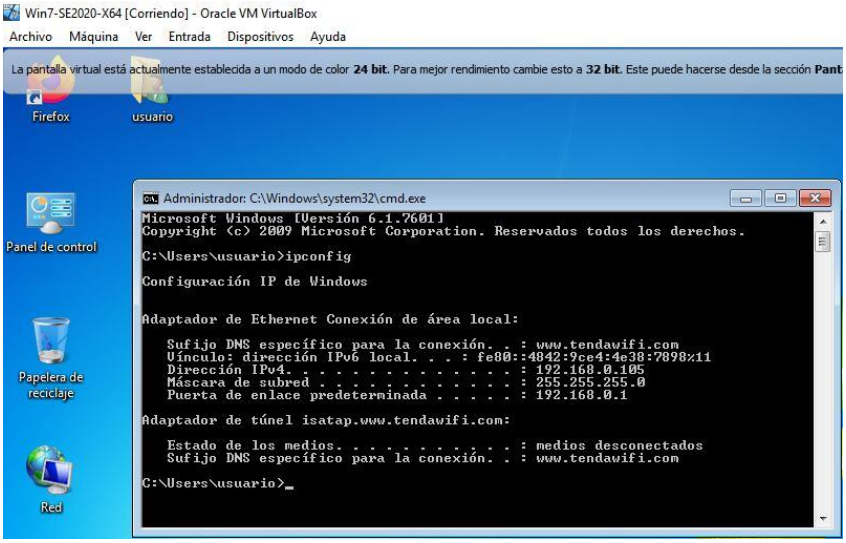
Al encender las máquinas procedo a hallar las direcciones IP de cada una para evidenciar la comunicación.

Figura 4. Dirección IP Kali Linux 192.168.0.102



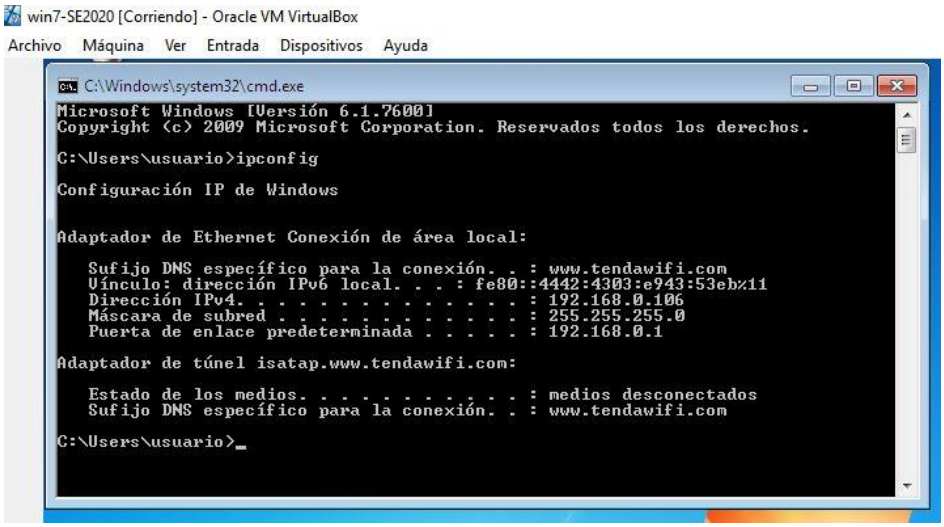
Fuente: Propia

Figura 5. Dirección IP Windows 7 X64 192.168.0.105



Fuente: Propia

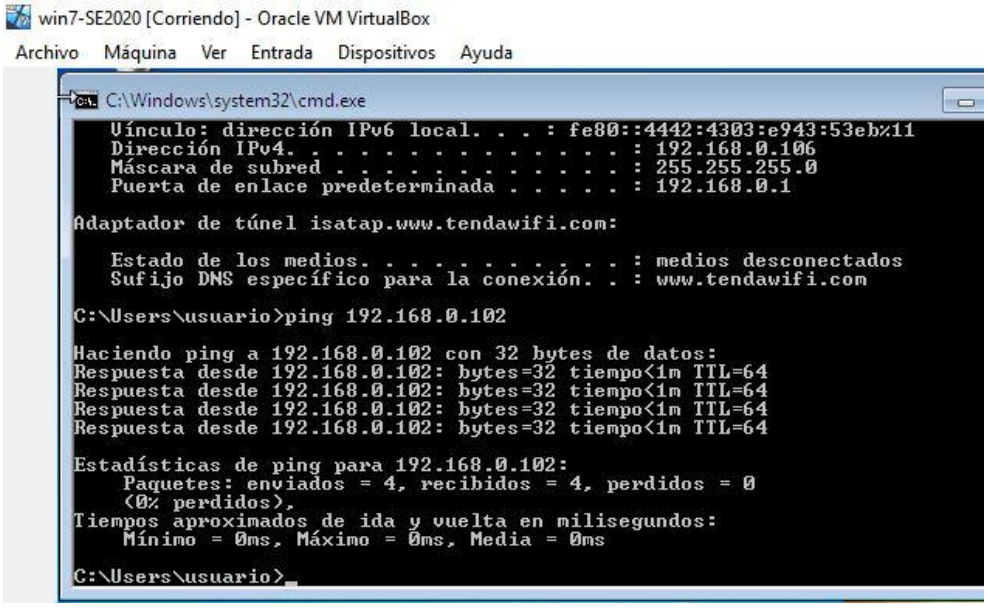
Figura 6. Dirección IP Windows 7 X86 192.168.0.106



Fuente: Propia

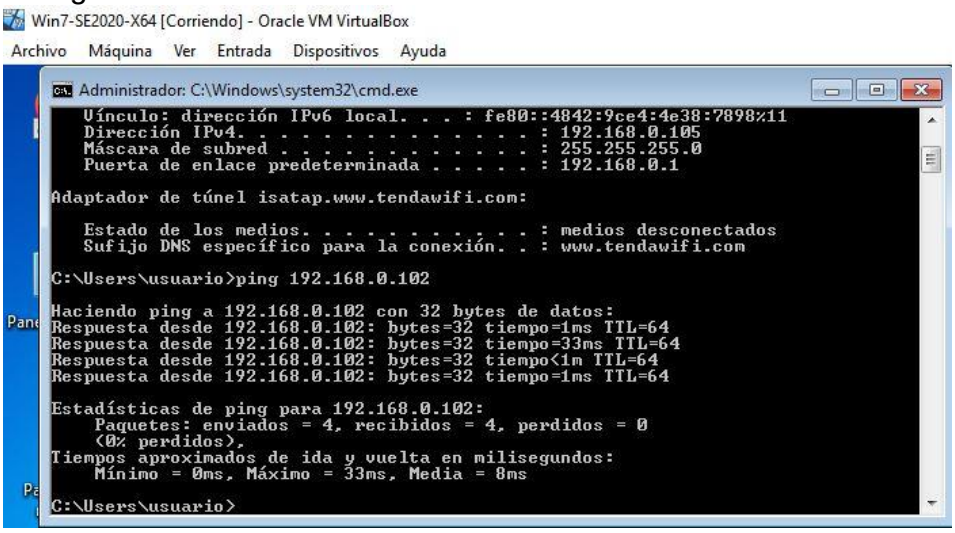
Luego de conocer las direcciones IP se procede a hacer ping entre máquinas para verificar conexión:

Figura 7. Ping de Windows 7 X86 a Kali Linux



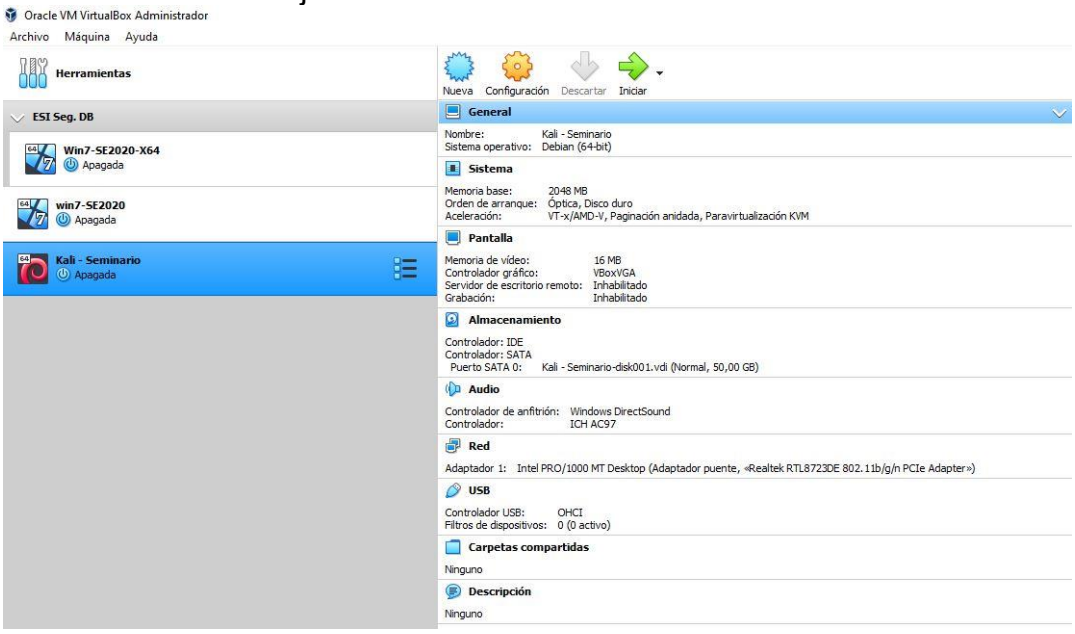
Fuente: Propia

Figura 8. Ping de Windows 7 X64 a Kali Linux



Fuente: Propia

Figura 9. Banco de trabajo final



Fuente: Propia

5.2 ACTIVIDADES REALIZADAS EN LA ETAPA 2 REFERENTES A LOS ASPECTOS ÉTICOS Y LEGALES DE EQUIPOS RED TEAM Y BLUE TEAM

5.2.1 Aspectos ilegales del contrato y del acuerdo.

De acuerdo con el **Anexo 2**[16] es irresponsable y falta de ética, entregar a unos terceros que se van a catalogar como los integrantes de los equipos Red Team y Blue Team, un contrato que fue realizado por una persona que ya no trabaja en la organización, sin previa revisión de la alta gerencia y al cual no se le hicieron modificaciones, con esto se evidencia que no hacen una elección del personal profunda y exhaustiva, pues son quienes van a estar a cargo de información confidencial e importante de personas y compañías que contratan servicios de la organización WhiteHouse Security.

También es evidente que, si la persona que hizo los contratos fue despedida por actividades ilícitas, es menos alguien en quien confiar, así que con mayor razón, los contratos debieron haberse revisado y modificado, antes de entregarlos a unos terceros y pedir sólo tener cuidado a la hora de firmar.

El **Anexo 3** está relacionado con el Acuerdo de Confidencialidad, el cual es muy importante para definir parámetros fundamentales entre la organización WhiteHouse y el personal a contratar, donde se establezca su responsabilidad en cuanto al manejo de la información suministrada, para el desarrollo de sus actividades, con el fin de que no vaya a ser expuesta o divulgada por ningún integrante.

Haciendo un análisis de las cláusulas, se logra identificar algunos fragmentos que dejan en evidencia a la organización, de su forma de actuar poco ética y legal, de los cuáles se resaltan a continuación:

- "**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**."[17]

[16] Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. [Sitio Web]. Anexo 2 – Escenario 2. UNAD. [Consulta: 9 de septiembre de 2021]. Disponible en: https://campus109.unad.edu.co/ecbti95/pluginfile.php/680/mod_folder/content/0/Anexo%202%20-%20Escenario%202.pdf?forcedownload=1

[17] Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. [Sitio Web]. Anexo 3 – Acuerdo. UNAD. [Consulta: 9 de septiembre de 2021]. Disponible en:

Análisis: De acuerdo con lo resaltado anteriormente se puede inferir que la organización realiza procesos ilegales y que mediante una cláusula que consideran legal por estar estipulada, las personas contratadas no puedan revelar los actos que allí se evidencien de manera irregular, que tampoco puedan hacerlo frente a autoridades legales, con esto no da confiabilidad el actuar de la empresa y ya da una mala impresión, no sólo a nivel general sino también de sus empleados. Quien firme esta cláusula ya está incurriendo en falta de ética por estar dispuesto a firmar el acuerdo, pues está afirmando el permitir ocultar información que avale procesos ilegales dentro de una organización.

- "**Segunda. Ítem 2:** Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "**datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos**".[18]

Análisis: Con la parte resaltada de la anterior cláusula se evidencia la manera ilegal y falta de ética de actuar de la organización para conseguir información, vulneran las fuentes de investigación, interceptan llamadas de forma ilegal, infringen las leyes colombianas, se siguen ocultando detrás de las cláusulas para manejarlo como si fuera legal, la persona que firme con esta cláusula tampoco actuaría de forma ética.

- "**Cuarta. Ítem 3**: No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."[19]

Análisis: Aunque se esté estableciendo una obligación laboral, con el punto anterior se obliga al profesional a no denunciar este tipo de actividades, pero, aunque la organización es reconocida a nivel mundial, su actuar no prima por encima de las leyes del país, de esta manera se está convirtiendo en cómplice el profesional quien firme el acuerdo, cualquier actividad ilegal debe ser denunciada.

- "**Cuarta. Ítem 4:** Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas."[20]

---

https://campus109.unad.edu.co/ecbti95/pluginfile.php/680/mod_folder/content/0/Anexo%203%20-%20Acuerdo.pdf?forcedownload=1

[18] Anexo 3 - Acuerdo Óp. Cit., p. 3.

[19] Anexo 3 - Acuerdo Óp. Cit., p. 4.

[20] Anexo 3 - Acuerdo Óp. Cit., p. 4.

Análisis: Así como en el ítem 3, se está prohibiendo el denunciar sobre actividades ilegales, al cumplir con ello, el profesional que firme el acuerdo se convertirá en cómplice de la organización, si se evidencian este tipo de actividades.

- "**Cuarta. Ítem 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."[21]

Análisis: Con ésta ítem de la cláusula 4 se le está dejando toda la responsabilidad al profesional que firme el acuerdo, de todas las falencias que se encuentren al momento de hacer un allanamiento, es decir, que, si se hayan actividades ilícitas, la empresa se salva de cualquier culpabilidad, dejando como responsable al receptor, esto no es para nada ético, teniendo en cuenta que en cláusulas anteriores se infiere que la información confidencial es considerada como propiedad de WhiteHouse Security.

- **"Quinta. Obligaciones de la parte reveladora:** Son obligaciones de la parte reveladora: 1. Mantener la reserva de la **información confidencial** hasta tanto"[22]

Análisis: Esta cláusula está inconclusa, es decir, pueden la organización si lo desea agregar otras cosas a su beneficio, luego de que el profesional haya firmado y sin tener conocimiento al respecto, no se tiene en esta cláusula argumentos realmente concluyentes.

- **"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."[23]

Análisis: Con esta cláusula la organización WhiteHouse Security busca librarse de cualquier perjuicio que le pueda ocasionar el realizar actividades ilegales, porque con todo lo estipulado en el acuerdo se evidencia que no actúa de forma ética ni legal, de esta manera, toda responsabilidad recaería en el receptor, el profesional que firme el acuerdo, cualquier proceso judicial dejaría exenta a la organización y recaería en el receptor, terminando en un proceso que lo podría hasta privar de la libertad.

[21] Anexo 3 - Acuerdo Óp. Cit., p. 4.
[22] Anexo 3 - Acuerdo Óp. Cit., p. 5.
[23] Anexo 3 - Acuerdo Óp. Cit., p. 5.

Con todo lo anteriormente visto, es importante que el profesional candidato a ser contratado, haga un análisis de si realmente vale la pena dejar a un lado su parte ética, para ser cómplice de actividades ilegales y que por supuesto no afectaría en primera instancia a la organización sino a la persona, la cuál podría tener desde suspensión de su tarjeta profesional, como incurrir en multas o terminar en prisión, es decir, no vale la pena arriesgar tanto por tan poco, puesto que ningún dinero puede comprar la ética, la moral y menos por terminar en procesos fuera de la ley.

5.2.2 **Análisis de los Anexos según la Ley 1273.**

Es evidente que existe una explotación laboral por parte de la organización, debido a que en Colombia antes de realizarse cualquier tipo de contrato debe especificarse las responsabilidades contractuales, así como las extracontractuales, puesto que como se verifica tanto en el anexo 2 como 3, toda la responsabilidad está recayendo en el profesional candidato al cargo. Ahora teniendo en cuenta los artículos que son vulnerados en la ley en mención, a continuación se especifican:

- **Cláusula Primera. Objeto**: Para esta cláusula los artículos que se vulneran de acuerdo con la ley 1273 son:

Art. 269F. Relacionado con la violación de datos personales, con el acuerdo de confidencialidad la organización se cuida en salud y así proceder a violar datos personales, así mismo obliga a el receptor a que se oculte información ilegal o procesos del mismo tipo.

Art. 269H. En el numeral 3 se indica sobre aprovecharse de la confianza de quien tiene la información o si se tiene un vínculo contractual, numeral 7 que trata sobre utilizar a un tercero de buena fe como instrumento, puesto que la organización, abusa de la confianza del receptor para impedirle que denuncie actividades ilícitas.

- **Cláusula Segunda. Definición de información confidencial**: se incumplen los siguientes artículos:

Art. 269A. Trata sobre el acceso abusivo a un sistema informático, lo cual con la cláusula correspondiente evidencia que la información se obtiene de forma ilegal, por esto se incurriría en una pena desde 48 a 96 meses y podría ocasionar una multa de hasta 1000 salarios mínimos legales mensuales vigentes.[24]

[24] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). De la protección de la información y de los datos. En: Diario Oficial. Enero, 2009. Nro. 47223. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Art. 269C y Art. 269H. Hacen alusión a la interceptación de datos informáticos, que se evidencia en la organización se hace sin una orden judicial, así mismo esto se penaliza si se hace sobre sistemas de comunicaciones o informáticos, en la cláusula del acuerdo se enfatiza sobre chuzadas, accesos abusivos a sistemas informáticos.

- **Cláusula Cuarta. Obligaciones de la parte receptora:** En los ítems 3, 4, 8 y 9, se estarían violando los siguientes artículos:

269A, 269C, 269F en ellos se relaciona el acceso abusivo y espionaje, asimismo interceptación de información de forma ilegal y sin autorización, se están violando datos personales, así como empresariales,

269H. Así como en la cláusula anterior, hace referencia a los numerales 1 (la organización trabaja con sistemas informáticos, sistemas de comunicaciones y redes no sólo a nivel nacional sino también mundial), 3 (se evidencia abuso de confianza), 5 (obtiene provecho propio o tiene intereses particulares).

- **Cláusula Quinta. Obligaciones de la parte reveladora.** Esta cláusula está inconclusa, así que queda abierta a asignarle lo que más le convenga a la organización, quiere decir que si el receptor firma, acepta cualquier otra situación que posteriormente se agregue. Con esto se puede atentar contra la ley 1273 puesto que sin haber claridad se puede dar por hecho ciertas conductas punibles.

- **Cláusula Octava. Solución de Controversias.** Con esta cláusula se estaría violando el artículo 269H, literal 7, que hace alusión a que se utiliza un tercero para dejarle toda la responsabilidad de los delitos cometidos, si en sus manos se encuentra cualquier tipo de información ilegal y la organización se libera de cualquier responsabilidad ya sea de tipo legal o penal, aunque sean los autores intelectuales de los hechos punibles, buscan dejar en manos de terceros las actividades delictivas.

5.2.3 **Análisis de la propuesta laboral.**

Existen procesos poco confiables en el Acuerdo y que atentan contra el código de ética COPNIA, así que NO aplicaría al trabajo en WhiteHouse, a pesar de que el contrato sea vitalicio y sea muy buen remunerado, ninguna cantidad de dinero vale mi ética profesional. Los motivos por los cuáles no aceptaría los comparto a continuación:

- Si formo parte de esta organización y firmo este Acuerdo, teniendo en cuenta que se especifica que la parte receptora no puede divulgar ningún tipo de información relacionada con sucesos ilegales, estaría siendo

participe de los mismos, atentando en gran medida contra varios de los artículos del código de ética del COPNIA.

- A pesar de que se relaciona a esta organización como reconocida a nivel mundial, pienso que realmente terminaría diluyéndose en poco tiempo, por su manera de actuar y de tratar de imponer otros responsables para lavarse las manos.

- Los artículos sobre los que se atentaría son:

Inciso b. Art. 31. El cuál trata de cuidar documentación, bienes e información de la cual se tenga acceso o que se haya delegado, impedir o evitar el uso indebido.[25]

Es evidente que se está violando este artículo, lo que tendría como consecuencia la suspensión de mi matrícula profesional, por supuesto, llegaría a su fin mi labor como ingeniero.

Inciso f del mismo artículo que indica denunciar todos los delitos cometidos contra el código de ética, faltas teniendo en cuenta lo que realice en la profesión y por supuesto aportando todas las pruebas del caso, con varias de las cláusulas del acuerdo que infieren que no se podrá denunciar cualquier situación ilícita de la organización, al firmarlo, se estaría violando este inciso.

Inciso b. Art. 32. Se estaría violando puesto que de acuerdo con lo que se indica se estaría permitiendo o tolerando un ejercicio ilegal de la profesión.

Art. 34. Tanto la organización como el profesional están infringiendo este artículo, pues se ofrece y se acepta un trabajo que va en contra de la legislación colombiana.

Art. 35. No se está velando por el buen prestigio de la profesión, al incurrir en acciones fraudulentas y además no hacer las denuncias respectivas.

Art. 40. El inciso a que hace referencia a prestar un servicio de dudoso cumplimiento y así mismo con un objeto cuya procedencia no sería legal.

Es importante poder dar cumplimiento al código de ética denunciando todo suceso o actividad ilegal y que vaya en contra de la profesión, no obstaculizar las investigaciones que realizan las autoridades competentes, colaborar en todo lo que sea necesario para que sea eficaz el desarrollo de las funciones asignadas, cumplir con toda la normatividad, respetar las leyes y nunca aceptar cualquier

[25] COPNIA.GOV.CO. [Sitio Web]. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines. [Consulta: 10 de septiembre de 2021]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

trabajo que vaya en contravía de lo anteriormente dispuesto, velar por una correcta reputación de la profesión.

5.2.4 **Análisis del caso "Operación Andrómeda BUGGLY"**

Con el análisis del caso Andrómeda se evidencian implicaciones éticas y legales por varios de los funcionarios que conformaban esta organización, muchos profesionales pudieron caer desprevenidamente y ser utilizados con fines individuales, ya haya sido por entidades privadas o algunos funcionarios del estado, por el hecho de aceptar acuerdos sin tener en cuenta minuciosamente todo lo que allí se especifica, analizando el contexto, la situación, todo esto teniendo en cuenta el código de ética como profesional en ingeniería y los delitos informáticos que se cometieron.

Según las declaraciones del Ejército y como lo enuncia El Tiempo, "Investigación halló fallas de seguridad. No controlaron actividades de personal militar y civil."[26], así mismo se indica que su existencia se encontraba dentro del marco legal. "La creación de la fachada 'Buggly Hacker' fue legal, con base en la Constitución Política de Colombia, directrices, reglamentos y el 'Manual de Manejo de Redes de Informantes', el cual se refiere a la 'fachada' y a la 'historia ficticia', relató en su momento el general Ernesto Maldonado, auditor general de la institución Militar".[27]

Es evidente que se buscaron personas talentosas en el ámbito, proponiendo gran valor lucrativo por adquirir servicios específicos, basados en estrategias sucias e ilegales, llevando a alcanzar los objetivos propuestos, se utilizaron malas prácticas de seguridad y no se visualiza un hacker que realmente esté fundamentado sobre la ética, para haber realizado un análisis exhaustivo, la supervisión requerida, que mostrará alto grado de experiencia y que generara un informe donde se exaltaran todos los controles que se debieron haber implantado junto con una correcta auditoría.

Definitivamente hubo un gran fallo de ética profesional y de legalidad, varios militares incurrieron en graves delitos, hubo graves atropellos en contra de los sistemas de información, chuzadas, se sustrajeron ilegalmente bases de datos, hubo espionaje, se revelaron secretos políticos, fugas de información, entre otras tantas faltas que atentan contra la seguridad.

---

[26] EL TIEMPO. [Sitio Web]. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [Consulta: 10 de septiembre de 2021]. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-15141236

[27] ENTER.COM. [Sitio Web]. Detrás de Buggly: La historia de la fachada Andrómeda [Consulta: 10 de septiembre de 2021]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Hizo falta generar acuerdos de confidencialidad claramente establecidos dentro del marco legal y ético, así como contratos donde se indicara realmente las labores a realizar, el fin de cada labor, para poder evidenciar las intenciones de la organización. Hay demasiado personal ingenuo que piensa que poner todas sus habilidades a favor de cualquier organización, que puede mostrar un perfil aparentemente bueno y que ofrezca grandes sumas de dinero, es suficiente para alcanzar sus metas, sin mirar más allá o el trasfondo de las cosas, que puede poner en peligro su profesión o libertad, por no anteponer la ética, moral y legalidad ante cualquier situación.

5.3 COMPILACIÓN ETAPA 3 DONDE SE EJECUTAN Y EVIDENCIAS PRUEBAS DE INTRUSIÓN

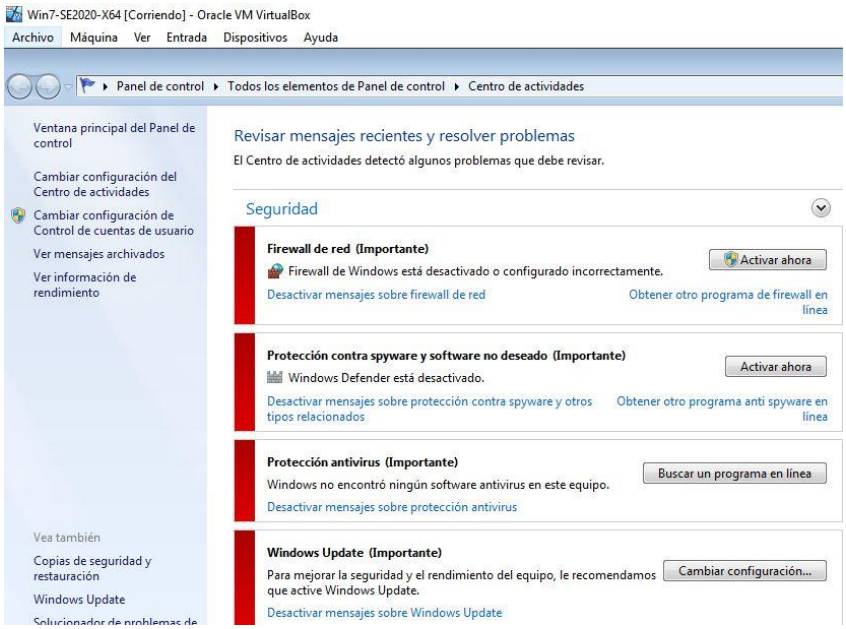
Es importante verificar el Anexo 4 – Escenario 3 para entender el contexto de la situación y proceder a instalar lo necesario para realizar con éxito la actividad, haciendo énfasis en que ya se había instalado previamente el banco de trabajo.

5.3.1 **Herramientas y procedimientos utilizados de acuerdo con los pasos del pentesting para dar solución al escenario de red team.**

Antes de empezar a definir las herramientas y procesos realizados en cada una de las etapas del pentesting es fundamental instalar la aplicación que se indica en el Anexo 4, Rejetto, con ello se podrá proceder a explicar en detalle lo realizado para dar solución a todas las preguntas orientadoras solicitadas en la guía de actividades.

Así mismo es fundamental desactivar Windows defender en la máquina víctima, así como el firewall y verificar que no tenga antivirus o también esté desactivado, como se muestra en la siguiente imagen:

Figura 10. Deshabilitar seguridad en máquina Windows X64



Fuente: Propia

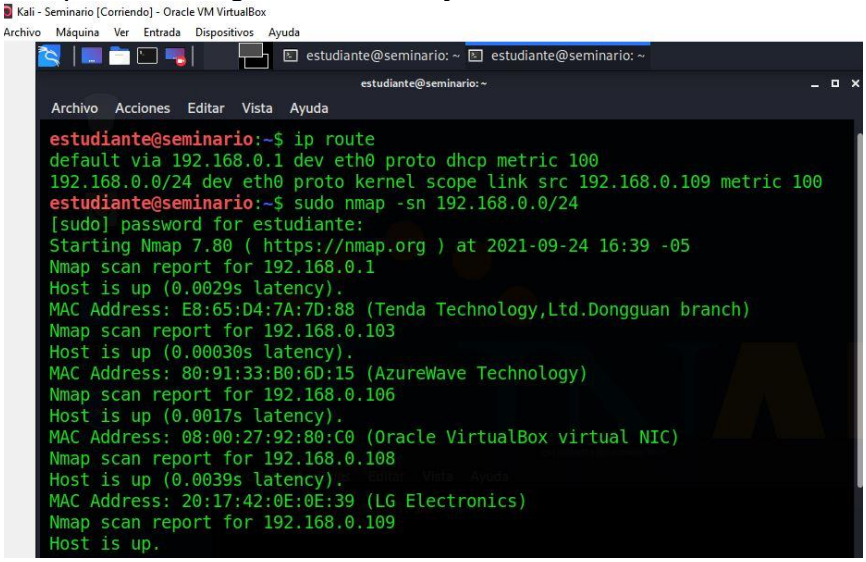
A continuación, se define en cada una de las etapas del pentesting las herramientas y procedimientos utilizados para poder darle solución a lo expuesto en el escenario 4 y cómo actuarían los integrantes del Red Team.

- **Fase de recopilación de información:** En esta etapa de reconocimiento se recopila toda la información que sea posible sobre la máquina víctima, es una etapa fundamental, puesto que al ser el comienzo del pentesting se busca encontrar la mayor cantidad de vulnerabilidades de acuerdo con lo recopilado y así poder explotarlas, se intenta hallar que tipo de sistema operativo tiene la máquina objetivo, su versión, si la máquina víctima tiene puertos abiertos, los servicios en ejecución, así que para ello se procede a utilizar la herramienta **nmap** presente en Kali Linux**.**

Se inicia utilizando nmap para buscar el segmento de red y verificar los hosts que están en ese segmento con el fin de conocer la dirección IP de la máquina objetivo.

Cómo se puede evidenciar en la imagen siguiente, hay 5 dispositivos activos, dos de los cuales corresponden a las máquinas virtuales, se descarta una de esas direcciones pues corresponde a la máquina Kali Linux, cuya dirección es 192.168.0.109, por ende, la dirección IP asociada con la máquina objetivo correspondería a **192.168.0.106.** Con ello se puede realizar nmap directamente a la máquina víctima

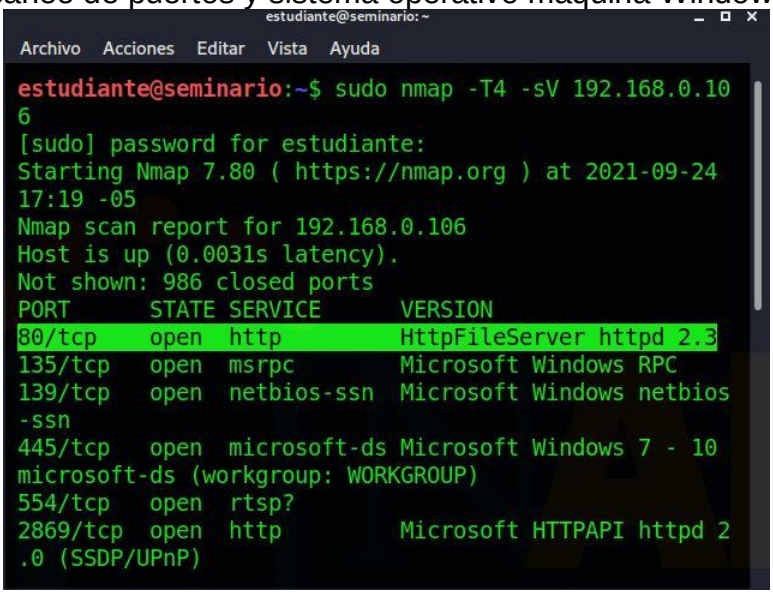
Figura 11. Búsqueda de segmento de red y hosts activos



Fuente: Propia

Conociendo la IP de la máquina víctima, se puede proceder a indagar sobre puertos abiertos, sistema operativo, servicios, entre otros.

Figura 12. Escaneo de puertos y sistema operativo máquina Windows X64



Fuente: Propia

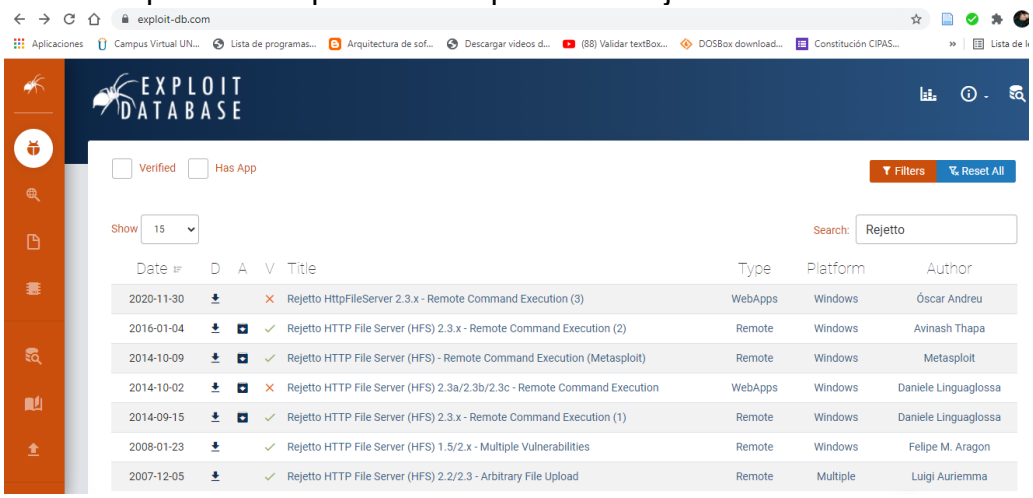
Además de lo anterior se recurre al Anexo 4, puesto que allí se dan unas pautas importantes que sirven para empezar a recolectar información relevante, por ejemplo, se indica que el sistema operativo de la máquina es un Windows 7 con

arquitectura x64, con esto ya se puede evidenciar una falla de seguridad puesto que ese sistema operativo en la actualidad no cuenta con actualizaciones de seguridad, se recomienda que los sistemas operativos tengan actualizaciones recientes, con sus correspondientes parches, esta información es relevante.

Adicional a lo anterior, en el anexo también se indica que hay una aplicación instalada llamada Rejetto v.2.3, por ende, se procede a investigar que tipo de aplicación es ésta, si tiene asociado algún exploit que dé pautas para realizar fases posteriores.

- **Búsqueda de vulnerabilidades:** La aplicación Rejetto v.2.3 es un servidor de archivos Http remoto, que permite enviar y recibir archivos por medio de internet, se puede empezar a conocer si existe vulnerabilidades al tener instalada esta aplicación y así mismo si pueden ser explotadas, para empezar a tener más información de este tipo se puede revisar la base de datos de exploits, colocando el nombre de la aplicación, como se muestra a continuación:

Figura 13. Búsqueda de exploits de la aplicación Rejetto

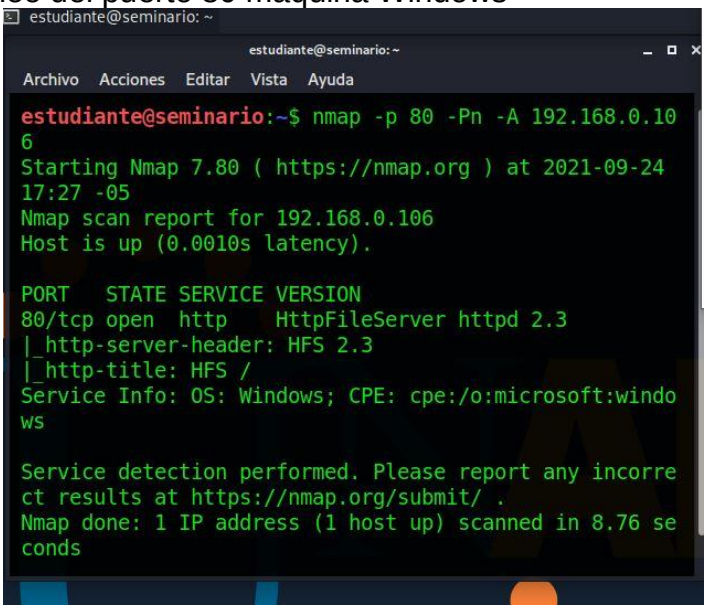


Fuente: Propia

Se evidenció que, si existe exploits para la aplicación instalada en la máquina objetivo, es decir, que si es una aplicación con vulnerabilidades y que estas pueden ser explotadas en una fase posterior.

Teniendo en cuenta que en la recopilación de información se encontraron varios puertos abiertos y que uno de ellos es el puerto 80, se procede a hacer un escaneo a este puerto para verificar que vulnerabilidades se encuentran para luego realizar su explotación.

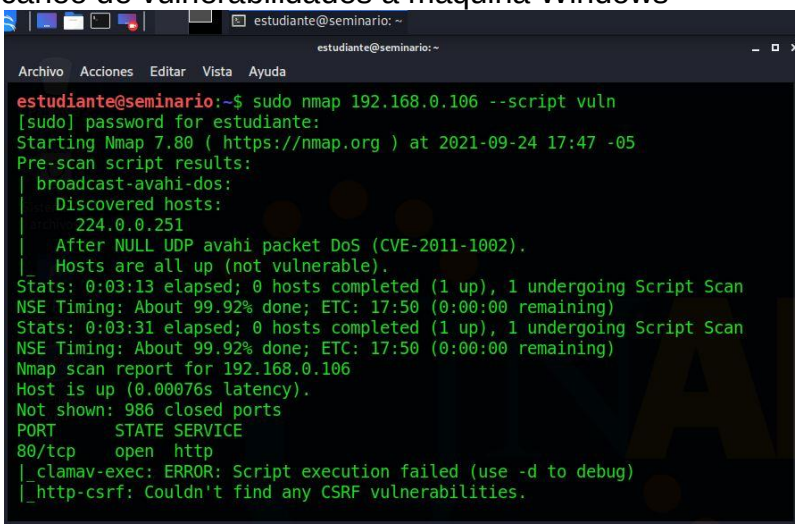
Figura 14. Escaneo del puerto 80 máquina Windows



Fuente: Propia

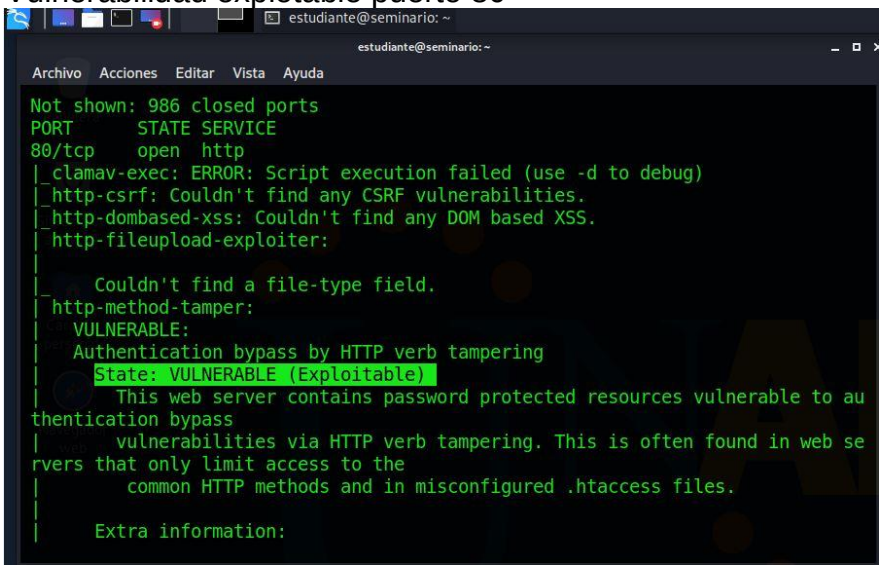
Al hacer escaneo al puerto 80 de la máquina Windows X64 se evidencia que es por donde se está ejecutando la aplicación rejetto v.2.3, se puede confirmar las vulnerabilidades al utilizar el comando nmap con los parámetros -script vuln.

Figura 15. Escaneo de vulnerabilidades a máquina Windows



Fuente: Propia

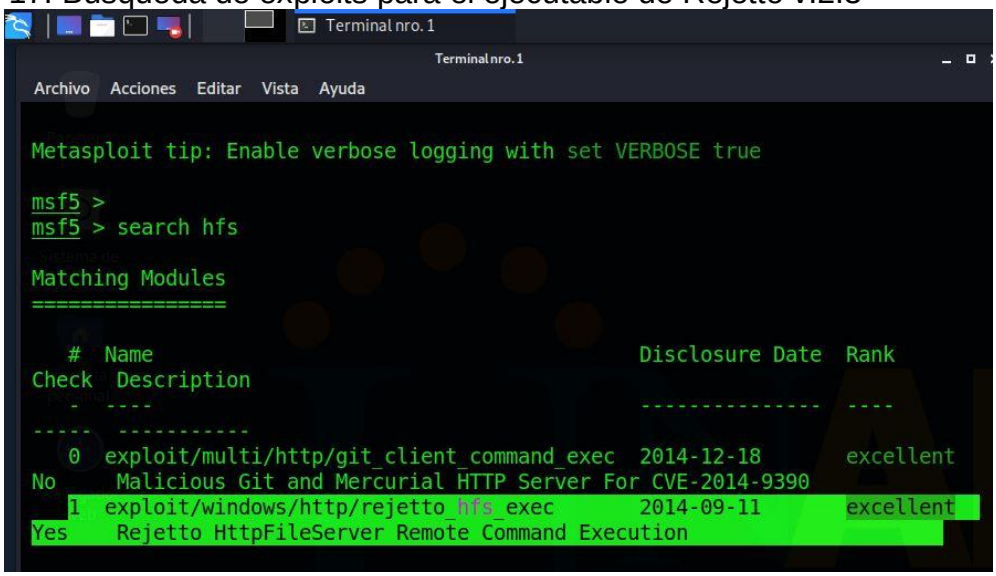
Figura 16. Vulnerabilidad explotable puerto 80



Fuente: Propia

- **Explotación de Vulnerabilidades:** Luego de hallar la vulnerabilidad se procede a explotarla, por tal razón se utiliza otra herramienta de Kali Linux llamada metasploit, al abrirla puede proceder a buscar el ejecutable en la aplicación para verificar que exista el exploit como se muestra a continuación:

Figura 17. Búsqueda de exploits para el ejecutable de Rejetto v.2.3

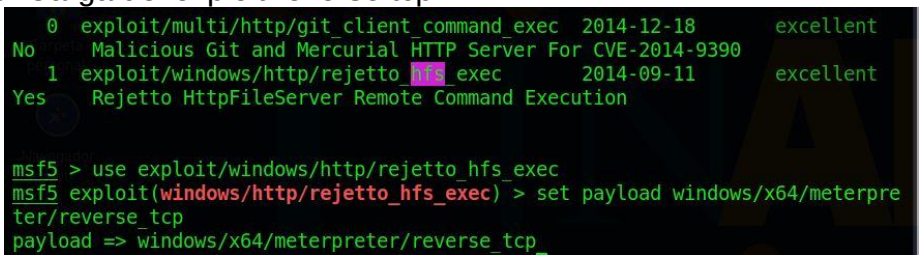


Fuente: Propia

Con lo anteriormente visto, se puede buscar la vulnerabilidad exacta la cual es CVE-2014-6287[28], es una vulnerabilidad severa, tiene un puntaje base asignado de 9.8 lo que la hace crítica y hace alusión a validaciones erróneas en la librería ParsetLib que permite a atacantes remotos ejecutar programas indeseados y que pueden terminar en una escalada de privilegios, como el mismo enunciado del Anexo 4 lo indica.

Se procede a ejecutar el exploit que puede terminar en una Shell reversa como se expresaba en el Anexo 4 y abrir una sesión meterpreter, esto se realiza cargando el payload.

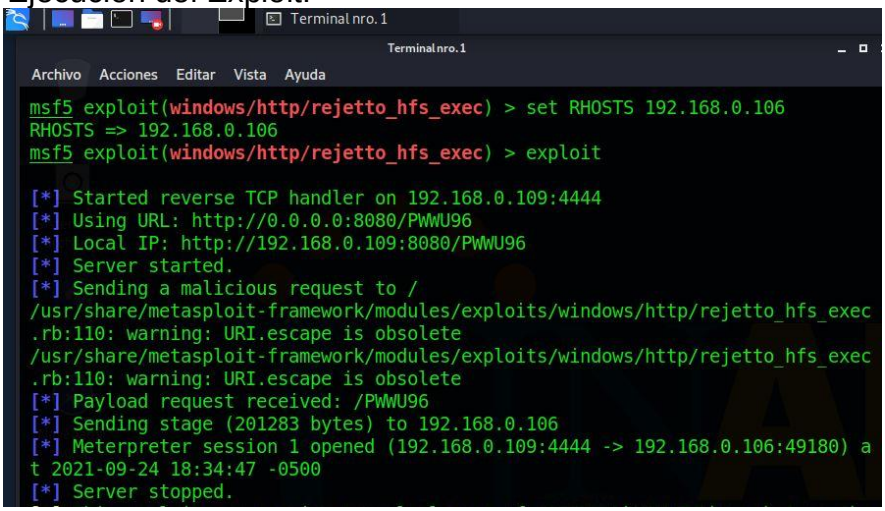
Figura 18. Carga del exploit reverse tcp



Fuente: Propia

Es necesario configurar el exploit, se utiliza el comando SET para establecer la IP del host que se va a atacar. Luego se ejecuta el exploit, con lo cual se va a conectar con la máquina Windows X64, con ello se abre una sesión meterpreter y allí se va a poder interactuar por medio de línea de comandos.

Figura 19. Ejecución del Exploit.



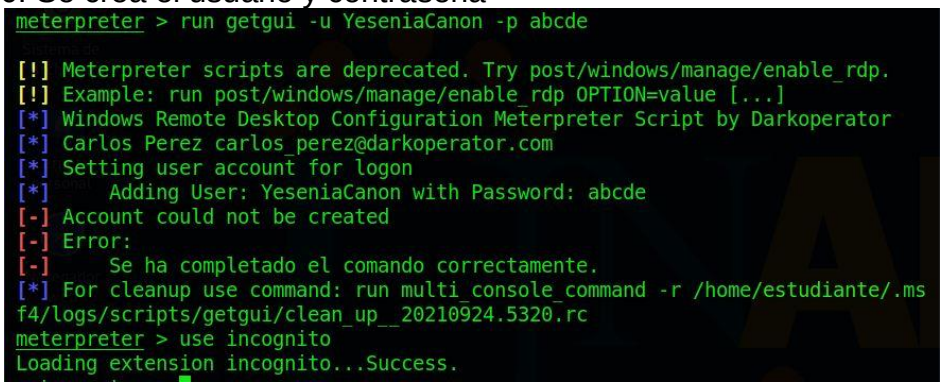
Fuente: Propia

[28] NVD.NIST.GOV. [Sitio Web]. CVE-2014-6287 Detail. [Consulta: 24 de septiembre de 2021]. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2014-6287

- **Fase de Post Explotación:** Se busca en esta fase causar un gran impacto en el objetivo de acuerdo con las vulnerabilidades explotadas, para ello el punto clave es poder realizar una escalada de privilegios y acceder a información crítica. Así como se indicó en el Anexo 4, ya teniendo una sesión de meterpreter se puede escalar privilegios, se crea un usuario Administrador con mi nombre y apellido en la máquina Windows, también se le crea una contraseña, se utiliza el comando run getgui y con esto se evidencia que se puede tener todo el control de la máquina.

Se utiliza el comando use incognito para que el usuario pueda tener acceso como administrador, con esto el usuario creado en Windows se asocia al grupo correspondiente.

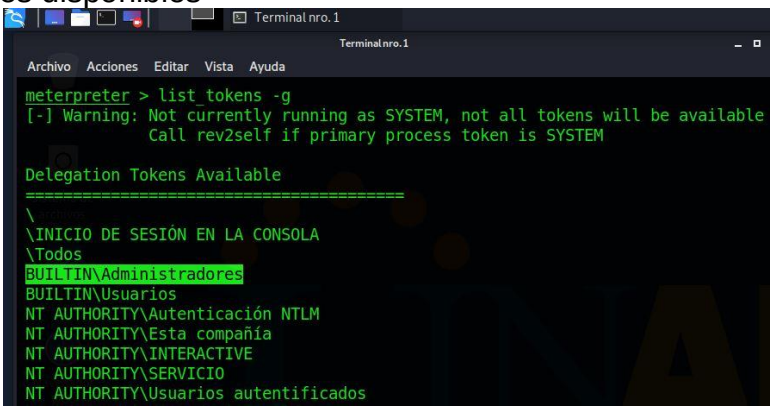
Figura 20. Se crea el usuario y contraseña



Fuente: Propia

Para poder ver la lista de tokens del sistema o también podrían llamarse grupos, se puede utilizar el comando list_tokens -g, con ello se puede observar el grupo Administradores

Figura 21. Roles disponibles



Fuente: Propia

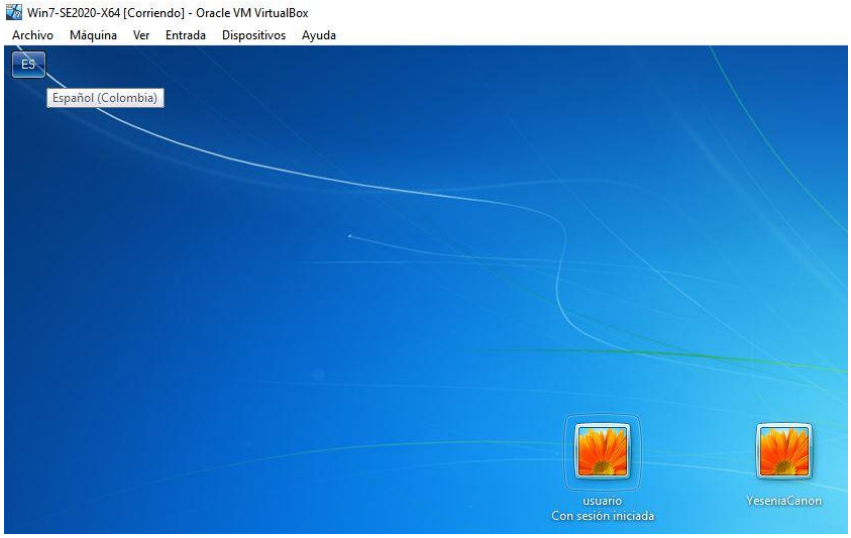
Con el comando señalado en la imagen se agrega el usuario YeseniaCanon al grupo de Administradores:

Figura 22. Asignación de usuario como Administrador

```
meterpreter > add_localgroup_user "Administradores" "YeseniaCanon"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[*] Attempting to add user YeseniaCanon to localgroup Administradores on host
127.0.0.1
[+] Successfully added user to local group
```

Fuente: Propia

Figura 23. Usuario creado en Windows X64.



Fuente: Propia

- **Fase de Reportes o Informe de Resultados:** En esta fase se puede evidenciar el presente informe**,** las vulnerabilidades y falencias halladas, se anexan imágenes o capturas de pantalla donde se evidencia todo el proceso realizado en las fases anteriores, así mismo se deben brindar las soluciones correspondientes a las vulnerabilidades halladas.

5.3.2 Datos e información del anexo 4 – escenario 3 que fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 7 x64.

Un aspecto importante que señala el anexo es que habla de una fuga de información, indica que hay uno de los equipos por los cuales se está accediendo a sus recursos, es decir, que los niveles de seguridad de este equipo están fallando, ya sea por falta de antivirus, firewall desactivado, Windows defender, sin actualizaciones, sin parches de seguridad, lo que hace pensar que para mantener

el sistema seguro es fundamental, estar revisando que cada equipo cuente con ese esquema de seguridad que debería ser el mínimo.

Otro aspecto importante que señala el anexo es que informa de una vez el tipo de sistema operativo, Windows 7, su arquitectura 64 bits, así como la aplicación que tiene instalada, Rejetto v.2.3, lo que llevó a hacer un primer análisis y recopilación importante, puesto que también indica que a ese software puede estar relacionado un exploit, el cual puede generar una Shell reversa y una sesión abierta de meterpreter, con estos datos se empieza a hacer un diagnóstico, como se hizo en la fase de recolección de información, se puede averiguar en un buscador que tipo de aplicación es y si se encuentran vulnerabilidades asociadas a ella.

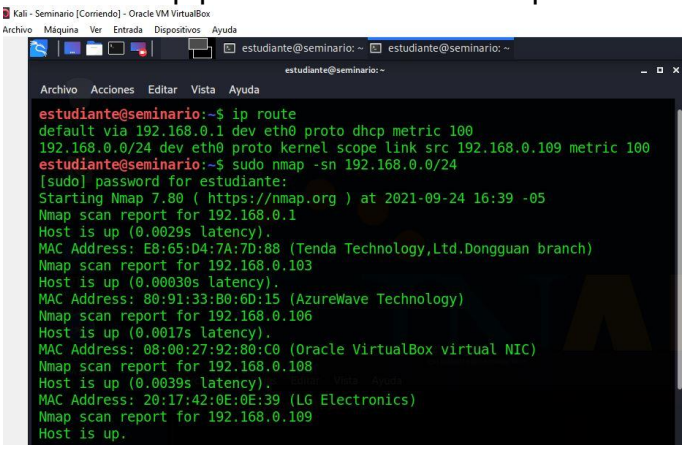
Se da indicios sobre una escalada de privilegios, además de que se indica que el usuario creado tenía permisos de administrador, lo que significa que la vulnerabilidad es crítica, porque se llego al punto de tener el control total de la máquina Windows, todo esto da pistas para indagar sobre la vulnerabilidad específica y los parámetros utilizados para explotarla. Por supuesto, con todo esto se va pensando en todas las medidas a implementar para que en determinado sistema no vaya a suceder lo mismo que en el escenario propuesto.

Todas las evidencias recolectadas, lo compartido en cada fase del pentesting, sirve para demostrarle a los altos directivos una prueba de concepto. Así se conocen las vulnerabilidades para posteriormente resolverlas.

5.3.3 **Herramientas utilizadas para poder identificar los fallos de seguridad de la máquina windows 7 y puerto abre la aplicación específica en el anexo**

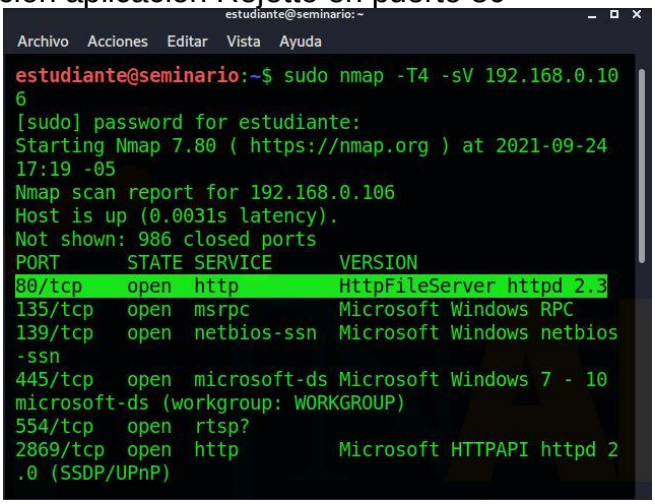
Se utilizó la herramienta nmap, primero indagando la dirección IP, luego verificando aquella dirección (192.168.0.106) para constatar servicios ejecutados, puertos abiertos, entre otros, de esta manera se puede acceder al **puerto** específico que abre la aplicación Rejetto v.2.3 el cual es el **80**, con ello se puede hacer un escaneo al puerto específico y así evidenciar que tan vulnerable es, para luego utilizar un exploit y sacar provecho a las vulnerabilidades encontradas.

Figura 24. Utilización de Nmap para hallar IP de la máquina Windows X64



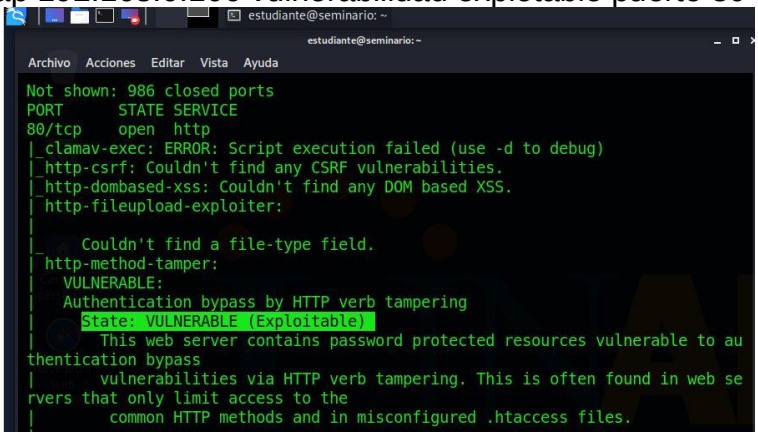
Fuente: Propia

Figura 25. Verificación aplicación Rejetto en puerto 80



Fuente: Propia

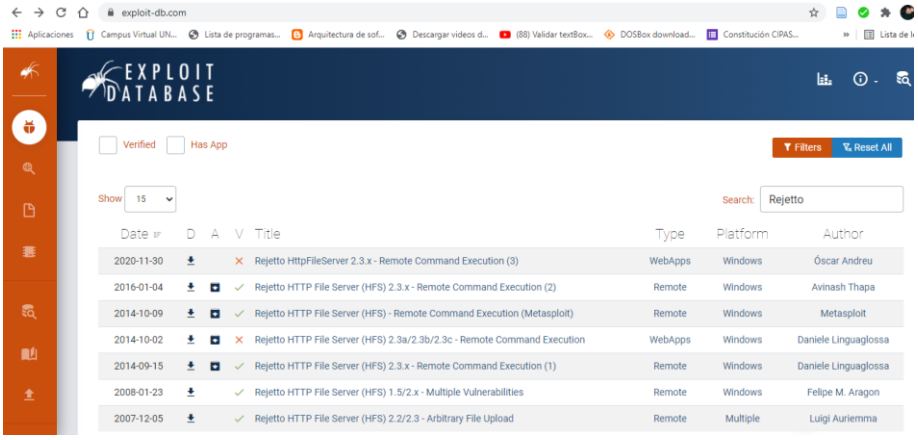
Figura 26. Nmap 192.168.0.106 vulnerabilidad explotable puerto 80



Fuente: Propia

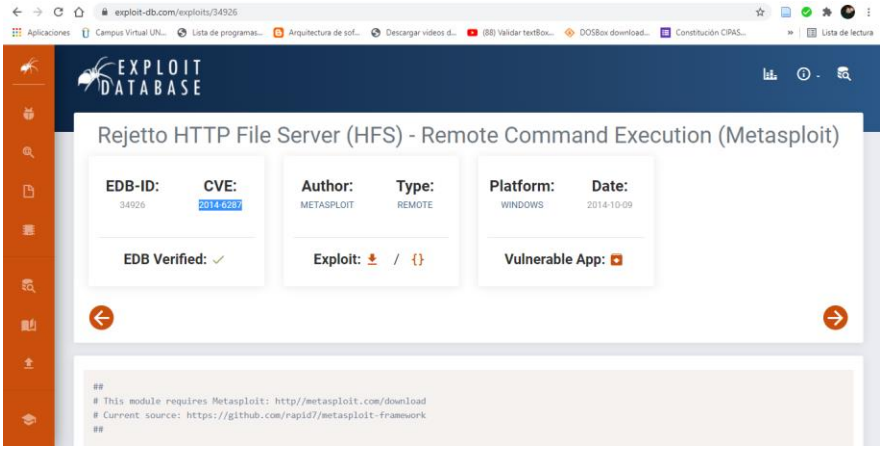
Así mismo, con la información suministrada en el anexo, se utilizó el buscador de Google para conocer un poco más sobre la aplicación Rejetto v.2.3, se buscó además en la base de datos de exploits donde se confirma que tiene una vulnerabilidad crítica, con ello también se accedió al CVE específico, el cual dio una base más amplia de lo grave de la vulnerabilidad y sus consecuencias.

Figura 27. Base de Datos de Exploits



Fuente: Propia

Figura 28. CVE-2014-6287



Fuente: Propia

5.3.4 **Consecuencias del ataque a la máquina (windows 7 x64)**

Es grave el ataque a la máquina Windows puesto que por estarse ejecutando la aplicación Rejetto, se tiene abierto el puerto 80, lo que permite la ejecución del exploit, por la vulnerabilidad que presenta la aplicación, esto conlleva a poder tomar posesión de la máquina Windows y así realizar una escalada de privilegios, el objetivo sufre un gran impacto, puesto que se puede acceder a información

crítica, se buscaría actuar como una amenaza persistente avanzada, con el fin de descubrir brechas de seguridad, no solo en sistemas internos, sino que abarque seguridad perimetral.

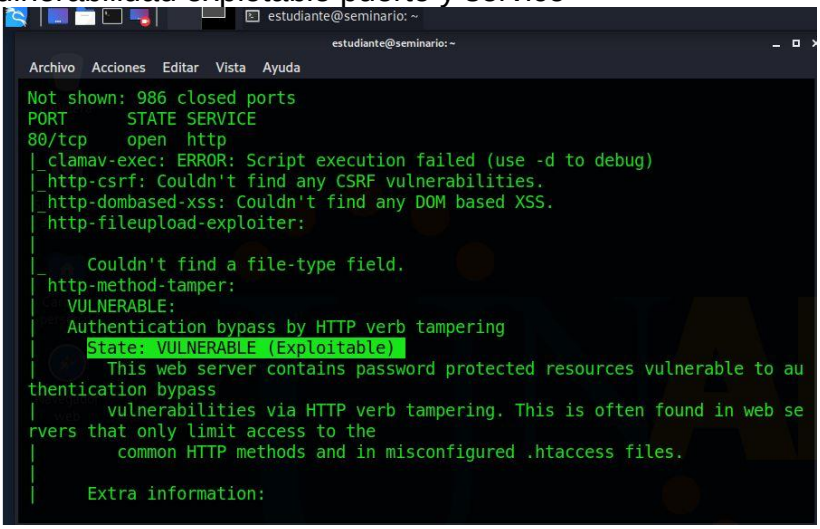
Figura 29. Ataque realizado

Fuente: Propia

5.3.5 **Evidencias explotación de vulnerabilidad en la máquina windows 7**

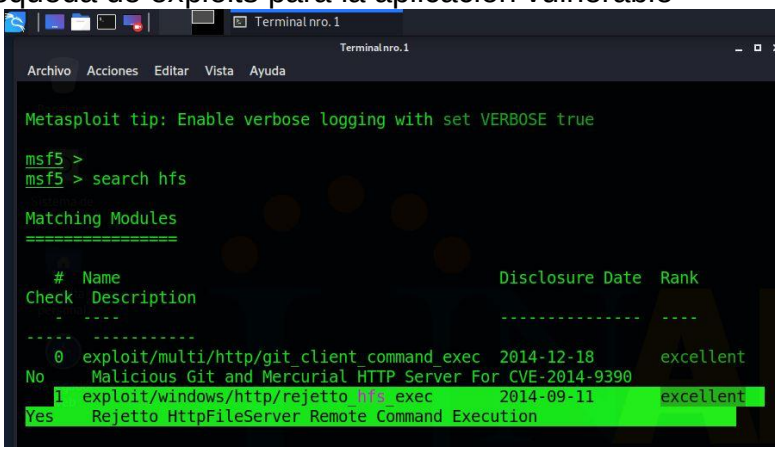
Para explotar la vulnerabilidad hallada se verifica el servicio y el puerto, luego se busca el exploit correspondiente.

Figura 30. Vulnerabilidad explotable puerto y servico



Fuente: Propia

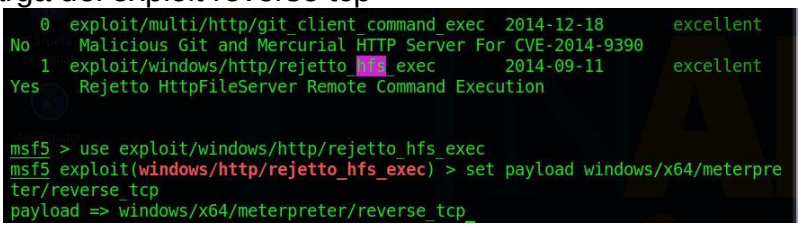
Figura 31. Búsqueda de exploits para la aplicación vulnerable



Fuente: Propia

Se procede a ejecutar el exploit que puede terminar en una Shell reversa como se expresaba en el Anexo 4 y abrir una sesión meterpreter, esto se realiza cargando el payload.

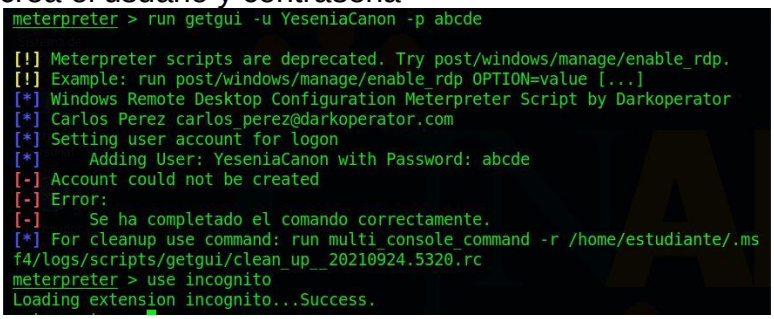
Figura 32. Carga del exploit reverse tcp



Fuente: Propia

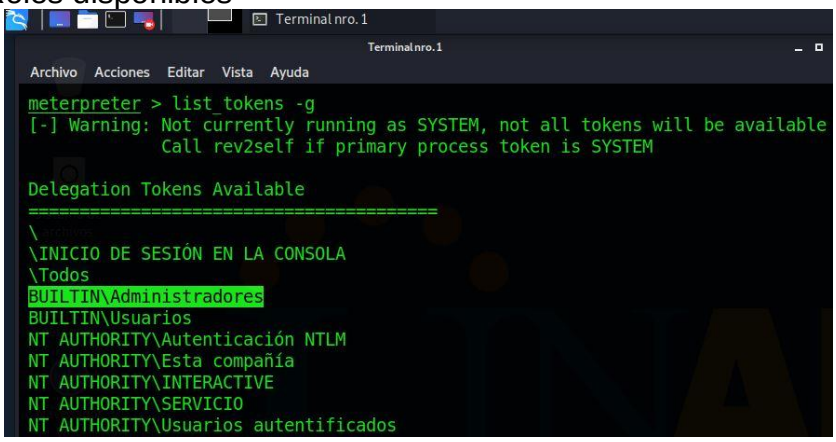
Es necesario configurar el exploit, se utiliza el comando SET para establecer la IP del host que se va a atacar. Luego se ejecuta el exploit, con lo cual se va a conectar con la máquina Windows X64, con ello se abre una sesión meterpreter y allí se va a poder interactuar por medio de línea de comandos. Se utiliza el comando use incognito para que el usuario pueda tener acceso como administrador, con esto el usuario creado en Windows se asocia al grupo correspondiente.

Figura 33. Se crea el usuario y contraseña



Fuente: Propia

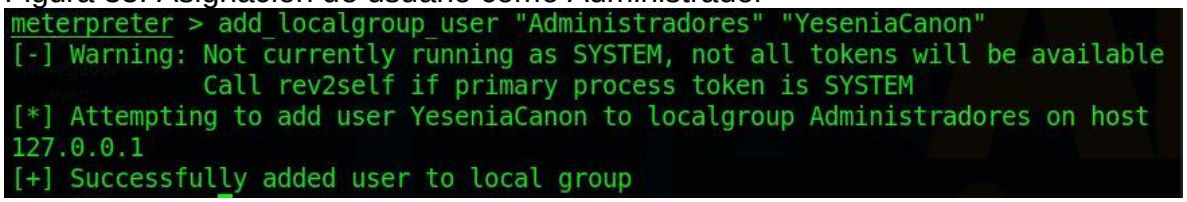
Figura 34. Roles disponibles



Fuente: Propia

Con el comando señalado en la imagen se agrega el usuario YeseniaCanon al grupo de Administradores:

Figura 35. Asignación de usuario como Administrador



Fuente: Propia

5.4 SOLUCIÓN DE LA ETAPA 4 DONDE SE FORMULAN ESTRATEGIAS DE CONTENCIÓN PARA EVITAR ATAQUES INFORMÁTICOS

Para el desarrollo de la presente actividad se verifica el Anexo 5 – Escenario 4 para entender el contexto de la situación y se procede a dar solución a los interrogantes planteados en la guía de la Etapa 4.

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

De acuerdo con el escenario propuesto en el Anexo 5, se busca que los integrantes del Blue Team puedan contener un ataque informático en tiempo real que incluye a una de las máquinas que conforman la estructura de Red la cual corresponde a la Windows 7 X6. Se debe llevar a cabo un análisis de lo sucedido y poner en práctica las medidas necesarias para su contención.

Teniendo en cuenta que una de las máquinas fue accedida sin autorización y vulnerada, lo primero que se debe hacer es aislar dicho equipo del resto de la red, con el propósito de evitar que se propague cualquier software malicioso en los demás equipos de la red local, con el fin de que el ataque pueda afectar servidores de la red u otros equipos, así mismo, es primordial aislar la información o datos críticos que puedan ser robados por los atacantes con la intrusión.

El siguiente paso por ejecutar es analizar el equipo que fue vulnerado, en primera instancia verificando actualizaciones, antivirus, firewall, entre otros. Analizando la máquina Windows 7 X64 se evidencia que tiene deshabilitado el firewall, el Windows defender y no posee antivirus. Se procede a instalar un antivirus, activar el firewall, Windows defender y todas las actualizaciones correspondientes.

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

Para evitar sufrir un ataque como el perpetrado por el Red Team en la Etapa 3, se deben implementar ciertas medidas de hardenización, que va desde lo más básico hasta acciones más relevantes como las que se indican a continuación:

- Es importante mantener los sistemas operativos de todos los equipos de una organización actualizados, aconsejable que sea en sus últimas versiones y que se pueda contar con sus correspondientes parches.

- Mantener los equipos con antivirus actualizados o si no se cuenta con ellos realizar la respectiva instalación.

- Activar el firewall, verificar periódicamente que esté correctamente configurado, definir reglas de entrada y salida que se puedan aplicarse a los puertos del sistema.

- Mantener cerrados los puertos que no sean necesarios para evitar que el atacante haga uso de vulnerabilidades relacionadas con puertos abiertos.

- Establecer políticas para el uso y generación de contraseñas de usuario, donde se evidencie que se deben definir de acuerdo a la utilización obligatoria de números, letras, símbolos, por lo menos una mayúscula, se debe cumplir con todos los estándares de seguridad, teniendo en cuenta el histórico, puesto que no se deben repetir contraseñas que hayan sido utilizadas anteriormente, así mismo que se deben cambiar cada determinado tiempo y bloquear cuentas cuando se ingrese determinado números de veces contraseñas erróneas.

- Deshabilitar el acceso remoto si no se va a utilizar o por lo menos reforzarlo limitando la cantidad de conexiones que se puedan aceptar, así mismo se podría limitar los permisos a los usuarios que se deseen conectar de esa manera. Otra opción en el caso de que, si se requiera conexión remota, sería establecer por SSH un canal de comunicación cifrado.

- Teniendo en cuenta el reporte generado por el Red Team, verificar si el ataque se lleva a cabo siempre desde un rango de IPs específico, se pueden bloquear por medio de listas negras.

- Podría ser una muy buena opción implementar una VPN con el fin de que el acceso externo al sistema sea más reforzado.

- Realizar un inventario de usuarios inactivos y activos del sistema, verificar los privilegios asignados, es importante de igual manera tener en cuenta los permisos que se asignan a nivel de sistema operativo.

- Deshabilitar los usuarios de tipo genérico, eliminar usuarios locales que no s estén utilizando y renombrar el usuario que esté como administrador.

- Actualizar en su última versión las aplicaciones instaladas o en su defecto eliminar las que no sean necesarias o sean peligrosas. Así mismo, verificar los procesos que se estén ejecutando.

- Es importante utilizar un software para escaneo de vulnerabilidades, con el fin de poder blindar el sistema, por ejemplo, se puede utilizar Nessus u Openvas el cual incluye algunas soluciones dependiendo de la vulnerabilidad hallada y así se podría aplicar. Conociendo las

vulnerabilidades que hay en nuestro sistema será más fácil tomar las correspondientes medidas para disminuirlas, eliminarlas o controlarlas.

- Implementación de procesos de auditoría y de monitoreo permanente de logs, con el fin de verificar eventos sospechosos.

- Implementar sistemas de detección de intrusos y herramientas de monitoreo a nivel de red, con el fin de que puedan realizar tareas automatizadas, donde se brinde un escaneo constante y se generen las alertas correspondientes siempre que haya accesos no autorizados.

- Establecer políticas de copias de seguridad y su correspondiente administración.

5.4.3 Diferencias entre blue team y equipo de respuestas a incidentes informáticos

A continuación, se describe tanto el Blue Team como el equipo de respuesta a incidentes informáticos CSIRT, al finalizar este ítem se realizará un cuadro resumen de sus principales diferencias:

El **Blue Team**, también llamado equipo azul, está conformado por un grupo de profesionales especializados en seguridad, que visualizan la organización de adentro hacia afuera. Su función es defender los activos más importantes de un sistema de información de la organización, buscando protegerlos de cualquier tipo de amenaza. Están fielmente conscientes de cuáles son los objetivos y estrategias en cuanto a seguridad refiere la organización. En otras palabras, busca fortalecer los muros de la información para que ningún atacante pueda sobrepasarlos.

Algunas de las tareas hechas por el Blue Team son:

- **La evidencia debe ser guardada**: Es sumamente importante salvaguardar toda la evidencia posible de los incidentes hallados, para asegurarse de tener información visible que pueda ser analizada, organizarla y tomar las acciones correspondientes para mitigar los riesgos.

- **La evidencia debe ser validada**: No todas las pruebas o alertas generadas, conducirán a una violación del sistema válida. Si esto sucede, se debe catalogar como un índice de compromiso.

- **Incluir a todas las personas que sean necesarias y que contribuyan a mejorar la seguridad**: Los integrantes del Blue Team deben saber qué hacer con el índice de compromiso, ser consciente de ello e incluir a los equipos más importantes, que varían según la empresa.

- **Evaluar el suceso**: Algunas veces el Blue Team puede requerir involucrar a las fuerzas de orden público, o es posible que necesiten una orden judicial con la cual se pueda llevar a término una investigación adicional, una correcta evaluación puede influir en este proceso.

- **Visualizar el alcance de la brecha**: En esta instancia el Blue Team tiene bastante información para conocer el alcance de la brecha.

- **Crear un plan de remediación:** El Blue Team debe elaborar un plan de remediación para contrarrestar al atacante.

- **Establecer el plan**: Luego de que el plan es finalizado, el Blue Team necesita ponerlo en práctica y recuperarse de la brecha de seguridad.

Un **equipo de respuestas a incidentes informáticos**, o **CSIRT**, es un grupo de profesionales con el objetivo principal de un CSIRT es responder a los incidentes de seguridad informática de manera rápida y eficiente, recuperando así el control y minimizando los daños. Esto implica seguir las cuatro fases de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST):

- Preparación.
- Detección y análisis.
- Contención, erradicación y recuperación.
- Actividad posterior al incidente.

Para hacerlo, los CSIRT pueden asumir muchas responsabilidades, incluidas las siguientes:

- Crear y actualizar planes de respuesta a incidentes.
- Mantener y comunicar información a entidades internas y externas.
- Identificar, evaluar y analizar incidentes.
- Coordinar y comunicar los esfuerzos de respuesta.
- Remediar incidentes.
- Informar sobre incidentes.
- Gestionar auditorías.
- Revisar las políticas de seguridad.
- Recomendar cambios para prevenir incidentes futuros.

Cuadro 1. Diferencias entre Blue Team y CSIRT

BLUE TEAM	**EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS**
Equipos Externos de la Organización.	Equipos internos de la organización,

Se centran en contener y conservar la seguridad de los sistemas informáticos de la organización que los contrata. Tipo de seguridad defensiva, busca disminuir riesgos, prevenir amenazas, contrarrestar ataques. Dependen de los informes que los Red Team entregan de acuerdo con los ataques controlados que hayan hecho. Analiza comportamiento de las personas, aplicaciones, sistema en general. El tipo de vigilancia que maneja es permanente, documenta completamente todo el proceso realizado, lo que ayuda a ejecutar procedimientos que beneficia a la organización.	utiliza su propio recurso humano. Verifican las vulnerabilidades y así mismo las contienen y las eliminan. Se centran en las incidencias de seguridad, que puede ser un hecho sospechoso o real. Identifica y analiza tanto las causas como las consecuencias del incidente. El tipo de vigilancia que maneja es periódico puesto que se centra en objetivos específicos. Tienen la capacidad de desarrollar herramientas de seguridad. Se basa en incidentes, es decir, puede haber ocurrido un ataque y puede llevar a un estado crítico, busca remediar lo ocurrido.

Fuente: Elaboración propia

5.4.4 **Pertinencia de trabajar con CIS "center for internet security" como propuesta de aseguramiento por parte de blue team**

Antes de expresar con qué fin utilizaría CIS como propuesta de aseguramiento de Blue Team, es importante conocerlo y abordar sus principales características, las cuales expongo a continuación:

El Centro de Seguridad de Internet (CIS) es una organización sin fines de lucro enfocada en mejorar la preparación y respuesta en ciberseguridad del sector público y privado. Se estableció en octubre de 2000 e inició con dos objetivos claramente establecidos:

- Identificar, desarrollar, validar, promover y mantener soluciones de mejores prácticas para la defensa cibernética.

- Construir y liderar comunidades para permitir un entorno de confianza en el ciberespacio.

Con sede en Nueva York, la organización cuenta con cientos de profesionales de seguridad de TI que representan agencias gubernamentales, militares, grandes corporaciones, conglomerados e instituciones académicas.

Con el tiempo, estableció el estándar global para la seguridad de Internet y las mejores prácticas, la mayoría de las cuales se describen en sus Controles CIS y puntos de referencia CIS.

Para ayudar a las organizaciones y las personas con la seguridad cibernética, el CIS proporciona a los miembros recursos como correos electrónicos con consejos sobre seguridad cibernética, guías y documentos en línea, videos y podcasts instructivos. El CIS también brinda asesoramiento para el desarrollo de políticas de ciberseguridad tanto a nivel nacional como internacional.

El mundo del ciberdelito es voluble. Está compuesto por decenas de miles de personas que trabajan de forma autónoma, cada una con sus propios objetivos, métodos y estrategias. En términos de seguridad, esta descentralización crea un problema enorme. Hay demasiados delincuentes y demasiadas áreas potenciales de ataque para que una organización las maneje por sí sola.

Para combatir los ataques, CIS evita un modelo de control de seguridad de arriba hacia abajo. En cambio, favorece una defensa de grupo única que depende en gran medida del crowdsourcing. Los miembros individuales del CIS son suplentes. Esto les da autoridad para realizar dos tareas principales:

- Identificar pasivos de seguridad.
- Proponer mejoras a las medidas de seguridad.

Una alerta o recomendación es compartida y evaluada por la comunidad, y luego se somete a votación. Si pasa, la medida de seguridad se integra.

A lo largo de los años, esta colaboración ha ayudado a formar el marco para los controles y parámetros de seguridad críticos de CIS. Los controles de seguridad crítica de CIS se componen de 20 protocolos de seguridad esenciales, que se agrupan en tres niveles:

- Básico - Controles 1-6
- Fundamental - Controles 7-16
- Organizacional - Controles 17-20

Los controles CIS no son todos los posibles protocolos de seguridad disponibles; sin embargo, forman una primera línea de defensa vital contra la mayoría de los ciberataques, por tal razón lo tendría en cuenta para definir una serie de

prioridades y acciones a desplegar con el fin de realizar eficazmente el proceso de contención de ataques.

Al utilizar los controles de seguridad básicos, por ejemplo, los primeros 5 controles son los más críticos, pueden detener el 85% de los ataques, teniendo en cuenta que a lo largo de los años se han agregado, refinado y actualizado controles básicos. Con cada versión recién lanzada, las prescripciones de seguridad son más aplicables y procesables.

Debido a que los controles se actualizan periódicamente utilizando datos de ataques actuales, pueden seguir siendo efectivos contra las amenazas cibernéticas en evolución de la actualidad. Los controles CIS actúan como un modelo para que los operadores de red eliminen el desorden de innumerables recomendaciones hechas por innumerables fuentes, para mejorar la ciberseguridad al sugerir acciones específicas que se deben realizar en un orden de prioridad.

Teniendo en cuenta todo lo anteriormente expuesto, a continuación, defino cómo actuaría dentro del Blue Team al momento de aplicar los controles de seguridad básicos, para no extenderme señalando los demás controles.

- C1 - Inventario y control de activos de hardware. La amenaza: los piratas informáticos siempre están monitoreando los objetivos y esperando que nuevos sistemas desprotegidos ingresen a la red, en particular traer sus propios dispositivos.

La respuesta: realizar una gestión activa (inventario, seguimiento y corrección) de los dispositivos de hardware para asegurarse de que solo los autorizados tengan acceso a la red. Los que no autorizados y además no administrados deben identificarse inmediatamente y denegarse el acceso.

- C2 - Inventario y control de activos de software. La amenaza: los piratas informáticos monitorean constantemente los objetivos, en busca de software vulnerables para ser explotados.

La respuesta: realizar una gestión activa (inventario, seguimiento y corrección) del software en general de la red para asegurarse de que únicamente el autorizado esté instalado y además pueda ejecutarse. El software que se encuentre como no autorizado y por ende no administrado debe identificarse y bloquearse para que no se pueda instalar o ejecutar.

- C3 - Gestión continua de vulnerabilidades. La amenaza: los piratas informáticos están buscando brechas de exposición que se producen entre

las amenazas de seguridad identificadas recientemente y las acciones correctivas.

La respuesta: recopilar, analizar y actuar continuamente sobre la nueva información (actualizaciones de software, avisos de seguridad, boletines de amenazas, parches) para resaltar las exposiciones y minimizar su amenaza.

- C4 - Uso controlado de privilegios administrativos. La amenaza: una de las formas más comunes en que los atacantes pueden propagarse dentro de una organización objetivo es mediante el uso indebido de privilegios administrativos, lo que sucedió en la práctica realizada en la etapa anterior, el escalamiento de privilegios.

La respuesta: supervisar los privilegios administrativos en computadores, aplicaciones y redes. Utilizar herramientas para rastrear, controlar, prevenir y corregir configuraciones, usos y asignaciones administrativas.

- C5: configuración segura para hardware y software en dispositivos móviles, computadores portátiles, estaciones de trabajo y servidores. La amenaza: la mayoría de los dispositivos están diseñados para una fácil implementación y uso, pero no para la seguridad. Esto los hace vulnerables y explotables, especialmente en su estado predeterminado.

La respuesta: realizar una gestión activa (seguimiento, informe, corrección) de la configuración de seguridad de dispositivos como estaciones de trabajo, computadores portátiles y teléfonos móviles. Emplear la gestión de la configuración para mejorar la seguridad del dispositivo más allá de su estado predeterminado.

- C6: mantenimiento, supervisión y análisis de registros de auditoría. La amenaza: no registrar y analizar correctamente la seguridad permite a los piratas informáticos ocultar sus acciones, ubicación o malware en las máquinas.

La respuesta: Adquirir, administrar y evaluar los registros de auditoría de eventos para detectar un ataque, comprender lo que está sucediendo y luego responder adecuadamente.

Además de los controles de seguridad generales, CIS proporciona a los miembros guías complementarias que se adaptan a dispositivos o plataformas específicos. Así mismo, existen Benchmarks o puntos de referencia de CIS que incluye las mejores prácticas para garantizar una configuración segura de un sistema de tecnología específico. Si bien hay más de 100 puntos de referencia que cubren más de 14 grupos de tecnología, los Benchmarks notables incluyen:

- Sistemas operativos
- Amazon Linux
- Servicios web de Amazon
- Sistema Operativo de Apple
- Cisco
- Escritorio de Microsoft Windows
- Software de servidor
- Base de datos Oracle
- Proveedores de nube
- Servicios web de Amazon
- Plataforma de computación en la nube de Google
- Dispositivos móviles
- IOS de Apple
- Google Android
- Dispositivos de red
- Google Chrome
- Microsoft Office
- Navegador web de Microsoft
- Mozilla Firefox

Como se evidencia anteriormente, se incluyen sistemas operativos, lo cual es importante para contrarrestar lo ocurrido en la práctica de la etapa 3, puesto que se evidenció en el equipo víctima un sistema operativo desactualizado y con varias falencias, así que utilizar los Benchmarks dentro de las labores del Blue Team servirá para prevenir posibles ataques y eliminar vulnerabilidades.

Es importante tener en cuenta que normalmente, un CIS Benchmark se clasifica en uno de dos niveles de perfil:

- Perfil de nivel 1: los protocolos y prescripciones de seguridad básicos. Estos están diseñados para reducir la superficie de ataque de la organización sin afectar la usabilidad y funcionalidad de la máquina.

- Perfil de nivel 2: los perfiles de defensa en profundidad se crean para la máxima seguridad. Pueden afectar negativamente la usabilidad y la funcionalidad de la máquina, especialmente si no son implementadas por profesionales de TI.

En conclusión, es importante aplicar los controles y Benchmarks de CIS a la organización, teniendo en cuenta que se puede estar bajo amenaza constante de ataques cibernéticos y esa amenaza continúa evolucionando. El CIS se creó para ayudar a las organizaciones, tanto grandes como pequeñas, a proteger los datos y

redes. Al unirse y colaborar, los expertos en seguridad pueden adelantarse a los piratas informáticos. Pero, incluso si algún integrante de la organización no desea convertirse en miembro de CIS, es esencial aplicar sus controles de seguridad y Benchmarks para frustrar la gran mayoría de las intrusiones cibernéticas.

5.4.5 **Funciones y características principales de un SIEM**

SIEM significa seguridad de información y gestión de eventos. La tecnología SIEM agrega datos de registro, alertas de seguridad y eventos en una plataforma centralizada para proporcionar análisis en tiempo real para el monitoreo de la seguridad.

Los centros de operaciones de seguridad invierten en software SIEM para optimizar la visibilidad en los entornos de su organización, investigar los datos de registro para la respuesta a incidentes de ataques cibernéticos y violaciones de datos.

5.4.5.1 ¿Cómo funciona SIEM?. Las herramientas SIEM funcionan recopilando datos de eventos y registros creados por sistemas host, aplicaciones y dispositivos de seguridad, como filtros antivirus y firewalls, en toda la infraestructura de una empresa y reuniendo esos datos en una plataforma centralizada. Las herramientas SIEM identifican y clasifican los datos en categorías tales como inicios de sesión exitosos y fallidos, actividad de malware y otras posibles actividades maliciosas.

Luego, el software SIEM genera alertas de seguridad cuando identifica posibles problemas de seguridad. Con un conjunto de reglas predefinidas, las organizaciones pueden configurar estas alertas como de prioridad baja o alta.

Las soluciones SIEM pueden residir en entornos locales o en la nube. Al analizar todos los datos en tiempo real, SIEM utilizan reglas y correlaciones estadísticas para impulsar el conocimiento práctico durante las investigaciones forenses. La tecnología SIEM examina todos los datos y clasifica la actividad de las amenazas de acuerdo con su nivel de riesgo para ayudar a los equipos de seguridad a identificar a los actores maliciosos y mitigar los ciberataques rápidamente.

5.4.5.2 Importancia de SIEM. SIEM es importante porque facilita a las empresas la gestión de la seguridad al filtrar cantidades masivas de datos de seguridad y priorizar las alertas de seguridad que genera el software. El software SIEM permite a las organizaciones detectar incidentes que, de otro modo, podrían pasar desapercibidos. El software analiza las entradas del registro para identificar signos de actividad maliciosa. Además, dado que el sistema recopila eventos de diferentes fuentes en la red, puede recrear la línea de tiempo de un ataque, lo que permite a una empresa determinar la naturaleza del ataque y su impacto en el negocio.

Un sistema SIEM también puede ayudar a una organización a cumplir con los requisitos de cumplimiento mediante la generación automática de informes que incluyen todos los eventos de seguridad registrados entre estas fuentes. Sin el software SIEM, la empresa tendría que recopilar datos de registro y compilar los informes manualmente.

Un sistema SIEM también mejora la gestión de incidentes al permitir que el equipo de seguridad de la empresa descubra la ruta que toma un ataque a través de la red, identifique las fuentes comprometidas y proporcione las herramientas automatizadas para prevenir los ataques en curso.

5.4.5.3 Beneficios de SIEM. Algunos de los beneficios de SIEM incluyen los siguientes:

- Acorta el tiempo que lleva identificar las amenazas de manera significativa, minimizando el daño de esas amenazas.

- Ofrece una visión global del entorno de seguridad de la información de una organización, lo que facilita la recopilación y el análisis de la información para mantener los sistemas seguros.

- Todos los datos de una organización van a un repositorio centralizado donde se almacenan y son fácilmente accesibles.

- Las empresas pueden utilizarlo para una variedad de casos de uso que giran en torno a datos o registros, incluidos programas de seguridad, informes de auditoría y cumplimiento, soporte técnico y resolución de problemas de red.

- Admite grandes cantidades de datos para que las organizaciones puedan seguir ampliando y aumentando sus datos.

- Proporciona detección de amenazas y alertas de seguridad.

- Puede realizar análisis forenses detallados en caso de que se produzcan violaciones importantes de la seguridad.

5.4.5.4 Herramientas y Software SIEM. Algunas de las herramientas que incluyen las siguientes:

- Splunk: Es un sistema SIEM local completo que admite el monitoreo de seguridad y ofrece capacidades avanzadas de detección de amenazas.

- IBM QRadar: Se puede implementar como un dispositivo de hardware, un dispositivo virtual o un dispositivo de software, según las necesidades y la capacidad de la empresa. QRadar on Cloud es un servicio en la nube entregado desde IBM Cloud basado en el producto QRadar SIEM.

- LogRhythm: Es un buen sistema SIEM para organizaciones más pequeñas, unifica SIEM, administración de registros, monitoreo y análisis forense de redes y terminales, así como análisis de seguridad.

- RSA: RSA NetWitness Platform es una herramienta de respuesta y detección de amenazas que incluye adquisición, reenvío, almacenamiento y análisis de datos.

5.4.5.5 ¿Cómo elegir el producto SIEM adecuado?. La selección de la herramienta SIEM adecuada varía según una serie de factores, incluido el presupuesto de una organización y la postura de seguridad. Sin embargo, las empresas deben buscar herramientas SIEM que ofrezcan las siguientes capacidades:

- Informes de cumplimiento.

- Respuesta a incidentes y análisis forense.

- Supervisión del acceso a la base de datos y al servidor.

- Detección de amenazas internas y externas.

- Monitoreo, correlación y análisis de amenazas en tiempo real en una variedad de aplicaciones y sistemas.

- Sistema de detección de intrusiones (IDS), IPS, firewall, registro de aplicaciones de eventos y otras integraciones de aplicaciones y sistemas.

- Monitoreo de la actividad del usuario (UAM).

5.4.6 **Herramientas para contención de ataques informáticos**

A continuación, defino herramientas para contención de ataques informáticos tanto en hardware como en software:

5.4.6.1 Firewall. Un firewall es un dispositivo de seguridad que puede ser hardware, software o ambos, que controla el tráfico tanto de la red entrante como de la saliente y decide de acuerdo con una serie de reglas específicas que la persona encargada de configurarlo define, si se permite o no que dicho tráfico acceda a la red o salga de ésta, los dos tipos principales de reglas de firewall son las reglas de entrada, que se aplican al tráfico de red entrante y las reglas de salida, que se aplican al tráfico de red saliente. Se busca proteger la red empresarial o doméstica contra accesos no autorizados, para preservar la privacidad, salvaguardar la información almacenada en equipos o servidores, prevenir ataques cibernéticos, entre otros.

Los firewalls también juegan un papel importante en el monitoreo, registro y auditoría. A menudo, pueden proporcionar resúmenes a los administradores de red sobre qué tipo y volumen de tráfico han procesado en un período de tiempo determinado. Este es un beneficio importante porque proporcionar este punto de bloqueo puede servir al mismo propósito en su red como lo hace un guardia armado para sus instalaciones físicas. De esta manera, los firewalls pueden ayudar a mantener a los ciberatacantes fuera de una red privada, al tiempo que ofrecen información valiosa sobre quién ha entrado o salido, así como cuándo y por qué lo hicieron.

5.4.6.2 Snort. es el líder de la industria en Sistema de Detección de Intrusos basado en red, pero todavía es de uso gratuito. Este es uno de los pocos IDS que se pueden instalar en Windows. Fue creado por Cisco. El sistema se puede ejecutar en tres modos diferentes y puede implementar estrategias de defensa, por lo que es un sistema de prevención de intrusos (IPS), así como un sistema de detección de intrusos (IDS).

Los tres modos de Snort son:

- Modo sniffer.
- Registrador de paquetes.
- Detección de intrusiones.

Se puede usar snort como un sniffer de paquetes sin activar sus capacidades de detección de intrusos. En este modo, obtiene una lectura en vivo de los paquetes que pasan por la red. En el modo de registro de paquetes, esos detalles del paquete se escriben en un archivo.

Cuando accede a las funciones de detección de intrusos de Snort, invoca un módulo de análisis que aplica un conjunto de reglas al tráfico a medida que pasa. Estas reglas se denominan políticas básicas y si no se sabe qué reglas se necesita, se pueden descargar del sitio web de Snort. Sin embargo, una vez se tenga la confianza en las metodologías de Snort, es posible escribir una regla propia. Hay una gran base comunitaria para este IDS y están muy activos en línea en las páginas de la comunidad del sitio web de Snort. Se puede obtener consejos y ayuda de otros usuarios y también descargar reglas que los usuarios experimentados de Snort han desarrollado.

Los métodos de detección dependen de las reglas específicas que se utilizan e incluyen tanto métodos basados en firmas como en anomalías.

La fama de Snort ha atraído seguidores en la industria de desarrolladores de software. Una serie de aplicaciones que otras casas de software han creado pueden realizar un análisis más profundo de los datos recopilados por Snort.

5.4.6.3 GRR Rapid Response. Es un framework de respuesta a incidentes informáticos. El objetivo de GRR es respaldar los análisis forenses y las investigaciones de una manera rápida y escalable para permitir a los analistas clasificar rápidamente los ataques y realizar análisis de forma remota. Consta de 2 partes: cliente y servidor.

El cliente GRR se implementa en sistemas que se podría querer investigar. En cada uno de estos sistemas, una vez implementado, el cliente GRR sondea periódicamente los servidores de GRR para el trabajo. Lo que significa ejecutar una acción específica: descargar un archivo, listar un directorio, etc.
La infraestructura del servidor GRR consta de varios componen

La infraestructura del servidor GRR consta de varios componentes y proporciona una interfaz gráfica de usuario basada en web y un punto final API que permite a los analistas programar acciones en los clientes, ver y procesar los datos recopilados.

5.4.6.4 Zonas Desmilitarizadas o DMZ. Se hallan dentro de la red interna de la empresa como parte de una red aislada. Por lo general, se ubican allí los recursos o servicios que necesitan accesibilidad desde internet, entre ellos podemos encontrar los servidores web o los de correo.

Pueden ser de tipo hardware o software y su función es no permitir conexiones que vayan desde la zona desmilitarizada a la red local, pero si el acceso a las conexiones generadas tanto de internet, así como de la red local de la organización donde se encuentran las estaciones de trabajo de los empleados. Los servicios de red que son aptos desde internet son más atraídos a vulnerabilidades, lo que permite un alto grado de pérdidas de información, por lo

tanto, al implementar el DMZ como contención a posibles ciberatacantes, arremeterán en primera línea a servicios que no estén en la red local, debido a que las conexiones originarias de la DMZ se hallan bloqueadas.

6 CONCLUSIONES

Sin lugar a dudas es importante contar con un equipo de Blue Team y Red Team, con la utilización de las pruebas de penetración realizadas por los miembros de los equipos mencionados se pueden identificar los aspectos más importantes a la hora de implementar estrategias, técnicas, procesos y procedimientos para mantener un alto grado de seguridad en la información, adicional a lo anterior es evidente que se puede manejar de acuerdo con criterios específicos que van inclinados dependiendo el ámbito de cada organización y lo que se desea obtener.

Existen variedad de herramientas Opensource que permiten a los miembros de los Blue Team y Red Team automatizar los diferentes procesos que conlleva realizar un análisis de vulnerabilidades, su automatización, la gestión de pruebas, la generación de reportes, su análisis y la remediación de las falencias encontradas, esto con el fin de combatir las brechas de seguridad de cualquier organización en donde se lleven a cabo las pruebas de penetración, pero para ello es fundamental que los integrantes de estos equipos se familiaricen con las herramientas, que si no las conocen todas en profundidad por lo menos se familiaricen con ellas, que se capaciten cada día si es el caso puesto que los atacantes no descansan y no pierden la oportunidad de tratar de acceder a la información más importante de la empresa en cualquier momento.

Los simulacros de los Red Team y Blue Team juegan un papel muy importante en cuanto a la protección de la organización contra una amplia gama de ciberataques de los sofisticados adversarios de hoy. Estas actividades ayudan a las empresas a identificar cuáles son los puntos más vulnerables en lo que respecta a sistemas, personas y tecnologías, determinar cuáles son las áreas que se deben mejorar en cuanto a los procesos defensivos y que buscan una respuesta rápida a incidentes en cada fase de la cadena de eliminación, desarrollar la experiencia propia de la organización sobre cómo detectar cualquier ataque dirigido y cómo contenerlo, así como desplegar actividades de respuesta rápida y remediación para devolver a la organización un estado normal de operaciones.

7 RECOMENDACIONES

Sin importar el tamaño o la industria de cualquier empresa, una de las maneras más efectivas y eficientes de revelar vulnerabilidades de la infraestructura y prevenir potenciales amenazas cibernéticas es creer en la experiencia de los Blue y Red Team. Realizar ejercicios de Red Team contra Blue Team puede ser una experiencia sorprendente. Ya sea que se estén evaluando las defensas de ciberseguridad de una organización contra amenazas o evaluando el talento de los miembros del equipo de seguridad, los ejercicios del Red Team contra el Blue Team pueden ser beneficiosos para organizaciones de todos los sectores y tamaños.

Las herramientas mínimas que se recomiendan utilizar a la hora de ejecutar las actividades de los Red Team y Blue Team son Kali Linux, Nmap, Nikto, Openvas, Wireshark y Metasploit, con ello se podrá construir un informe en donde se evidencian las vulnerabilidades a corregir y las soluciones a implementar para mejorar el modelo de seguridad de la organización.

Las técnicas mínimas de un Red Team deben incluir un escaneo de puertos, evaluaciones de vulnerabilidades, pruebas de penetración, ingeniería social incluido el phishing, herramientas de software para interceptar las comunicaciones que pueden ser analizadores de protocolos o rastreadores de paquetes y por último realizar evaluaciones de seguridad física, incluido el seguimiento.

Entre las responsabilidades mínimas del Blue Team se deben incluir el monitoreo de seguridad (redes, sistemas y dispositivos), la evaluación de riesgos, la respuesta a incidentes, la realización de análisis de vulnerabilidades internos y externos, crear, configurar y hacer cumplir las reglas de los firewalls, realizar segmentación de la red, mantener todo el software empresarial actualizado y licenciado, tener escenarios de ciberataques de ingeniería inversa, implementar sistemas de respuesta y detección de puntos finales y desarrollar políticas de remediación para que los sistemas vuelvan a funcionar normalmente después de la intrusión.

Es muy importante utilizar los controles CIS y Benchmarks, esto ayuda a ampliar diferentes técnicas y estrategias que evitan que los atcantes puedan tomar debilidades que a simple vista se puede pensar que no serían útiles para ellos. Generar un hábito de tener los controles mínimos de seguridad, permitirá ir un paso delante de los atacantes, salvaguardar la información es primordial pero para ello se deben utilizar todas aquellas herramientas que se tienen a la mano, también es importante estar capacitando a todo el personal de una organización, puesto que así sea una persona de servicios generales, por allí puede haber una fuga de información cuando se emplea la ingeniería social, por tal motivo se

aconseja crear políticas en donde se hagan capacitaciones periódicas a todo el personal para evitar que se caigan en errores que podrían ser evitables.

BIBLIOGRAFÍA

ALCALDÍA DE BOGOTÁ. [Sitio web]. Bogotá: Guardianes de la Información Penetration Testing. [Consultado: 1 de septiembre de 2021]. Disponible en: http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

BARRERA CUBIDES, Juan Sebastian, et al. Capacidades técnicas, legales y de gestión para equipos red team y blue team. . [en línea]. Seminario Especializado. UNAD, 2021. [Consultado: 1 de septiembre de 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/40286

CASTRO, Carlos. Pruebas de penetración e intrusión. [en línea]. Universidad Piloto de Colombia, 2019. [Consulta: 30 de agosto de 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6273/00005218.pdf?sequence=1&isAllowed=y

COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). De la protección de la información y de los datos. En: Diario Oficial. Enero, 2009. Nro. 47223. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1928 de 2018. (24, julio, 2018). Convenio sobre la Ciberdelincuencia adoptado el 23 de noviembre de 2001 en Budapest. En: Diario Oficial. Julio, 2018. Nro. 50664. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

COLOMBIA. SENADO DE LA REPÚBLICA. Ley 599 de 2000. (24, julio, 2000). De las Normas Rectoras de la Ley Penal en Colombia. En: Diario Oficial. Julio, 2000. Nro. 44097. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

COLOMBIA. SENADO DE LA REPÚBLICA. Ley estatutaria 1581 de 2012. (17, octubre, 2012). Disposiciones generales para la protección de datos personales. En: Diario Oficial. Octubre, 2012. Nro. 48587. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

COPNIA.GOV.CO. [Sitio Web]. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines. [Consulta: 10 de septiembre de 2021]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

EL TIEMPO. [Sitio Web]. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [Consulta: 10 de septiembre de 2021]. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-15141236

ENTER.COM. [Sitio Web]. Detrás de Buggly: La historia de la fachada Andrómeda [Consulta: 10 de septiembre de 2021]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

GUILLÉN ZAFRA, José Luis. Introducción al Pentesting. [en línea]. Universidad de Barcelona 2017. [Consultado: 30 de agosto de 2021]. Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. [Consultado: 30 de agosto de 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

KALI.ORG. [Sitio Web]. The Most Advanced Penetration Testing Distribution. [Consulta: 30 de agosto de 2021]. Disponible en: https://www.kali.org/

LÓPEZ ARBOLEDA, Claudia, et al. Capacidades técnicas, legales y de gestión para equipos blue team y red team. [en línea]. Seminario Especializado. UNAD, 2021. [en línea]. Seminario Especializado. UNAD, 2021. p. 16

NMAP. Nmap Reference Guide [En línea] Disponible en: https://nmap.org/book/man.html

NVD.NIST.GOV. [Sitio Web]. CVE-2014-6287 Detail. [Consulta: 24 de septiembre de 2021]. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2014-6287

OPENVAS.ORG. [Sitio Web]. OpenVAS - Open Vulnerability Assessment Scanner. [Consulta: 31 de agosto de 2021]. Disponible en: https://www.openvas.org/

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

PILLAY, Rishalin. (2019) Learn Penetration Testing: Understand the art of penetration testing and develop your white hat hacker skills. Packt Publishing Ltd. Disponible en: https://books.google.com.co/books?hl=es&lr=&id=t_eaDwAAQBAJ&oi=fnd&pg=PP1&dq=STAGES+OF+PENTESTING&ots=_C7dYCRXn4&sig=fY_Xk6dtx6jXqo6gIA

5laA11ouI&redir_esc=y#v=onepage&q=STAGES%20OF%20PENTESTING&f=false

QUIROZ, Silva y MACIAS, David. Seguridad en informática: Consideraciones. *Revista Científica Dominio de las Ciencias*. 2017, vol. 3, nro. 5, pp. 676-688. ISSN 2477-8818

RAMOS, Jorge. Pruebas de Penetración o Pent Test. *Revista de Información, Tecnología y Sociedad.* 2013, nro. 8. ISSN 1997-4044

Rapid7 Inc. Metasploit [En línea] Disponible en: https://www.metasploit.com/

RUEFLE, Robin. [En línea] Defining Computer Security Incide Response Teams. [Consulta: 3 de octubre de 2021]. Disponible en: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=294557

ROA BUENDÍA, José Fabián. Seguridad Informática. España: McGraw-Hill, 2013.
Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. [Sitio Web]. Anexo 2 – Escenario 2. UNAD. [Consulta: 9 de septiembre de 2021]. Disponible en: https://campus109.unad.edu.co/ecbti95/pluginfile.php/680/mod_folder/content/0/Anexo%202%20-%20Escenario%202.pdf?forcedownload=1

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. [Sitio Web]. Anexo 3 – Acuerdo. UNAD. [Consulta: 9 de septiembre de 2021]. Disponible en: https://campus109.unad.edu.co/ecbti95/pluginfile.php/680/mod_folder/content/0/Anexo%203%20-%20Acuerdo.pdf?forcedownload=1

SENA, Leonardo y TENZER, Simón Mario. Introducción a riesgo informático. Facultad de Ciencias Económicas y de Administración. Universidad de la República de Montevideo. Uruguay, 2004. p.16.

SOLARTE, Francisco; ENRIQUEZ, Edgar y BENAVIDES, Miriam. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL -RTE*. 2015, vol. 28, nro. 5, pp. 492-507.

VOUTSSAS, Juan. Preservación documental digital y seguridad informática. *Investigación bibliotecológica.* 2010, vol. 24, nro. 50. ISSN 2448-8321

Welivesecurity. Penetration Test, ¿en qué consiste?[En línea] Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

ANEXOS

Anexo A. Enlace del Video de Sustentación

http://youtu.be/SqnMjuu3zko?hd=1