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

SANDRA ELIANA CORTES CARIILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CHIQUINQUIRÁ

2021

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

SANDRA ELIANA CORTES CARIILLO

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

JOHN FREDDY QUINTERO

DIRECTOR DE CURSO

ALEXANDER LARRAHONDO NUÑEZ

TUTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CHIQUINQUIRÁ

2021

RESUMEN

El curso Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, se desarrolla en tres (3) unidades, la primera unidad corresponde al contexto ético, legal Red & Blue Team, la segunda unidad hace referencia a los pasos y procesos Red Team y la tercera unidad se enfoca en el análisis y contención en Blue Team.

Las actividades desarrolladas en el presente curso se realizan por etapas; inicialmente se identifican algunos conocimientos previos, mediante la respuesta a una serie de preguntas, establecidas en la guía de la etapa 1 - Conceptos equipos de Seguridad. La evaluación intermedia, se desarrolla mediante tres (3) guías de actividades, correspondientes a la etapa 2 - Actuación ética y legal; etapa 3 - Ejecución pruebas de intrusión y la etapa 4 - Contención de ataques informáticos. Enfocándose en temas relacionados con en el ámbito ético y legal de los equipos Red team y Blue Team, la identificación de los procesos para ejecutar análisis de vulnerabilidades, junto con los métodos de contención Hardenización.

La actividad o evaluación final corresponde a la etapa 5 - Socialización de informe técnico, donde se relacionan los aspectos más importantes del desarrollo de todas las actividades del curso, planteando las recomendaciones y conclusiones que aportan al mejoramiento de las estrategias usadas por Red Team & Blue Team.

Cabe resaltar, que, con el desarrollo de las diferentes actividades del presente curso, se analizan problemas contextualizados, aplicando métodos de identificación y evaluación utilizados en los equipos de Seguridad Red Team y Blue team.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACTIVO INFORMÁTICO[1]: Es cualquier componente, dispositivo o dato del entorno que apuntala actividades afines con la generación de información. Incluyen generalmente software, hardware e información.

ACUERDO DE CONFIDENCIALIDAD[2]: Es un contrato por medio del cual las partes se comprometen a no revelar la información de carácter confidencial que les es suministrada. Dependiendo del contexto, estos acuerdos pueden tener efectos unilaterales o bilaterales.

AMENAZA[3]: es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

ATAQUE INFORMÁTICO[4]: Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red.

BLUE TEAM[5]: Es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva.

CIBERATAQUE[6]: Los ciberataques pueden implicar un equipo muy unido de hackers de élite que trabajan bajo el mandato de un estado nación. Su intención es crear programas

[1] Ciberseguridad sin miedo. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://www.widefense.com/recursos/ciberseguridad/activo-informatico-gerente-cuidar/

[2] Asuntos legales. [Sitio web]. Acuerdos de Confidencialidad. [Consultado 08 de octubre 2021]. Disponible en: https://www.asuntoslegales.com.co/consultorio/acuerdos-de-confidencialidad-2941910

[3] Incibe. [Sitio web]. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [Consultado 08 de octubre 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[4] EcuRed. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

[5] UNIR (La Universidad en Internet). [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[6] tecnologías para los negocios. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en:

que aprovechen fallas previamente desconocidas en el software. Así consiguen filtrar datos confidenciales, dañar infraestructura clave o desarrollar una base para futuros ataques.

CIBERSEGURIDAD[7]: La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el Ciber entorno.

CONFIDENCIALIDAD[8]: Consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que, si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación. Este es uno de los principales problemas a los que se enfrentan muchas empresas; en los últimos años se ha incrementado el robo de los portátiles con la consecuente pérdida de información confidencial, de clientes, líneas de negocio, entre otros.

COPNIA[9]: El Consejo Profesional Nacional de Ingeniería – COPNIA, creado mediante la Ley 94 de 1937, es la entidad pública que tiene la función de controlar, inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional.

CVE[10]: Las Vulnerabilidades y exposiciones comunes (en inglés, Common Vulnerabilities and Exposures, siglas CVE), es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, que versiones del software están afectadas, posible solución al fallo (si existe) o como configurar para mitigar la vulnerabilidad y referencias

https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/

[7] Ciberseguridad. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://sites.google.com/site/jezabelydyddra/concepto

[8] Seguridad Informática. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://infosegur.wordpress.com

[9] COPNIA. [Sitio web]. Quiénes somos. [Consultado 08 de octubre 2021]. Disponible en: https://www.copnia.gov.co/nuestra-entidad/quienes-somos

[10] Wikipedia. [Sitio web]. Common Vulnerabilities and Exposures. [Consultado 08 de octubre 2021]. Disponible en: https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se demuestra su explotación.

DISPONIBILIDAD[11]: Se define como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios.

EXPLOIT[12]: Es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

HARDENING[13]: Hardening o también llamado endurecimiento informático, es el término que se le da al proceso de reducción de vulnerabilidades en el sistema. Esto se consigue, estableciendo unas medidas de seguridad con el objetivo de estar preparados ante un ataque informático.

INTEGRIDAD[14]: Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

PENTESTING[15]: Es una abreviatura de las palabras inglesas “penetration” y “Testing”, que significa test. Pentesting o Penetration Testing es la práctica de atacar diversos

[11] Seguridad Informática. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://infosegur.wordpress.com

[12] Dragoit. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://dragoit.com/blog/definicion-de-exploit-que-son-y-como-funciona/

[13] CISET. Hardening. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening?dt=1634086164526

[14] Seguridad informática. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://infosegur.wordpress.com

[15] Openwebinars. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://openwebinars.net/blog/que-es-el-pentesting/

entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.

PURPLE TEAM[16]: Existen para asegurar y maximizar la efectividad de los equipos rojo y azul. Lo hacen integrando las tácticas y controles defensivos del Blue Team con las amenazas y vulnerabilidades encontradas por el Red Team. Idealmente, no debería ser un equipo, sino una dinámica de cooperación entre los equipos rojo y azul.

RED TEAM[17]: Es un servicio en el cual, el scope o alcance es muchísimo más amplio y rico en relación con los activos y el tiempo para modelar los escenarios de ataque. Un servicio gestionado de Red Team no suele estar limitado en tiempos ni en infraestructura y aplicaciones a probar, y normalmente la ejecución de este suele ser tanto externo como interno, dando como resultado que el testeo de la postura de seguridad de la compañía sea mucho más real y completa que un penetration test tradicional.

VIRTUALBOX[18]: Es un software de virtualización para arquitecturas x86/amd64. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización.

VULNERABILIDAD[19]: es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

[16] UNIR (La Universidad en Internet). [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[17] BlackmantiSecurity. [Sitio web]. [Consultado 08 de octubre 2021]. Disponible en: https://www.blackmantisecurity.com/introduccion-al-red-team-parte-1/

[18] Wikipedia. . [Sitio web]. VirtualBox. [Consultado 08 de octubre 2021]. Disponible en: https://es.wikipedia.org/wiki/VirtualBox

[19] Incibe. [Sitio web]. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [Consultado 08 de octubre 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INTRODUCCIÓN

El presente informe técnico, contiene inicialmente hace referencia a la consulta y comprensión sobre la legislación de los delitos informáticos y ciberseguridad en Colombia; asimismo, en el presente informe se definen las etapas de las pruebas de penetración (pentesting) y algunas herramientas de ciberseguridad, reconociendo el escenario 1 correspondiente a la situación problema: montaje banco de trabajo, para el posterior análisis y configuración lo solicitado en la presente actividad.

El desarrollo de la segunda actividad se realiza, teniendo en cuenta la situación problema expuesta en el anexo 2, escenario 2 y el anexo 3 Acuerdo de confidencialidad. Por lo tanto, en el presente documento se genera el respectivo análisis legal y ético con relación a los casos en mención, señalándose los procesos ilegales y no éticos que se estipulan en el acuerdo en mención. De igual manera, en esta actividad, se presenta un análisis al caso a que hace referencia la noticia “OPERACIÓN ANDROMEDA BUGGLY” presentada en ciudad de Bogotá.

La actividad correspondiente a la etapa 3, consiste en identificar y analizar la situación problema Red Team, expuesta en el anexo 4- escenario 3 y teniendo en cuenta el banco de trabajo configurado previamente en la etapa 1 del presente seminario, en este documento se presenta un informe sobre las herramientas y procedimientos utilizados para dar solución al escenario en mención, el análisis sobre la solución al fallo identificado, indicando las herramientas utilizadas para identificar los fallos. Asimismo, se presenta un análisis del ataque presentado en cada una de las máquinas, junto con un informe sobre la explotación de las vulnerabilidades identificadas en el escenario 3 del anexo 4.

La actividad correspondiente a la etapa 4, consiste en identificar y analizar la situación problema Red Team, expuesta en el anexo 5- escenario 4 referente a equipo Blueteam y teniendo en cuenta el banco de trabajo configurado previamente en las anteriores etapas del presente seminario, en este documento se presenta un informe con el análisis de las acciones necesarias para contener un ataque en tiempo real, acciones de Hardenización a implementar para evitar que sucedan ataques de seguridad informática, análisis sobre las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos, análisis sobre la pertinencia de trabajar con CIS “Center For Internet Security” como propuesta de aseguramiento por parte de un equipo de Blue Team; análisis sobre las funciones y características principales de un SIEM y la elección de 3 herramientas que permitan contener ataques informáticos.

Finalmente, teniendo en cuenta el anexo 6 – escenario 5, el presente informe técnico relaciona y contiene los aspectos relevantes del desarrollo de las actividades correspondientes al curso Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team &Blue Team.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Planificar estrategias basadas en metodologías de ciberseguridad defensivas y ofensivas, que permitan hacer frente a un evento o incidente informático en una infraestructura TI, teniendo presente el cumplimiento de normas éticas y legales con el fin de mejorar el esquema de ciberseguridad de una organización.

1.2 OBJETIVOS ESPECÍFICOS

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.
- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

2 DESARROLLO DEL INFORME

2.1 ETAPA 1: CONCEPTOS EQUIPOS DE SEGURIDAD

2.1.1 Escenario 1: Situación Problema

Montaje banco de trabajo

The Whitehouse Security requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de The Whitehouse Security. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso. De manera simultánea The Whitehouse security requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

2.1.2 Análisis de la Legislación Relacionada con Delitos Informáticos y Protección de Datos Personales en Colombia

2.1.2.1 Ley 1273 de 2009

Por medio de la ley 1273 de enero 05 de 2009, el Congreso de la República de Colombia modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado “De la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[20]

Asimismo, la tipificación o clasificación de los delitos informáticos en Colombia se encuentran establecidos en la ley 1273 del 2009, en la cual se decreta en su artículo primero adición de los siguientes artículos en el código penal; en el capítulo primero, dicha hace referencia a los atentados contra la confidencialidad, la integridad y la

[20] COLOMBIA.CONGRESO DE LA REPÚBLICA. Ley 1273 (05, enero, 2009). “Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado- denominado “De la protección de la información y de los datos” y se preservan integralmente los sistemas que usen las tecnologías de la información y de las comunicaciones, entre otras disposiciones”. Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

disponibilidad de los datos y de los sistemas de información, denotándose de la siguiente manera:

- **Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.**
- **Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.**
- **Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.**
- **Artículo 269D. DAÑO INFORMÁTICO.**
- **Artículo 269E. USO DE SOFTWARE MALICIOSO.**
- **Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.**
- **Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.**
- **Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.**

De igual manera, la ley antes indicada, en su capítulo segundo hace referencia "De los atentados informáticos y otras infracciones", adicionando los siguientes artículos:

- **Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.**
- **Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.**

Cabe resaltar, que mediante la ley 1273 de 2009 se implementa el tratamiento digital de la información, teniendo en cuenta los principios de la seguridad informática, es decir, la integridad, disponibilidad y confidencialidad de la información.

2.1.2.2 Ley 1581 de 2012

Esta Ley estatutaria colombiana 1581, de fecha octubre 17 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", es reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada parcialmente por el decreto 1081 de 2015.[21]

La Ley 1581 del 2012, trata de la autorización del tratamiento de los datos personales de una persona, como son: Datos básicos, documentos de identidad, fechas de expedición, dirección de habitación, teléfono, profesión, asociaciones, contratos, entre otros. Cabe resaltar, que, a partir de la implementación de esta ley, toda la recolección de dicha información debe ser notificada y la persona debe autorizar el tratamiento de sus datos y tomar conciencia de que se suministra información delicada, además conocer para que,

[21] COLOMBIA.CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). "Por la cual se dictan disposiciones generales para la protección de datos personales.". Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

el uso y donde se registra la información en mención. El objetivo primordial a que hace referencia esta ley corresponde al derecho constitucional que tiene todas las personas a conocer, actualizar y rectificar la información suministrada y registrada en bases de datos o archivo.

Por medio de esta ley el Congreso de Colombia dicta las disposiciones generales para la protección de datos personales, decretando treinta (30) artículos, los cuales se encuentran distribuidos en nueve (9) títulos, dentro de los cuales el título 2 “principios rectores” Articulo 4, se caracteriza por que hace referencia a los principios para el tratamiento de datos personales, el cual dice así:

“Artículo 4°. Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;

c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;

f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

g) Principio de seguridad: La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."[22]

La ley 1581 de 2012, es reglamentaría y por ende está sujeta a lo decretado en la misma. Así mismo, esta ley hace referencia a las categorías especiales de los datos, derechos y condiciones de legalidad para el tratamiento de datos, procedimientos para consultas, reclamos, deberes de los responsables del tratamiento y de los encargados del tratamiento de los datos.

2.1.3 Etapas de las Pruebas de penetración o Pentesting

Las pruebas de penetración y/o pentesting, son los procesos por medio del cual se detectan las vulnerabilidades en un sistema de información de una organización, con el fin de corregirlas y evitar los ataques.

En la siguiente tabla se describen las etapas y/o fases de Pentesting.

[22] COLOMBIA.CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). "Por la cual se dictan disposiciones generales para la protección de datos personales.". Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Tabla 1. Etapas y/o fases de Pentesting

ETAPAS / FASES DE PENTESTING	DESCRIPCIÓN
Recolección de Información	En este proceso se reconoce y se obtiene toda la información de la organización, identificando los sistemas y programas.
Análisis de Vulnerabilidades	En esta fase se analiza toda la información recolectada en la anterior fase, identificando las vulnerabilidades o posibles vectores de ataques de los sistemas.
Explotación de vulnerabilidades	A partir de los resultados obtenidos de las anteriores etapas, se inicia el acceso a los sistemas de la organización, ejecutando exploits contra las vulnerabilidades identificadas o utilizando credenciales obtenidas para el acceso a los sistemas.
Post – explotación	En esta etapa, se intenta entrar al sistema vulnerado e insistiendo en conseguir credenciales o permisos de administradores o incluso vulnerar otros sistemas con más importancia dentro de la organización, por medio de técnicas de pivoting u otras.
Informes	Una vez finalizadas todas las etapas anteriores, se documenta todo lo realizado en un informe, en donde se especifica los procesos realizados en el test de intrusión, como las herramientas y técnicas utilizadas, mencionando las vulnerabilidades encontradas.

Fuente: Sandra Cortes

2.1.4 Herramientas y Servicios Utilizados en Ciberseguridad

2.1.4.1 Herramientas

2.1.4.1.1 Metasploit

(Open Webinars, 2018) menciona a metasploit framework como “Metasploit framework es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad y equipos Red Team y Blue Team. Red Team es el equipo ofensivo o encargado del hacking ético, que hace pruebas de intrusión, mientras que el Red Team es el equipo que lleva a cabo la securización y toda la parte defensiva”.

Este framework cuenta con la inclusión de varios exploits, los cuales atacan permiten atacar vulnerabilidades conocidas a través de payloads. Estos últimos son los fragmentos de código que se ejecutan.

Esta herramienta es utilizada en la etapa de explotación de las vulnerabilidades, una vez estas sean identificadas, junto con los servicios. Cabe anotar, que inicialmente se debe probar si las vulnerabilidades identificadas permiten al ciberdelincuente realizar un ataque y luego conocer cuál sería el daño dentro de la organización, en cuanto a los sistemas de información de la misma.

Metasploit es una herramienta que permite hacer pruebas, ya que esta presenta una base de exploits, permitiendo su ejecución y simulando las consecuencias que posteriormente se puedan presentar en caso de un ataque.

Puede ejecutarse en varios sistemas operativos, es decir es una aplicación multiplataforma, Windows, Linux. Así mismo, al contar con la búsqueda de varios módulos de explotación, puede utilizarse en una gran cantidad de motores de bases de datos.

La herramienta metasploit puede abrirse en Windows directamente desde el menú inicio como “Metasploit Console” y en Linux se puede ejecutar con la utilización del comando: sudo msfpro.

En esta herramienta se diferencian las siguientes:

- Metasploit pro- 3.5
- Metasploit Express 4.0
- Metasploit framework

2.1.4.1.2 Nmap

Esta herramienta es un programa de código abierto que busca puertos abiertos y describe los servicios que están operando en él, fue desarrollado por Gordon Lyon (más conocido por su alias Fyodor Vaskovich), es una herramienta que originalmente fue desarrollada para Linux, pero hoy en día es multiplataforma.

De igual manera, esta herramienta permite realizar auditoria de seguridad y se utiliza en la explotación de redes como en equipos personales. Actualmente, es utilizada en temas de seguridad ya que ofrece información detallada acerca de lo que sucede con los puertos abiertos que un sistema operativo presenta.

La utilización de esta herramienta es muy fácil e intuitiva, ya que con facilidad se puede obtener información de un computador con unos simples comandos y de esta misma manera es que los delincuentes logran enterarse de las debilidades y encuentran la oportunidad perfecta para realizar ataques y lograr hacer daño.

2.1.4.1.3 OpenVAS

Open Vulnerability Assessment System por sus siglas en inglés, es un compendio de software, que ofrece para el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos. Esta herramienta es de uso libre; cuenta con una interfaz web que posibilita y ofrece una ayuda sencilla para escanear las vulnerabilidades de un sitio web que contenga variados servicios, entre ellos las bases de datos.

Puede ser instalados en varios sistemas operativos, Windows, Mac OS y distribuciones Linux.

- Escaneo concurrente de múltiples nodos.
- Saporta SSL
- Saporta para WMI
- Escaneo automático temporizado.
- Reportes en múltiples formatos (XML, HTML, LaTeX, entre otros)
- Servidor web integrado.

OpenVAS cuenta con un entorno grafico a través de un navegador Web, por lo cual se diligencia un “formulario” en la sección de configuración, en el cual solicita la IP del Host a ser escaneado. De esta manera al ejecutar esta tarea, se obtendrán los resultados de las vulnerabilidades presentes.

2.1.4.2 Servicios en Línea

2.1.4.2.1 Exploit DB

Es un proyecto que presenta un repositorio de exploits gratuitas y públicas, con software vulnerable disponible para fines de investigación de vulnerabilidades y pruebas de penetración.

2.1.4.2.2 CVE (Common Vulnerabilities And exposures).

Es un programa que hace referencia a la lista de vulnerabilidades y exposiciones comunes, identificadas y catalogadas como las vulnerabilidades de ciberseguridad, las cuales son divulgadas de manera pública.

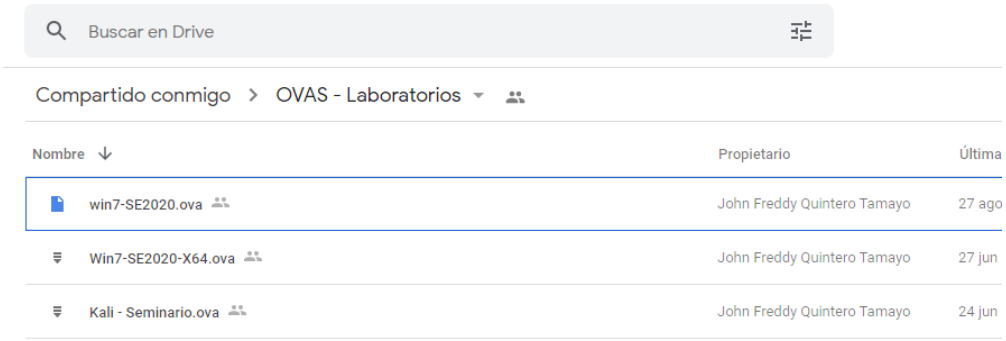
La lista de vulnerabilidades en ciberseguridad, se identifican con un numero CVE-ID, describiendo la vulnerabilidad con las versiones de software afectadas, dando una posible solución al riego o fallo que se presenta, con la configuración para mitigar dicha vulnerabilidad. De igual forma, indica los enlaces sobre la información de la base de datos de vulnerabilidad del NIST, donde se muestra los detalles de la vulnerabilidad.

2.1.5 Implementación Del "Banco De Trabajo" En Un Entorno Local

A continuación, se evidencia la instalación de las tres máquinas virtuales:

Se inicia descargando los sistemas virtualizados provistos por el tutor, así como lo muestra Fig. 1.

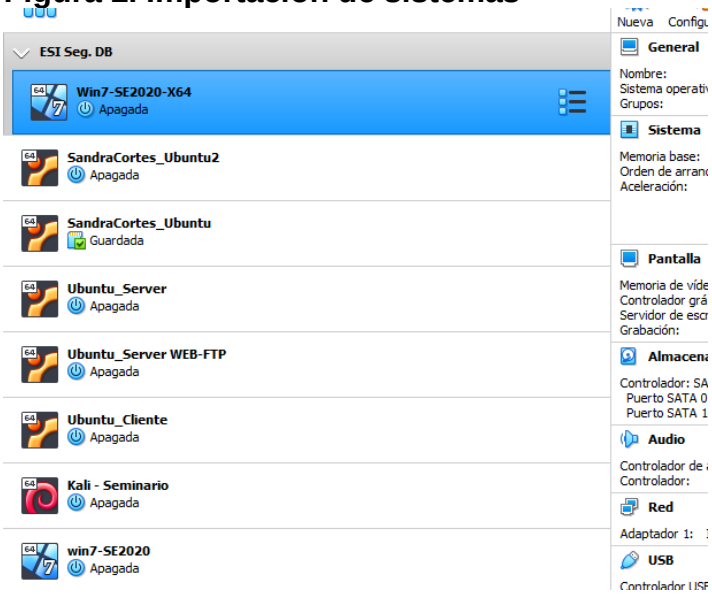
Figura 1. Descarga de sistemas



Fuente: Sandra Cortes

Posteriormente se importan en la herramienta VirtualBox, así como se muestra en la Fig. 2.

Figura 2. Importación de sistemas

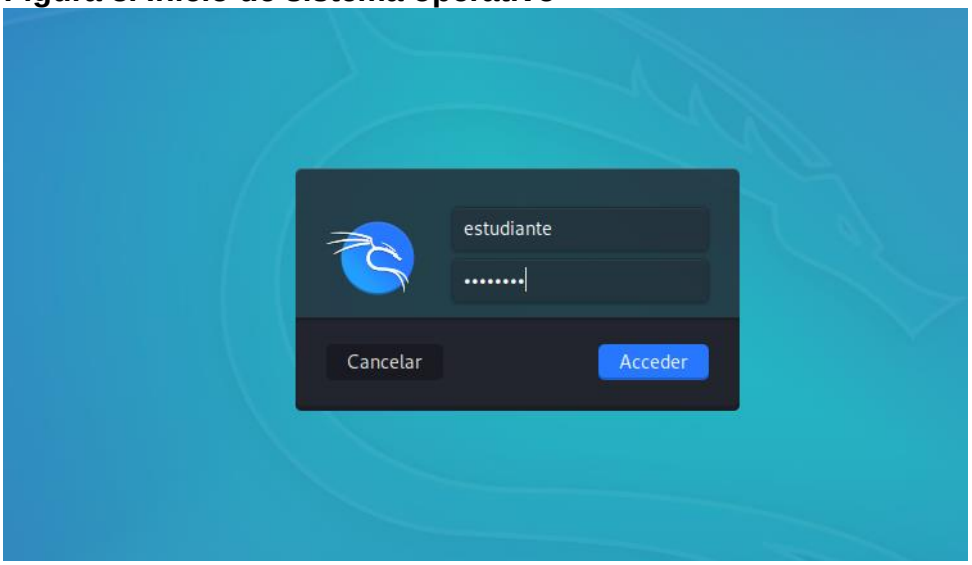


Fuente: Sandra Cortes

Ahora, se inicia el Sistema Operativo Kali – Seminario con los datos de logueo provistos:

User: estudiante
Password: unad2020

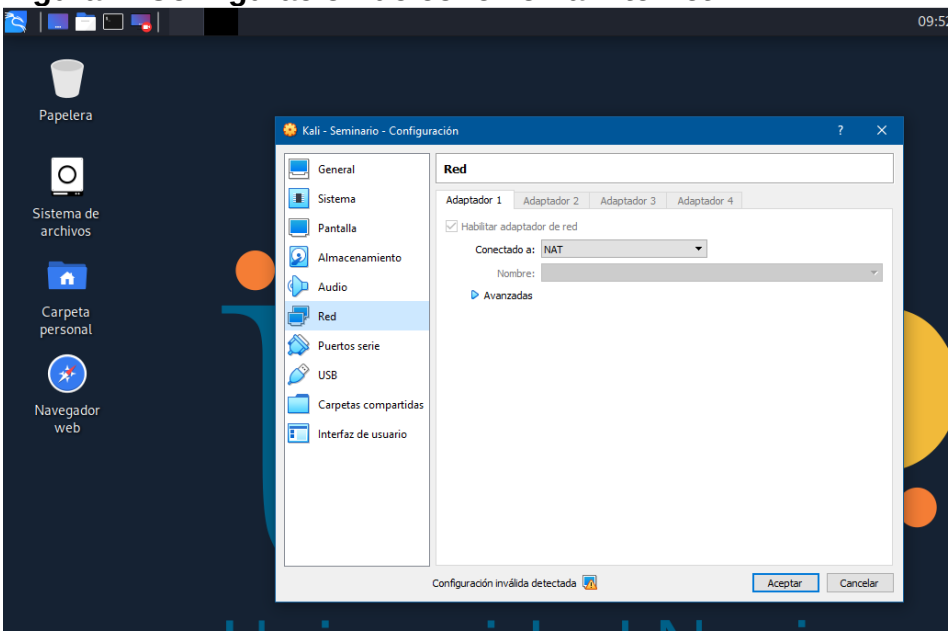
Figura 3. Inicio de sistema operativo



Fuente: Sandra Cortes

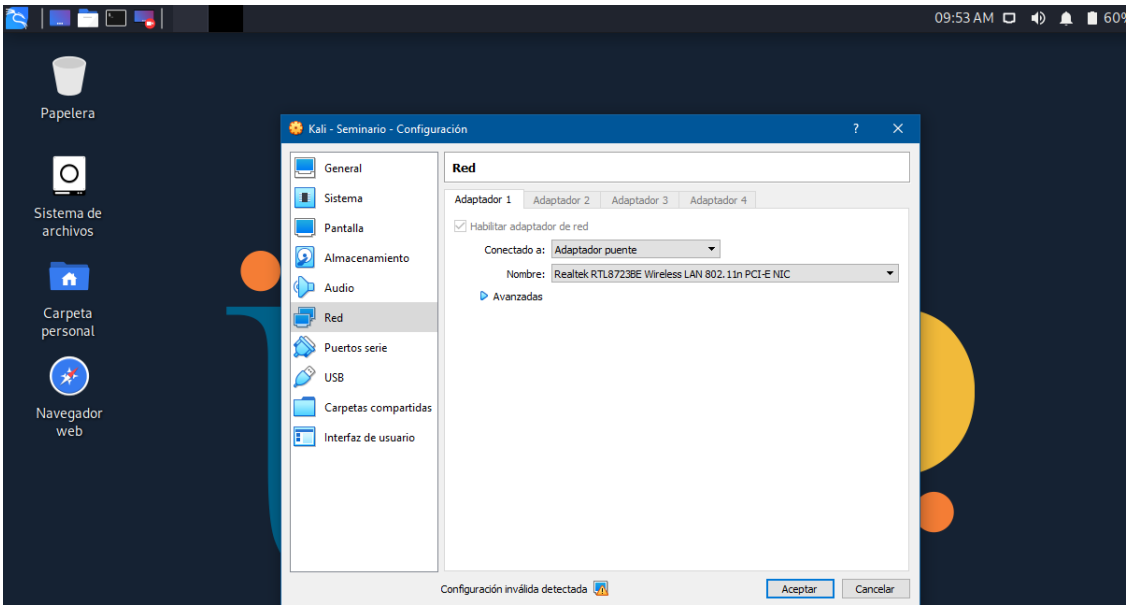
Posterior a ello, se configura la conexión a internet dentro del sistema operativo, como lo muestra la Fig. 4.

Figura 4. Configuración de conexión a internet



Fuente: Sandra Cortes

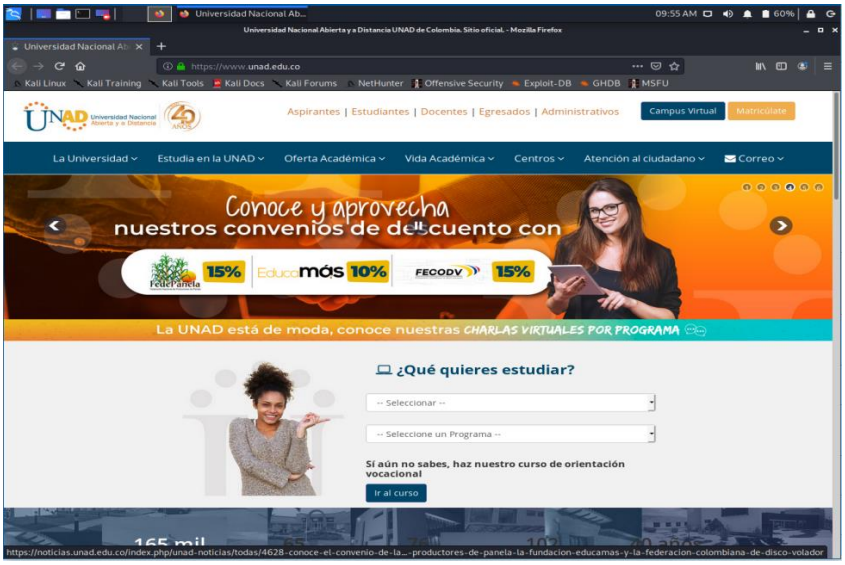
Figura 5. Configuración de conexión a internet



Fuente: Sandra Cortes

Ahora, se comprueba que tenga una conexión activa, así como lo muestra a continuación la Fig. 6.

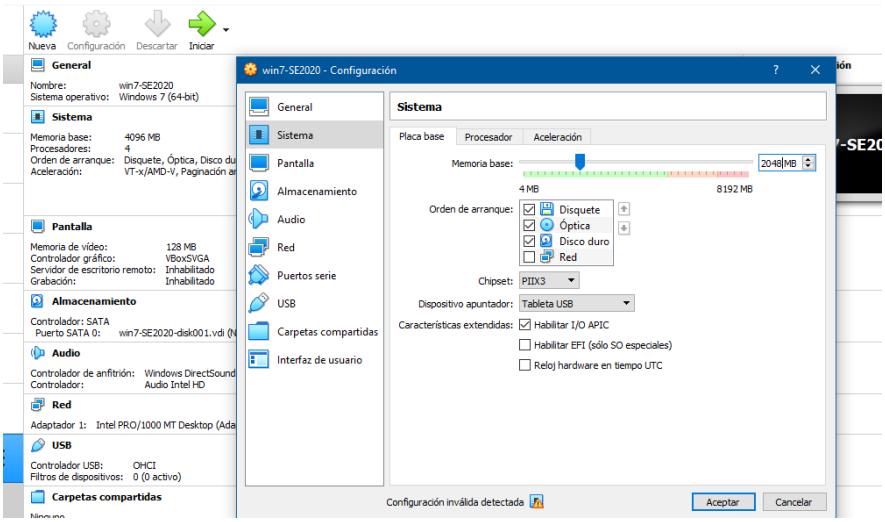
Figura 6. Verificación de existencia de una conexión activa



Fuente: Sandra Cortes

Al momento de iniciar los S.O de Windows se evidencia de que éstos fueron configurados con 4GB de RAM, pero debido a las características de la máquina física se hizo una reducción de memoria RAM a 2GB para ambos sistemas Windows.

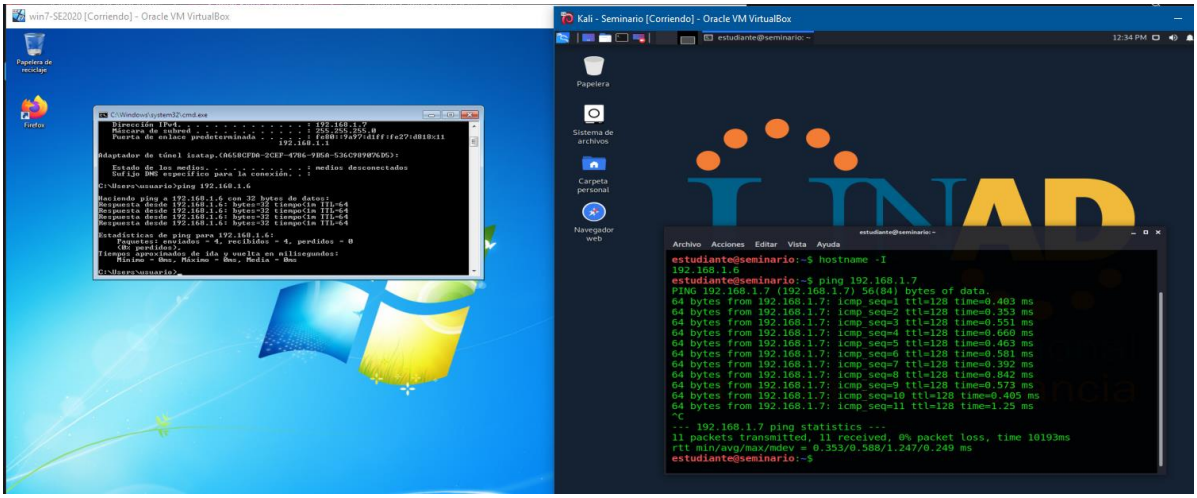
Figura 7. Reducción de memoria RAM



Fuente: Sandra Cortes

Al ejecutar la máquina *Windows 7 de 32 bits*, estaba configurada de manera satisfactoria en la red, por lo que se procede a verificar la comunicación entre las máquinas ***Windows 7 32 Bits y Kali Linux*** por medio del comando *PING.*

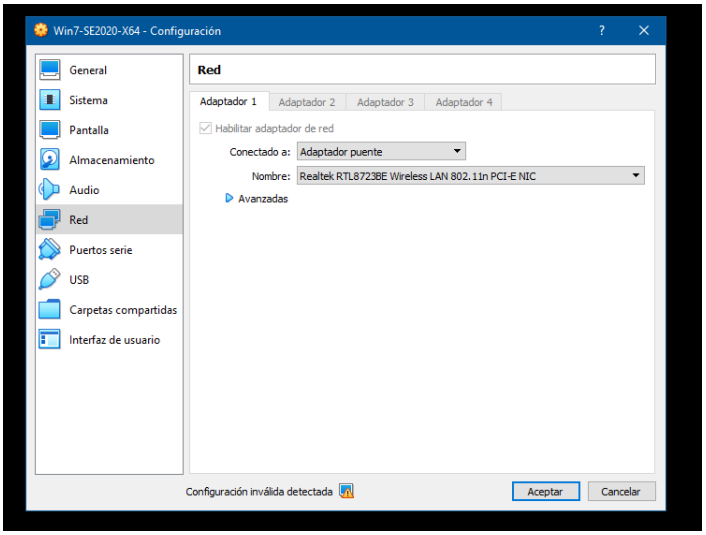
Figura 8. Verificación de la comunicación entre las dos máquinas



Fuente: Sandra Cortes

Al iniciar la máquina *Windows 7 64 Bits* no se encuentra configurada en la red, por lo que se procede a configurarla.

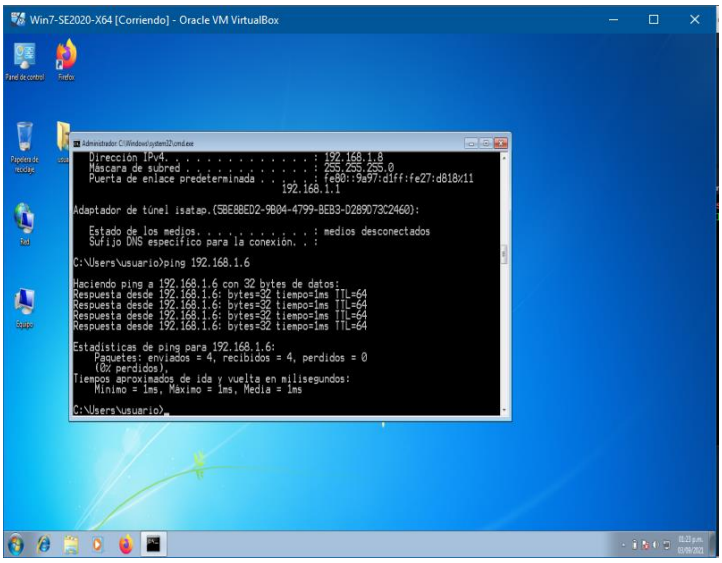
Figura 9. Configuración en la red de la máquina Windows 7



Fuente: Sandra Cortes

Posteriormente, se verifica que haya comunicación con la Máquina Kali, así como se muestra a continuación en la Fig. 10.

Figura 10. Verificación de comunicación la máquina Kali Linux



Fuente: Sandra Cortes

Tabla 2. Especificaciones del hardware de las máquinas

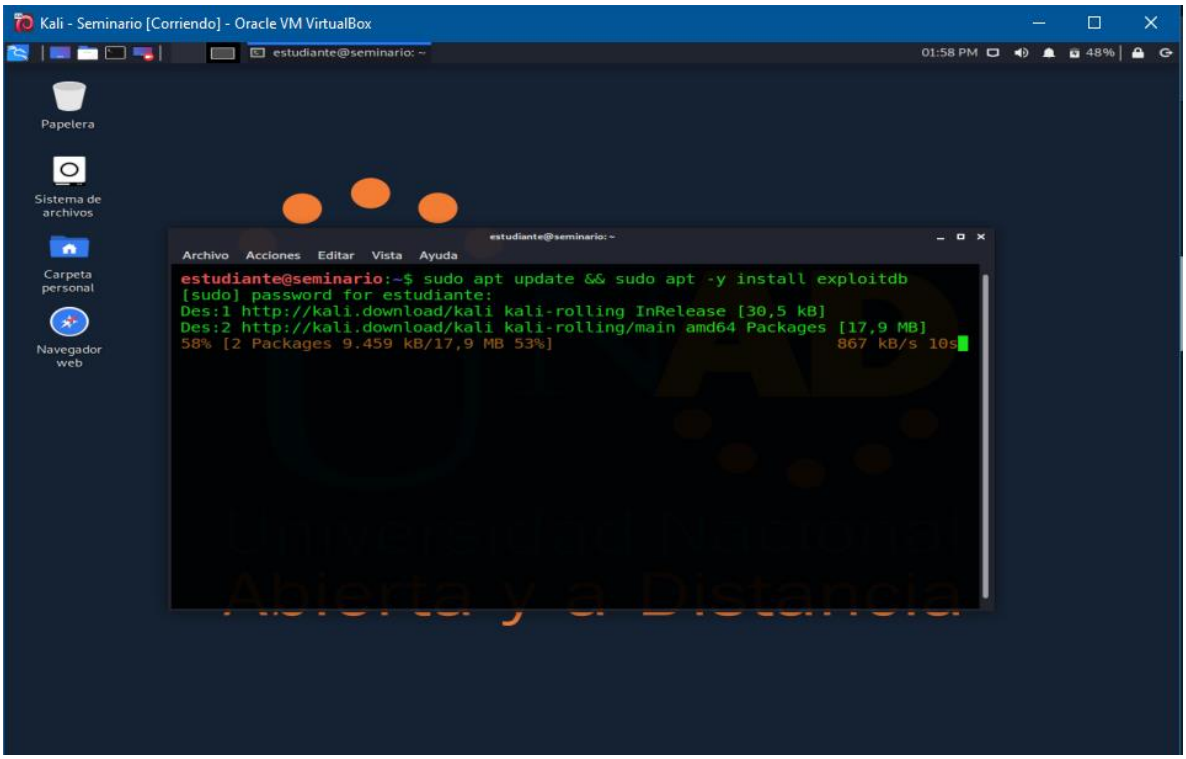
	Máquina Física			
		Máquina 1	Máquina 2	Máquina 3
Sistema Operativo	Windows	Debian	Windows	Windows
Versión	10 pro-64 Bits	Kali 64 Bits	7 Professional 32 Bits	7 Professional 64 Bits
Almacenamiento principal	8 GB RAM	2 GB RAM	2 GB RAM	2 GB RAM

Fuente. Sandra Cortes

2.1.5.1 Configuración

Se procede a la instalación de Explotaba, así como se muestra en la siguiente Figura.

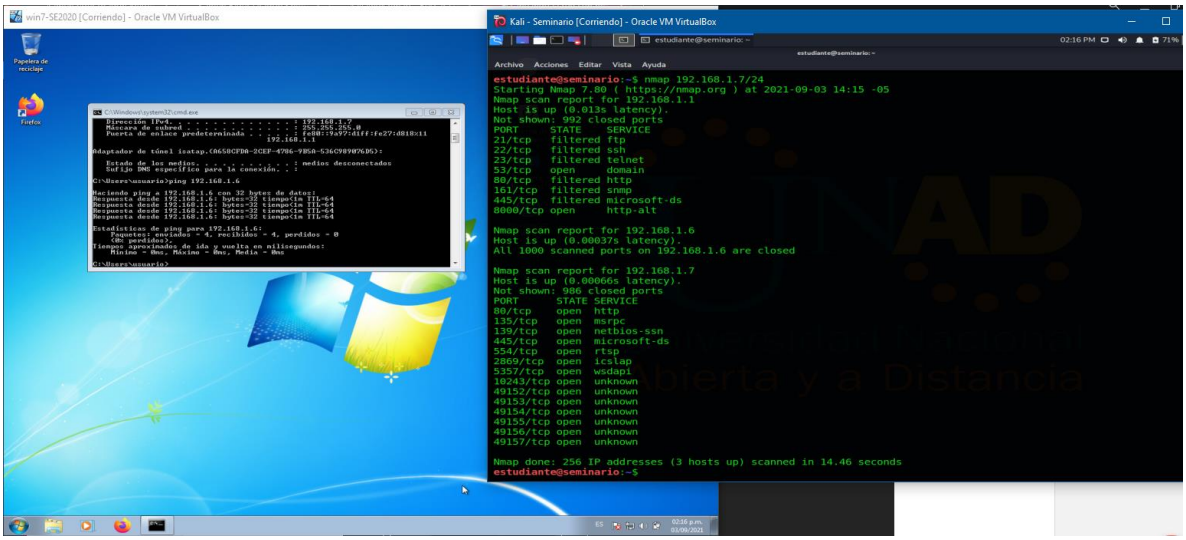
Figura 11. Instalación de Explotaba



Fuente: Sandra Cortes

Se hace uso de la herramienta Nmap para escanear la máquina Windows 7 32 Bits desde Kali Linux, así como se muestra en la siguiente Figura.

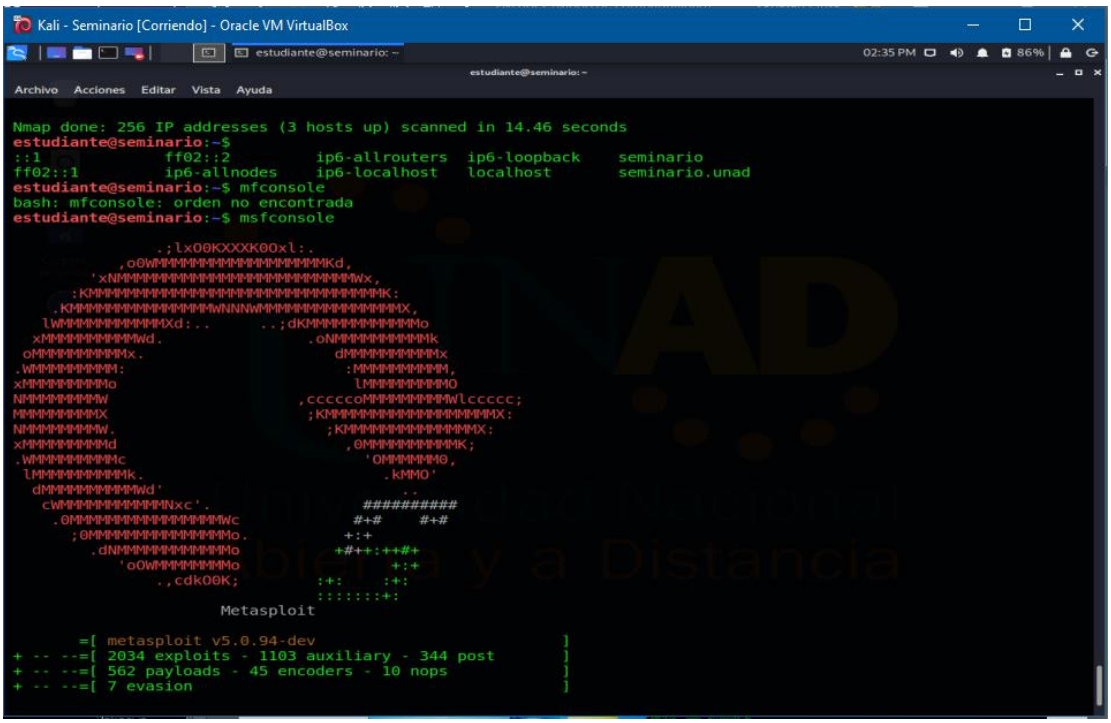
Figura 12. Escaneo de la máquina Windows 7 desde Kali Linux



Fuente: Sandra Cortes

Verificar metasploit dentro de la máquina virtual, así como se muestra a continuación en la Fig. 13.

Figura 13. Verificación de Metasploit



Fuente: Sandra Cortes

2.2 ETAPA 2: ACTUACIÓN ÉTICA Y LEGAL

2.2.1 Escenario 2

Situación problema: Análisis legal.

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

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

2.2.2 Acuerdo de Confidencialidad

Situación Problema: Análisis Legal.

ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y WHITEHOUSE SECURITY

Por la parte reveladora

Nombre: The WhiteHouse Security

Dirección: EE. UU

Teléfono: 1100011100

E-mail: Info@Thewhitehousesecurity.com

Por la parte **receptora de la información**

Nombre: Nombre estudiante

Dirección:

Teléfono:

E-mail:

Identificación del proyecto

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

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

2. Que la información de propiedad de Whitehouse Security Whitehouse Security ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

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

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

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

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

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

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Como Parte Receptora:

_____

Nombre del estudiante.

Estudiante UNAD.

C.C. No. de

Por la parte reveladora:

_____

Nombre Gerente de la empresa

Whitehouse Security

C.C. No. De

2.2.3 Análisis Legal y no Ético con Respecto a la Situación Problema Escenario 2 y el Acuerdo de Confidencialidad

2.2.3.1 Escenario 2

Teniendo en cuenta que el contrato es elaborado por un abogado que ya no labora con la organización, el cual fue despedido por encontrar algunos procesos ilícitos; inicialmente, con este hecho se evidencia un proceso sospechoso ilegal, ya que, este contrato debería haber sido elaborado y redactado por un profesional en derecho (abogado) con experiencia en contratación que estuviese laborando para la organización contratante.

Asimismo, en esta situación se evidencia que la alta gerencia de la organización no revisa los contratos del personal; actuación con la que se detecta que la alta gerencia no está cumpliendo con sus principales funciones, esto con el fin de no verse implicado en investigaciones.

2.2.3.2 Acuerdo de confidencialidad

Con relación a la situación planteada en el anexo 3, Acuerdo de confidencialidad, a continuación, se mencionan las cláusulas donde se evidencian procesos ilegales y no éticos.

En la **cláusula pprimera,** hace referencia a que la parte receptora, **se obliga a no divulgar directa, indirecta**, la **información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados**. Con esta cláusula se estaría incumpliendo con el código de ética y la dignidad de los profesionales, ya que está obligando a la parte receptora, a no informar sobre los hechos ilegales, incluso ni a las autoridades legales.

Con respecto a la cláusula **Segunda. Definición de información confidencial,** hacen referencia a que se entiende como Información Confidencial, para los efectos de dicho acuerdo, **datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos";** en esta cláusula se evidencia que algunos datos a que hacen mención en esta cláusula no son clasificados como confidenciales, puesto que algunos de ellos se catalogan ilegales ante la ley.

En la cláusula **Cuarta: Obligaciones de la parte receptora,** en el numeral 3 hace referencia a "**No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros";** lo cual indica que el profesional correspondiente a la parte receptora que cumpla con esta acción ilegal estaría violando el código de ética y buen nombre**.** De igual manera, en la cláusula cuarta, en el numeral 4 indica: "Abstenerse **de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas",** con esta obligación, el profesional que llegase a realizar esta acción estaría actuando ilícitamente y violando la ley.

Igualmente, el numeral 7 de la cláusula cuarta dice "**Responder por el mal uso que le den sus representantes a la información confidencial";** esta obligación se debe revisar, ya que en esta cláusula estamos hablando de las "**Obligaciones de la parte receptora",** por lo que creo que esta debe ser una responsabilidad de la parte reveladora y cada profesional es responsable de la información a su cargo.

En el numeral 9 de esta misma clausula cuarta, indica que La **parte receptora esta obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal** sin el previo consentimiento por escrito por parte de Whitehouse Security; con esta obligación se esa incumpliendo la ley, ya que toda información ilegal debe ser remitida a los entes de control, de lo contrario el profesional estaría infringiendo la ley , con la vinculación a la respectiva investigación.

En la **cláusula octava. Solución de controversias,** hace referencia que en caso de que la información ilegal o confidencial sea encontrada en manos del receptor, este debe acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security. Con esta cláusula se videncia las malas intenciones del acuerdo, ya que la parte reveladora no tendría en conclusión ninguna responsabilidad y en caso de que se presentara dicho caso, toda la responsabilidad recaería sobre el profesional especializado en seguridad informática que es la parte receptora.

En conclusión, con la celebración del convenio se estaría actuando ilegalmente tanto de la parte receptora como la parte reveladora.

2.2.4 Análisis de la Situación Problema y el Acuerdo de Confidencialidad con relación a los artículos vulnerados de la ley 1273 de 2009

Teniendo en cuenta la ley 1273 de 2009, el acuerdo de confidencialidad vulnera los siguientes artículos:

- **Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

  Con la cláusula segunda de dicho acuerdo, se está vulnerado el presente artículo 269A, ya que con la cláusula se d**efine la información confidencial, como: 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**".

  Asimismo, en esta cláusula segunda menciona que si la **parte receptora**, es decir el profesional en seguridad informática, tiene conocimiento de la información antes indicada o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados, esta también es información confidencial para la organización. Por lo tanto, con el acuerdo en mención, se está vulnerando la ley 1273, ya que cataloga la información ilegal como confidencial y, por ende, prohíbe publicar y denunciar la información ilegal que resulte de reuniones.

- **Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO.** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Esta cláusula se está vulnerado, por cuanto dicho acuerdo no permite divulgar los procesos ilegales que se presentan en la organización, los cuales pueden impedir y obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos contenidos en algún sistema de la misma organización.

- **Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

  Esta cláusula se vulnera con el acuerdo de confidencialidad en mención, por cuanto, en su clausula segunda define información confidencial de la organización **datos secretos como datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos.**

- **Artículo 269D. DAÑO INFORMÁTICO.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

  De igual manera, con el acuerdo de confidencialidad, se está vulnerando el articulo antes indicado de la ley 1273 de 2009, ya que, como antes se indicó, en dicho acuerdo se define la información confidencial de la organización de manera errónea, sin tener en cuenta lo indicado en la ley 1273 de 2009.

- **Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

  Cabe resaltar, que manipular de alguna forma los datos personales almacenados en las bases de datos, sistemas, entre otros, para bien propio o de algún tercero, sin estar autorizado y/o facultado está violando la ley, por tanto, el acuerdo de confidencialidad ante indicado, al no permitir denunciar actividades sospechosas o ilegales como espionaje, está contribuyendo a que se apropien de información de terceros y de esta manera la parte reveladora del acuerdo es decir los

representantes de la organización, serían los responsable del mal uso que se le da a la información confidencial.

2.2.5 Análisis y revisión de la propuesta laboral con respecto al punto de vista legal y ético

Teniendo en cuenta, el Código de Ética para Ingenieros (COPNIA), como Ingeniera de Sistemas, estudiante de la especialización en seguridad informática y una vez revisado el contrato y/o acuerdo, no aplicaría para dicha propuesta de trabajo ofertada por la organización The WhiteHouse Security, la cual tiene dispuesto un sueldo de quince millones de pesos colombianos mensuales ($15´000.000), con un contrato de por vida, ya que si tenemos en cuenta, el acuerdo y/o contrato en mención, presenta acuerdos y cláusulas que van en contra de la ley y la ética profesional.

El acuerdo y/o contrato está elaborado sin tener en cuenta la ley y el código de ética para ingenieros COPNIA, por consiguiente, el profesional que llegase a firmar dicho contrato estaría involucrado en asuntos legales y delito estipulados en la ley.

Cabe resaltar, que de acuerdo con el código de ética para ingenieros COPNIA, dicho acuerdo y/o contrato, va en contra de los principios establecidos en dicho código, ya que, por medio de este, se establece el reglamento y se legaliza la conducta profesional de los ingenieros en general y la violación de este será sancionada mediante los procedimientos establecidos en el mismo y las leyes afines.

Este código de ética profesional hace referencia a aquellas conductas profesionales, que se exigen, se prohíben o se inhabilitaban a los ingenieros en general y a sus profesionales afines o auxiliares. El código de ética profesional se establece en la ley 842 del 2003, el cual este compuesto por tres capítulos que hacen referencia a las disposiciones especiales, a los deberes, obligaciones y prohibiciones; junto con las inhabilidades e incompatibilidades, aplicadas a los profesionales en ingeniería en general, profesionales afines y auxiliares.

Teniendo en cuenta el código de ética COPNIA, y revisada las cláusulas de dicho acuerdo, la mayoría de estas, hacen referencia a acciones y procesos ilegales, que va en contra de la ética profesional, como se puede evidenciar, en los análisis realizados anteriormente.

El acuerdo y/o contrato con la empresa The WhiteHouse Security, es un documento que se puede considerar como ilegal, ya que va en contra del reglamento ético y legal de los profesionales de la ingeniería; a su vez, este documento demuestra, la utilización

indebida de información, el ocultamiento de procesos ilegales, entre otros, los cuales van en contra de la legislación vigente y la violación del código de ética COPNIA.

2.2.6 Análisis respecto a la Noticia del caso "Operación Andrómeda Buggly" Desde su posición teniendo en cuenta los Aspectos Legales y Éticos

La operación Andrómeda Buggly se basó en un conjunto de interceptaciones ilegales a las comunicaciones realizadas sobre el proceso de paz entre el equipo negociador del gobierno y el equipo negociador de las FARC.

Ethical Hacking "Comunidad Buggly" es el nombre de un establecimiento de dos pisos que estaba ubicado en Galerías, Bogotá, en el primer piso operaba un restaurante, en el segundo piso cumplía la función de un café internet, lleno de computadores, consolas de videojuegos entre otros; pero además de esto realizaban eventos donde reunían a personas participantes del Campus Party, estos jóvenes eran reclutados con la idea de aprender sobre el hacking ético, así fue como se conformó el personal de la central de interceptaciones ilegales, conformado por los jóvenes ya mencionados y un grupo de ejército.

A pesar de que la operación fue sustentada bajo la Ley 1621 de 2013, Plan Nacional de Inteligencia para identificar amenazas contra el Estado; el ejército aseguró que no haría interceptaciones para sabotear el proceso de paz, por tal motivo pierden legitimidad las acciones realizadas, además de esto, el caso reveló la información obtenida por la operación Andrómeda.

El informe obtenido de la operación Andrómeda revela que se encontraron evidencias de indisciplina y falta de control de las acciones realizadas por el personal militar sin su debido soporte legal, pero además de esto también de personas civiles ajenas al ejército lo que incumple la ley 1273 de 2009. Artículo 269C INTERCEPTACIÓN DE DATOS INFORMÁTICOS, también, se evidencia la filtración de documentación clasificada a una persona civil ajena a la organización lo que incumple los artículos 269F VIOLACIÓN DE DATOS PERSONALES.

Esta operación además de revelar la falta de seguridad y control en los procesos ejercidos por el ejército demuestra que la información y privacidad de las personas es vulnerada, dejando un cuestionamiento de la información que ha obtenido el gobierno de sus ciudadanos, a pesar de que varios sitios web o correos electrónicos aseguran la privacidad y seguridad de la información, esta es vulnerada por hackers, personas comunes, pero también por personas vinculadas al Estado.

2.3 ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN

2.3.1 Escenario 3

Situación problema: Análisis Red Team

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un Windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Dentro de la investigación también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema. El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

2.3.2 Herramientas y Procedimientos Utilizados para dar Solución al Escenarios 3 Red Team de acuerdo a los pasos de Pentesting

2.3.2.1 Nmap

Es una herramienta de código gratuita que permite realizar escaneos a los puertos de las redes en busca de vulnerabilidades que pueden servir como puerta de acceso por parte de usuarios no deseados, es utilizada frecuentemente en auditorías de seguridad y monitoreo de redes.

Comandos utilizados para la práctica:

Tabla 3. Comandos usados para la práctica

Comando	Descripción
nmap -A [ip]	Obtener los puertos y servicios de la máquina
nmap -sn [ip de red / máscara de subred).	Obtener la ip de los dispositivos conectados a la red
nmap -f –script vuln [ip]	Escaneo de vulnerabilidades

nmap -f -sS -sV –script default [ip]	Información por defecto que ofrece el script de Nmap
Nmap -f –script safe [ip]	Información que ofrece el script “safe”

Fuente: Sandra Cortes

*Para obtener la dirección ip de la red y su máscara se usó el comando “ip route”.

2.3.2.2 Metasploit

Es una herramienta de código abierto capaz de proporcionar información de vulnerabilidades en la seguridad en los computadores, además, permite realizar pruebas de penetración.

Comandos utilizados:

Exploits

exploit/windows/smb/ms17_010_psexec [Pantalla azul]

exploit/windows/smb/ms17_010_eternalblue [Acceder al computador víctima]

Otros

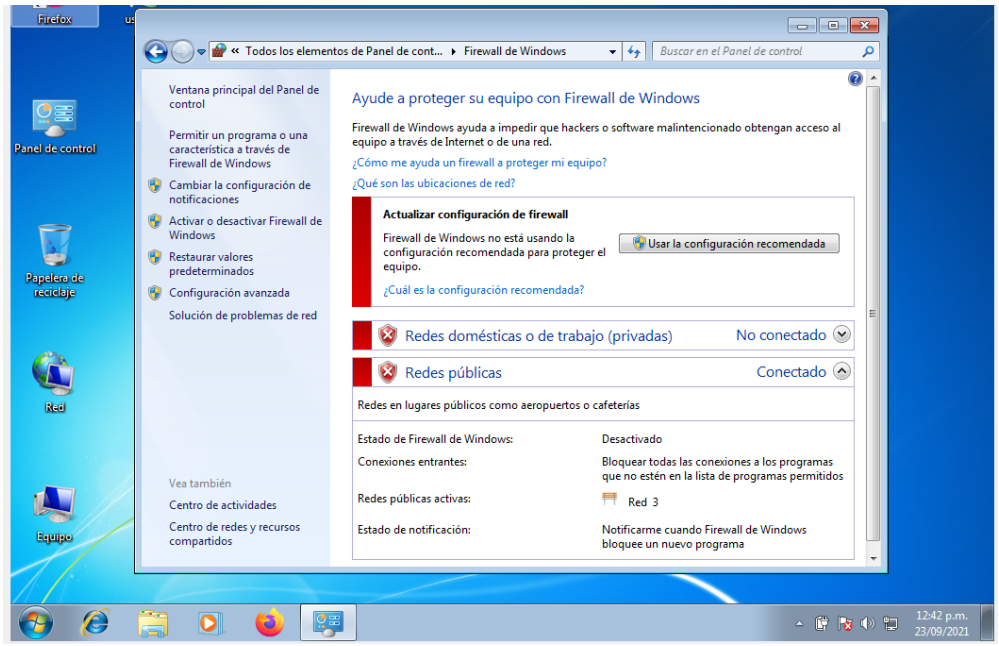
use auxiliary/dos/Windows/rdp/ms12_020_maxchannelids

set payload windows/x64/vncinject/reverse_tcp

2.3.2.3 Evidencia de los comandos utilizados y de cada herramienta utilizada

Desactivación del firewall de la máquina virtual Windows 7 x64.

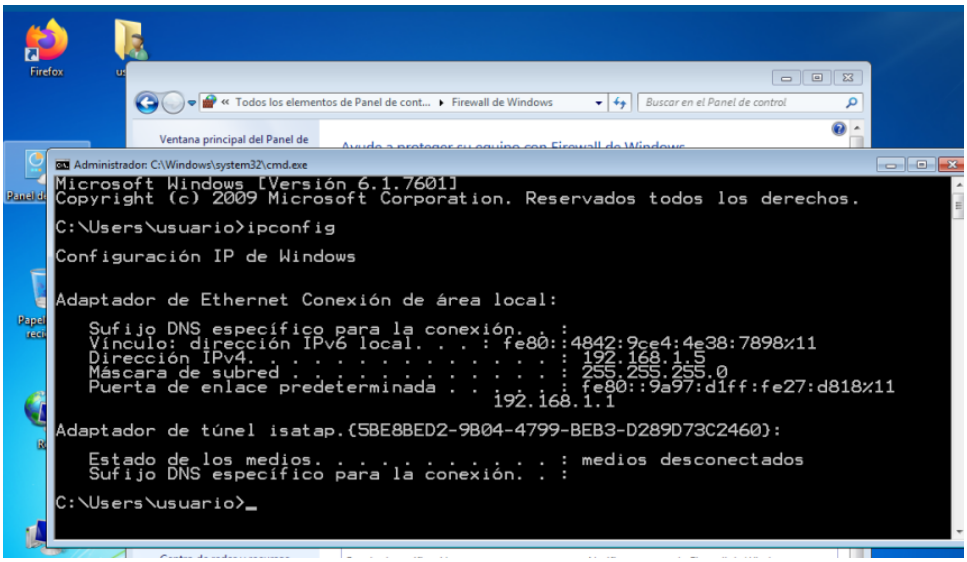
Figura 14. Desactivación del firewall de la máquina virtual Windows 7 x64.



Fuente: Sandra Cortes

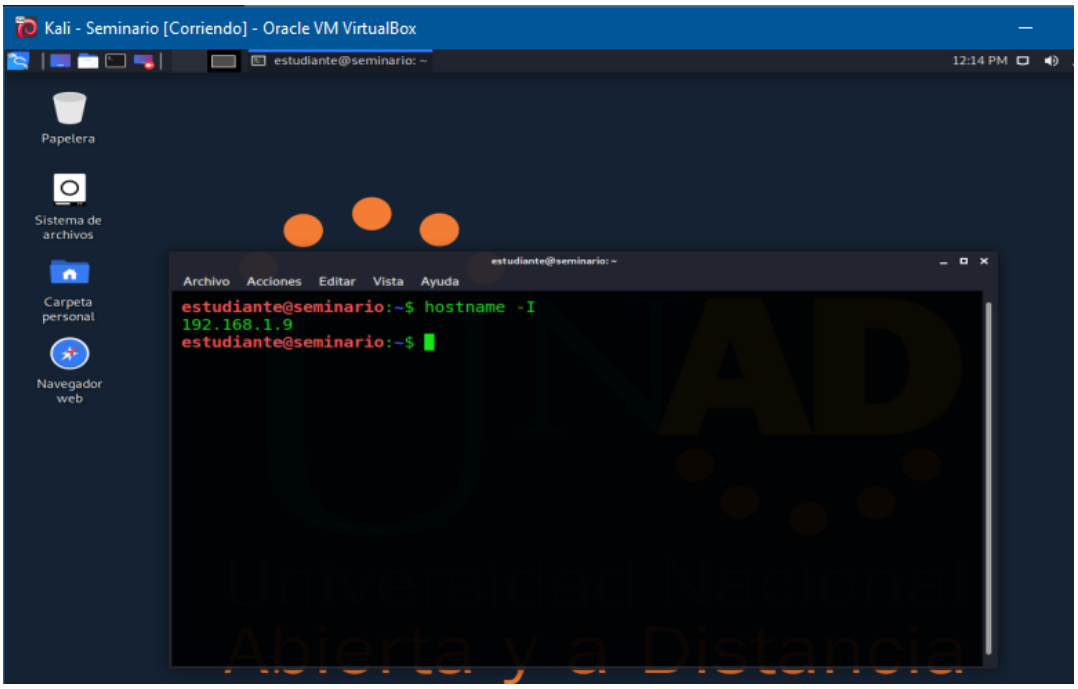
Para poder empezar con la práctica se procede a obtener las direcciones ip de las máquinas virtuales Windows 7 x64 y Kali-Linux.

Figura 15. Obtención de direcciones IP



Fuente: Sandra Cortes

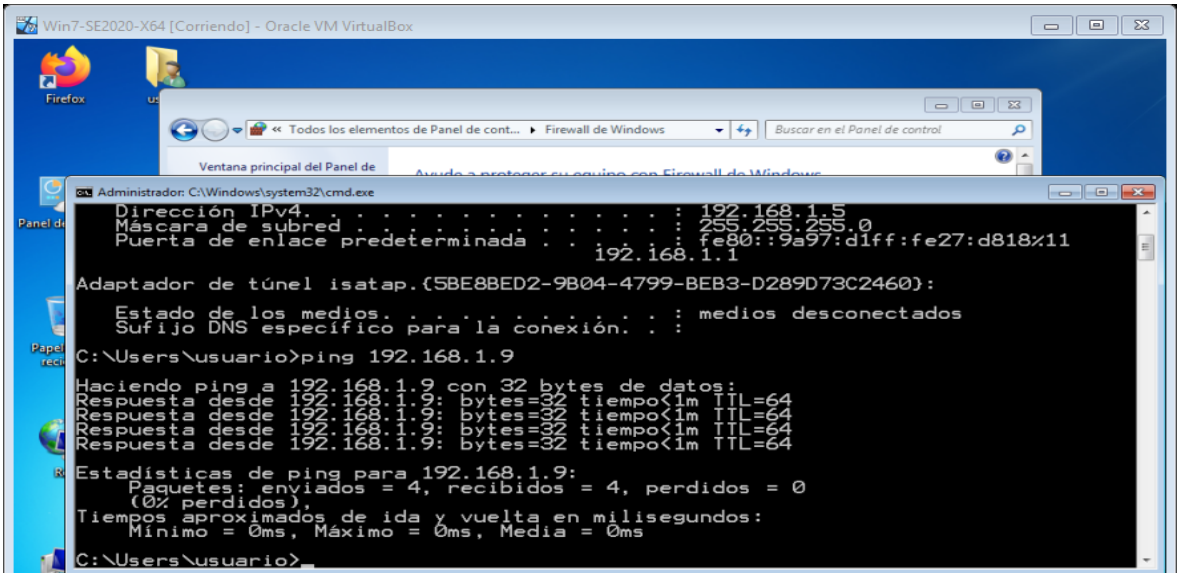
Figura 16.Obtención de direcciones IP



Fuente: Sandra Cortes

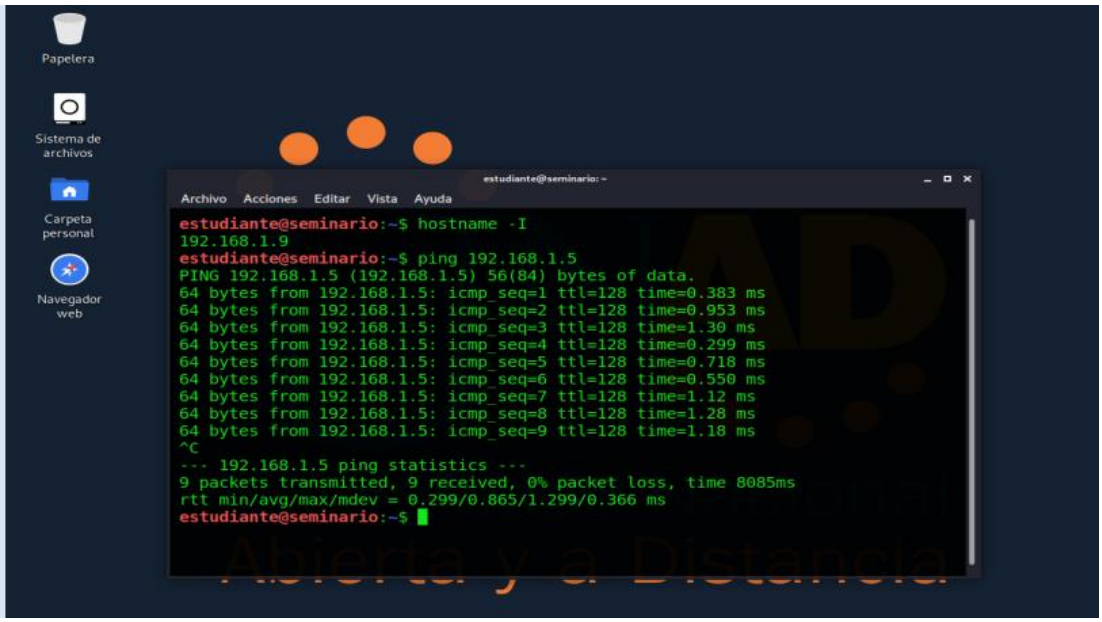
Posterior a conocer las direcciones ip se verifica que exista conexión entre las máquinas.

Figura 17. Verificación de existencia de conexión entre las máquinas



Fuente: Sandra Cortes

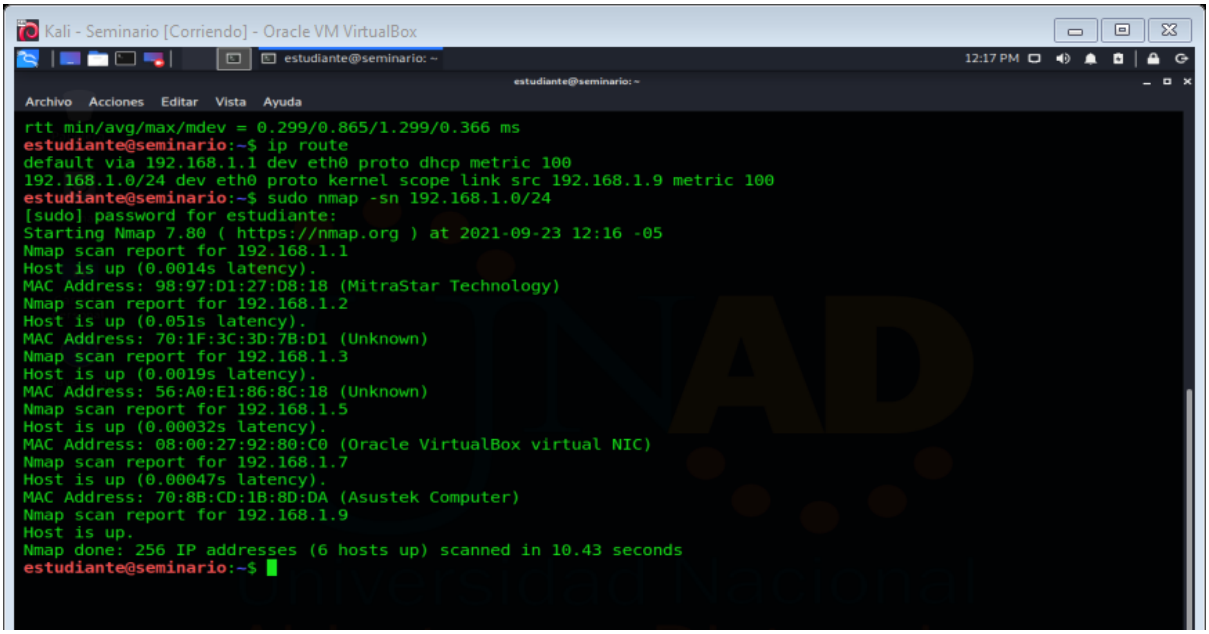
Figura 18. Verificación de existencia de conexión entre las máquinas



Fuente: Sandra Cortes

Utilizando la herramienta Nmap se analiza la red con el fin de conocer el número de dispositivos conectados a la red.

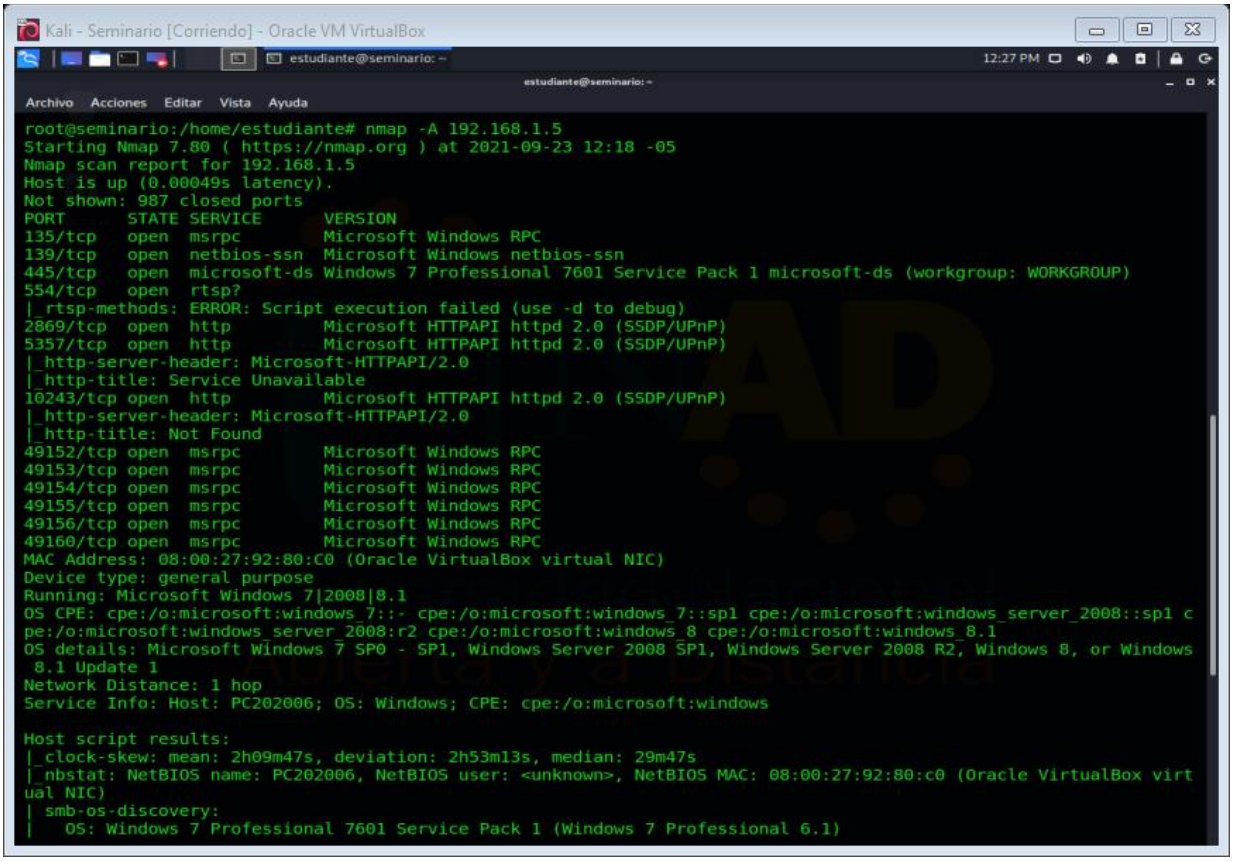
Figura 19. Análisis de la red



Fuente: Sandra Cortes

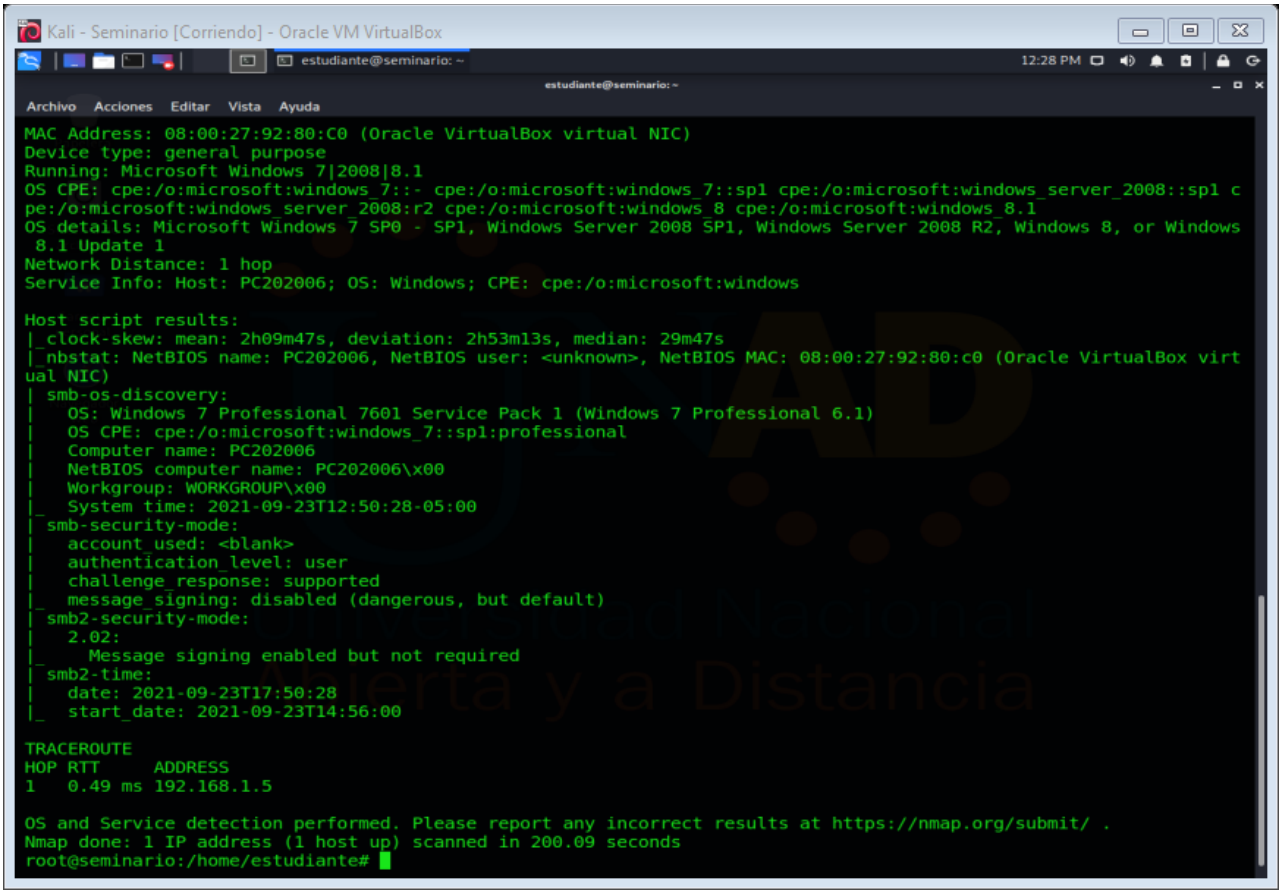
Para empezar con los ataques se inicia escaneando la máquina víctima a través de Nmap para conocer los puertos que tiene abiertos la máquina, en este caso se muestran sólo los puertos abiertos, incluyendo el 445/tcp puerto asignado a la NetBIOS.

Figura 20. Escaneo de máquina victima con Nmap



Fuente: Sandra Cortes

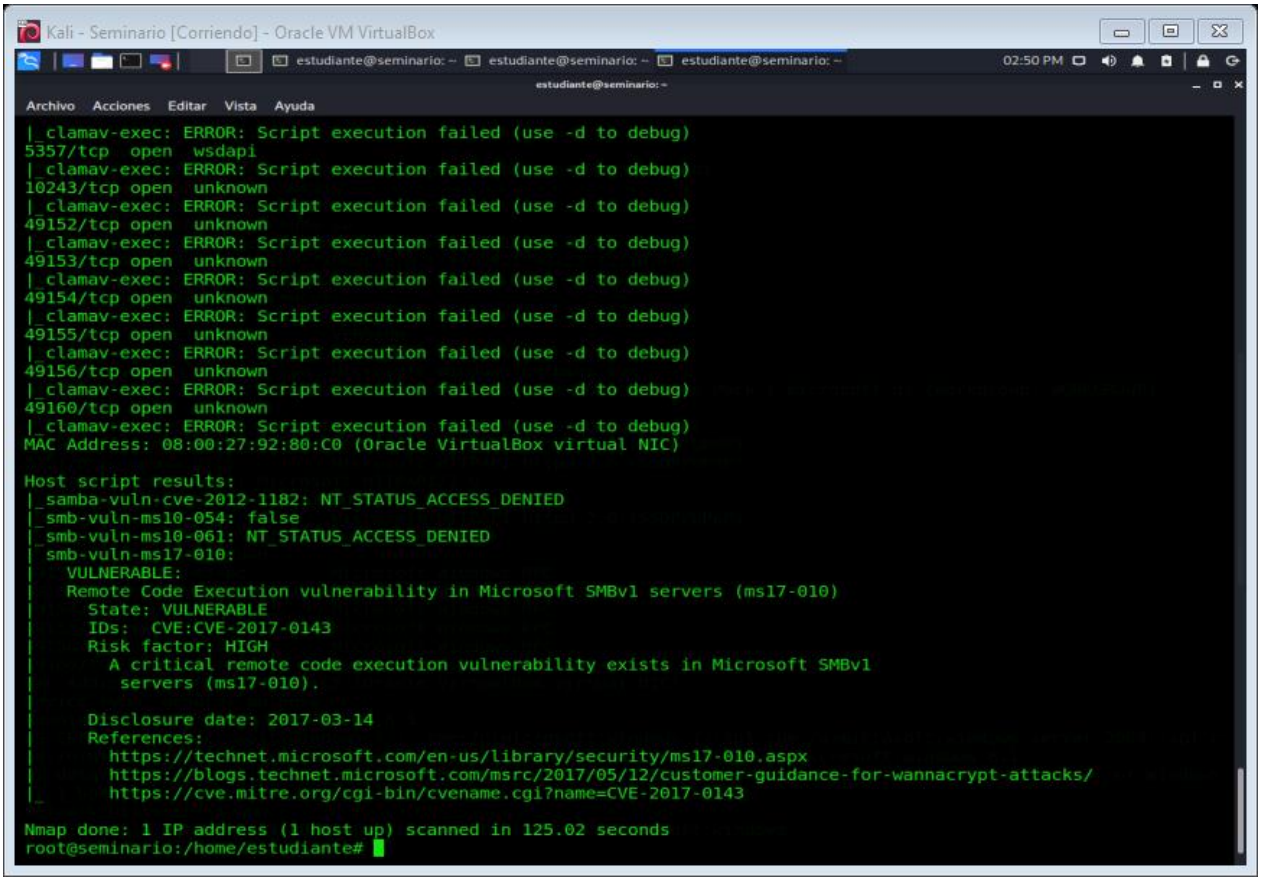
Figura 21. Escaneo de máquina victima con Nmap



Fuente. Sandra Cortes

Para conocer las vulnerabilidades de la máquina víctima se usa la herramienta Nmap con el comando nmap -f –script vuln 192.168.1.5

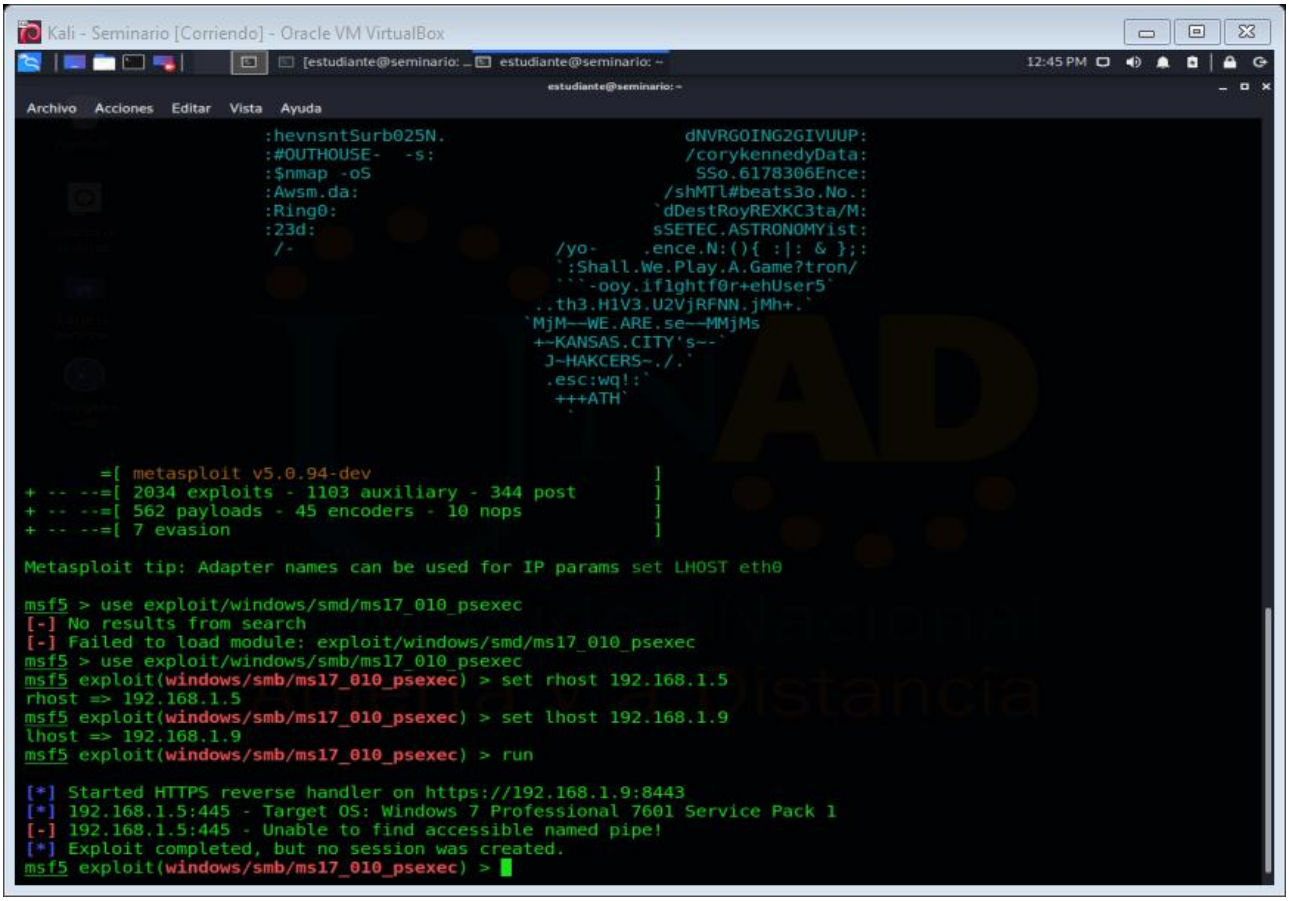
Figura 22. Conocer las vulnerabilidades de la máquina victima



Fuente. Sandra Cortes

Se empieza a utilizar la herramienta metasploit para los ataques.

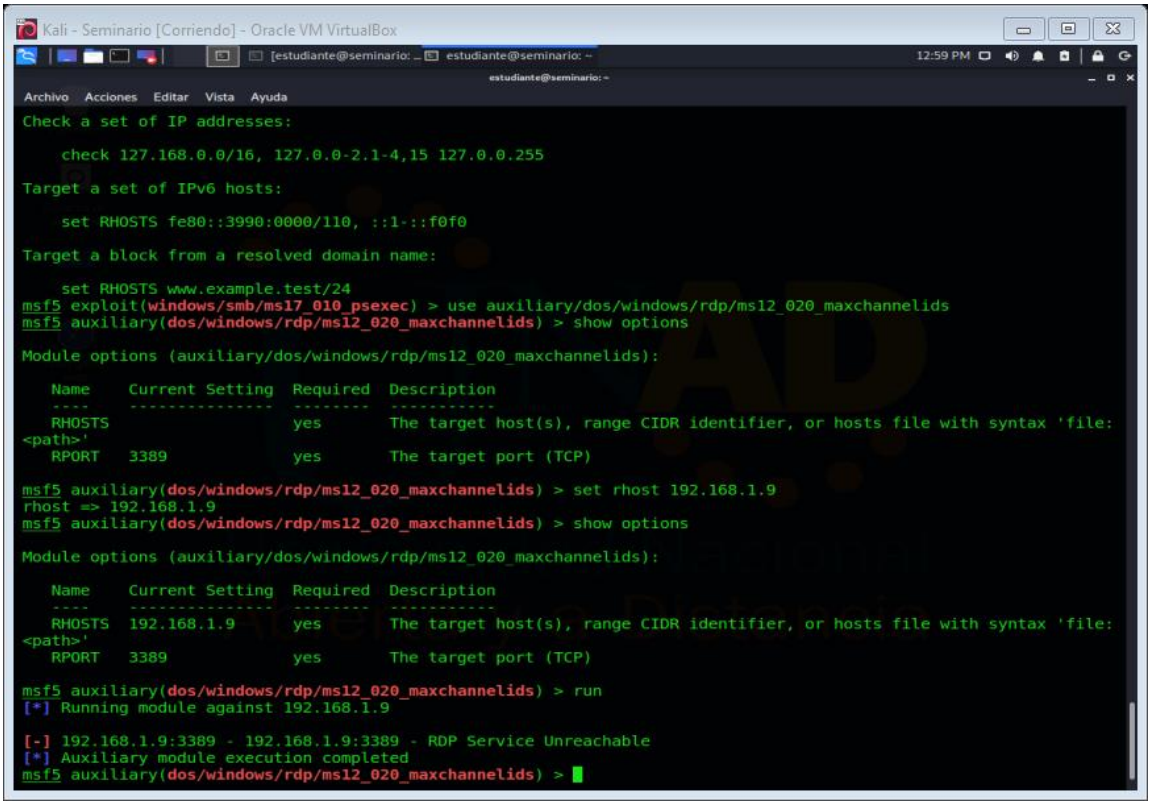
Figura 23. Uso de Metasploit para ataques



Fuente. Sandra Cortes

Se inicia intentando un ataque de pantalla azul a la máquina Win7x64, se empieza seleccionando el exploit necesario y usando un auxiliar, posterior a eso se indican la dirección rhost (víctima) y se ejecuta el exploit.

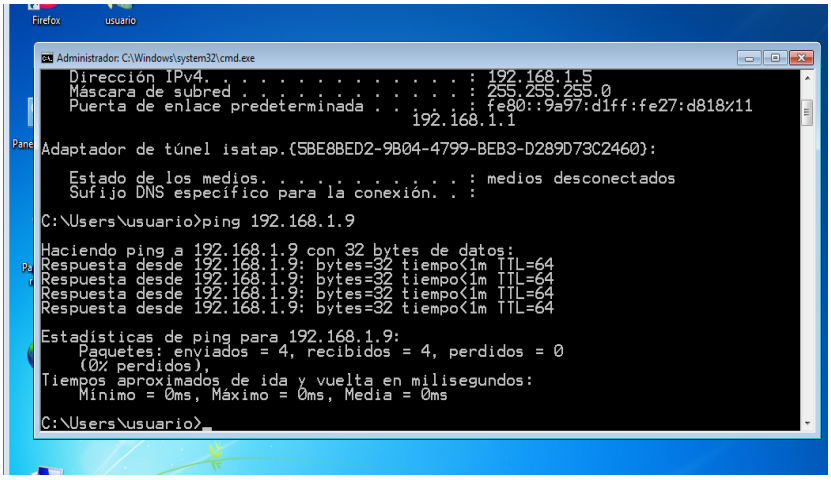
Figura 24. Uso de Metasploit para ataques



Fuente: Sandra Cortes

El ataque no tuvo resultados en la máquina víctima.

Figura 25. Ataque sin resultado en la máquina victima



Fuente: Sandra Cortes

Para el segundo ataque se usa el exploit de eternalblue usando el siguiente comando:

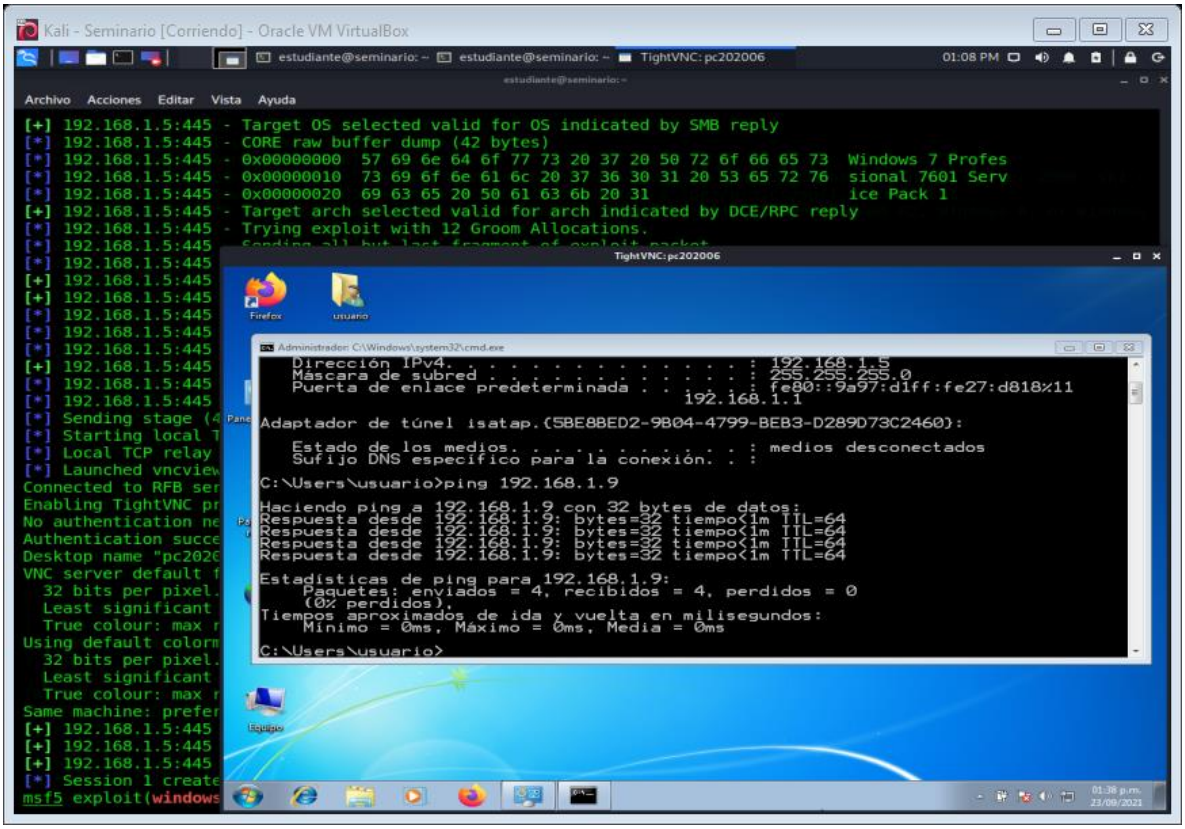
use exploit/windows/smb/ms17_010_eternalblue

También se setea un payload

set payload windows/x64/vncinject/reverse_tcp.

Se indican las direcciones rhost (víctima) y lhost (atacante); se procede a ejecutar el exploit.

Figura 26. el segundo ataque exploit de eternalblue

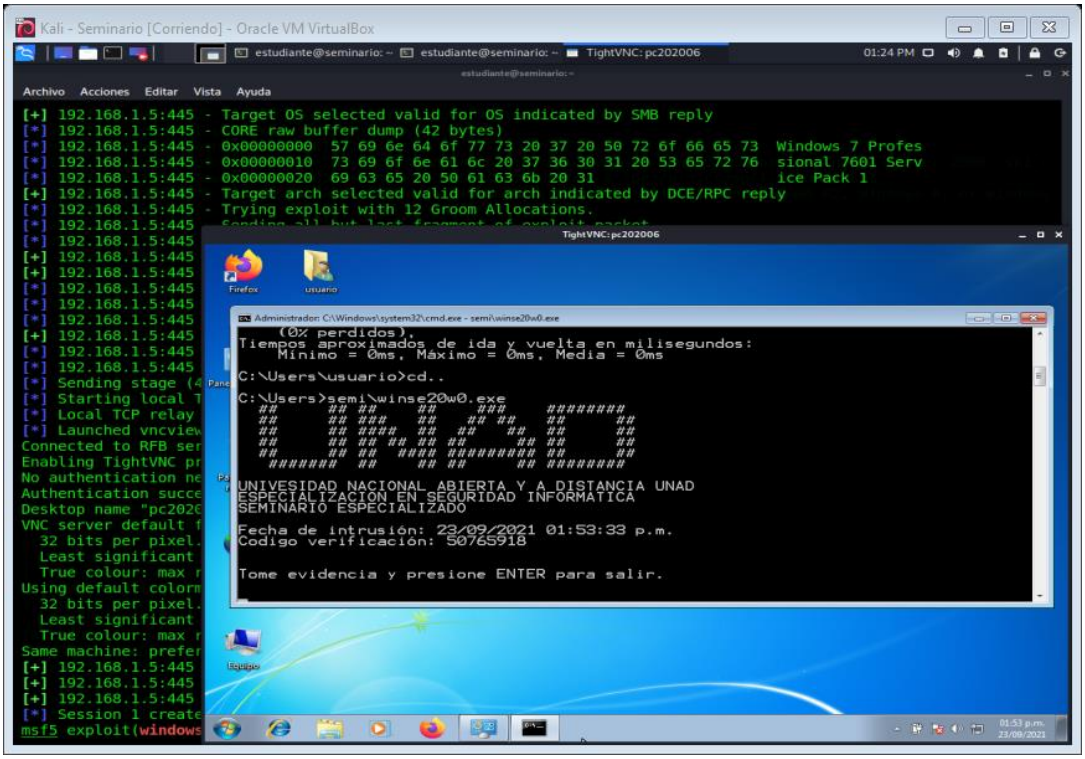


Fuente: Sandra Cortes

Se observa como este ataque concedió acceso al atacante a la máquina víctima.

A través de la ventana abierta por el exploit (TightVNC) se ejecuta el archivo “winse20w0” ubicado en la ruta “C:\Users\semi/winse20w0.exe”

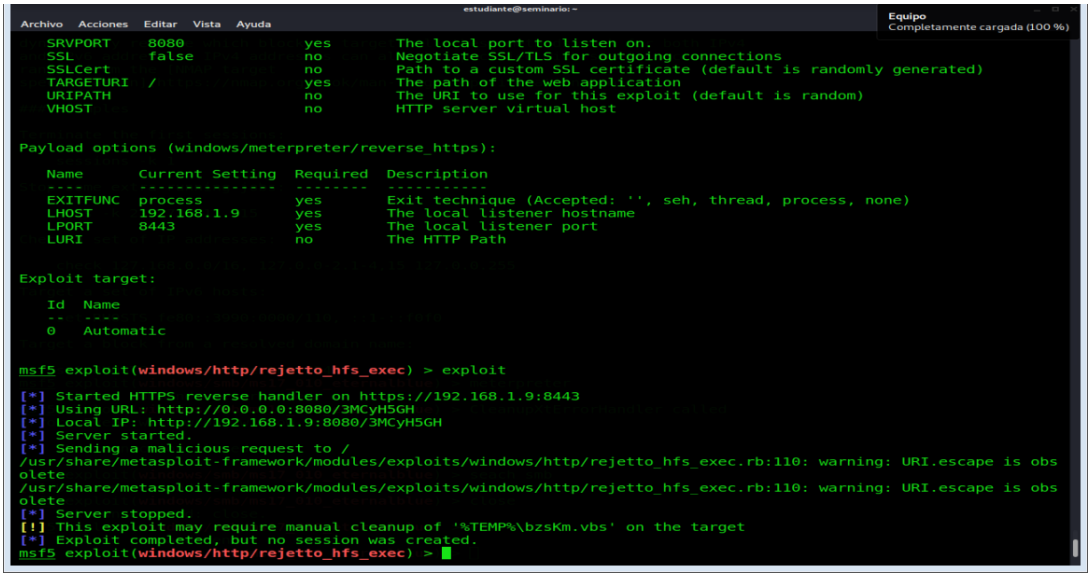
Figura 27. Acceso al atacante a la máquina virtual



Fuente: Sandra Cortes

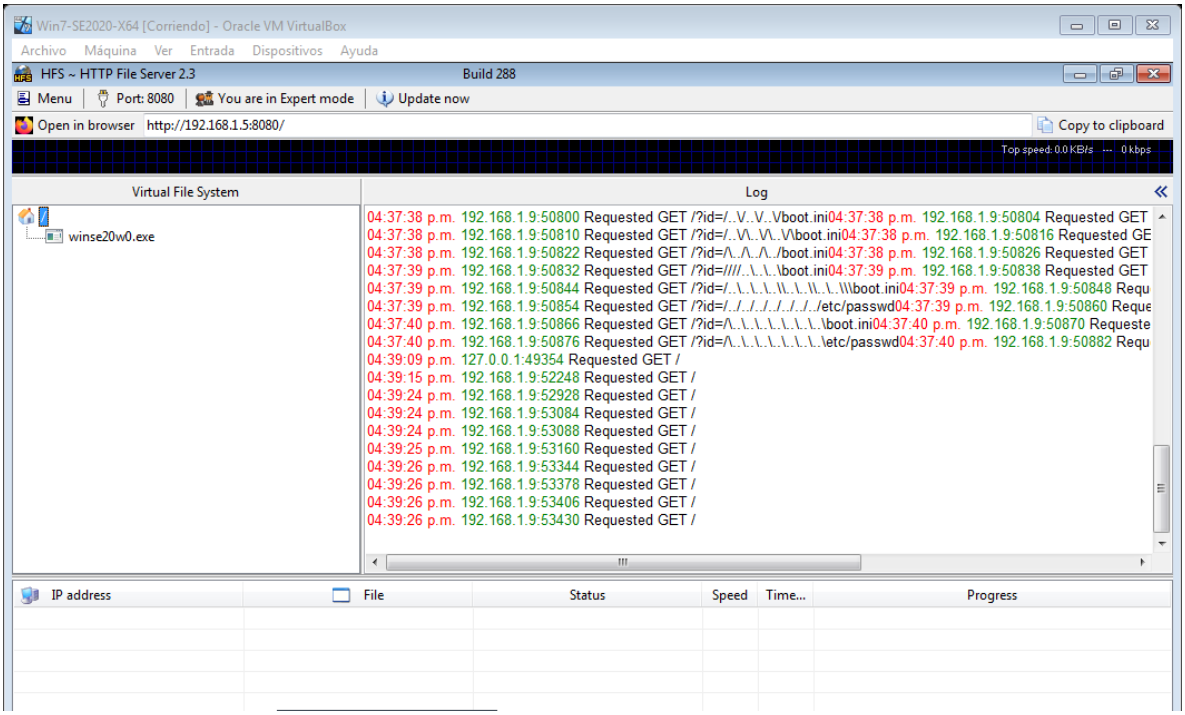
Se realiza un ataque a través de la aplicación Rejetto

Figura 28. Ataque a través de Rejetto.



Fuente. Sandra Cortes

Figura 29. Ataque a través de Rejetto.



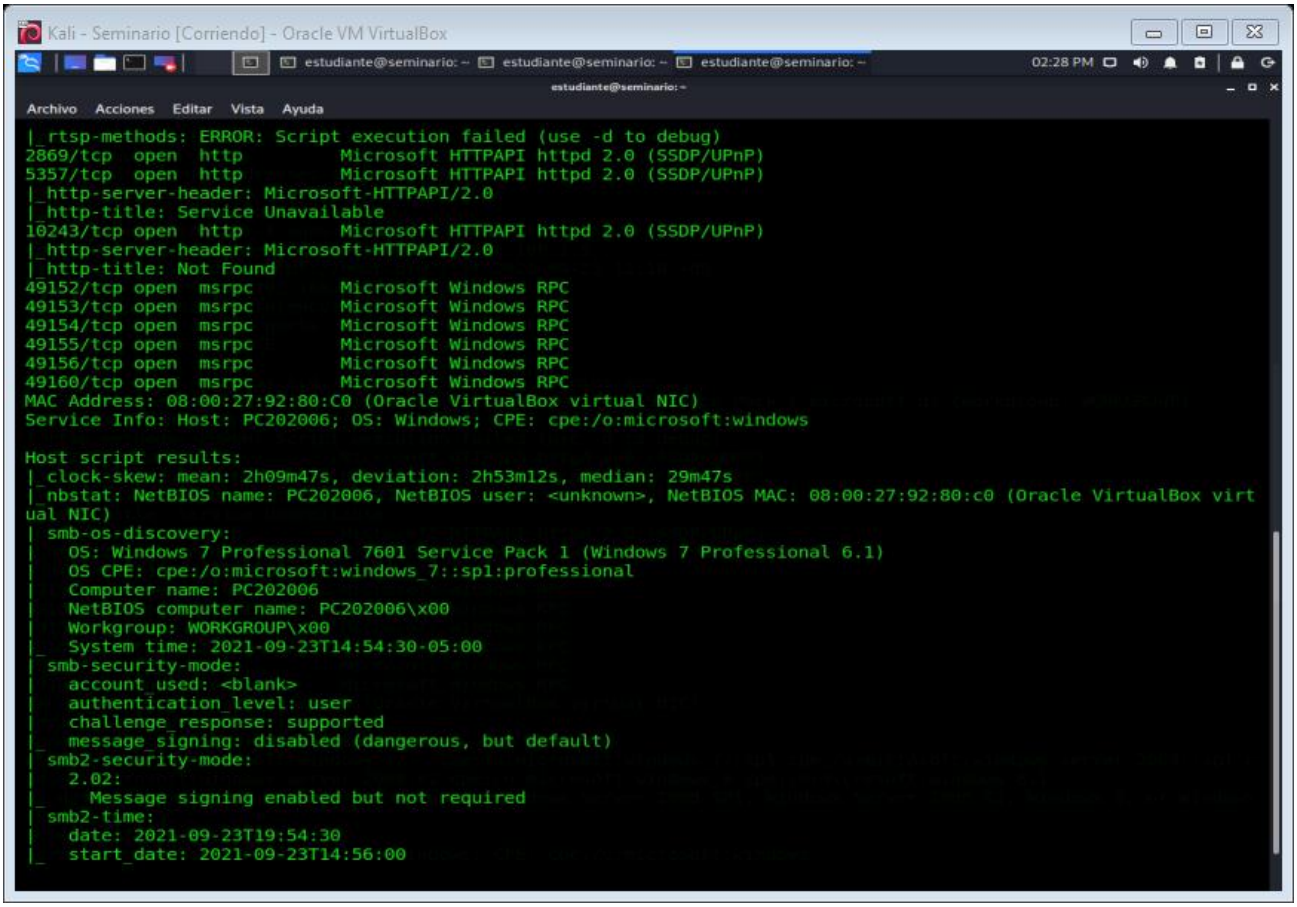
Fuente: Sandra Cortes

A parte de los ataques realizados se utiliza nmap para conocer más datos de la máquina víctima, mostrando datos como:

- Configuración del reloj
- MAC de NetBios
- Versión del S.O

También muestra si el usuario tiene una contraseña de acceso

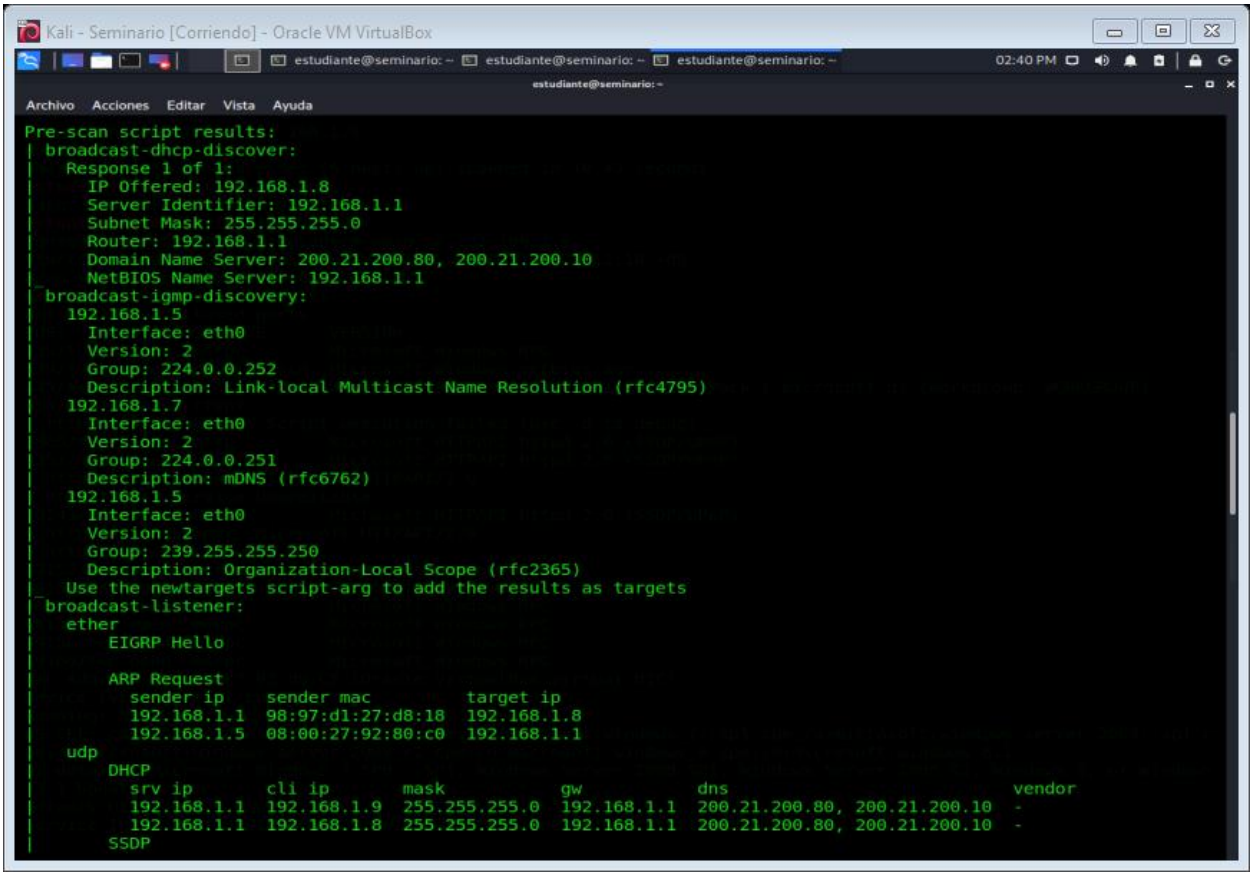
Figura 30. Conocer datos de la máquina victima



Fuente: Sandra Cortes

Utilizando el script *safe* se obtienen datos de configuración de la red, como la ip pública, información de las interfaces de red entre otros.

Figura 31. Datos de configuración de la red



Fuente: Sandra Cortes

2.3.3 Datos e información del escenario 3, utilizados para identificar el fallo de seguridad especifico, el cual ataca a la máquina Windows 7X64

Las computadoras que cuentan con Windows X86 y X64 son los sospechosos, ya que estos equipos presentan un sistema operativo antiguo con una aplicación que solo funciona en este, y no puede ser reemplazado ya que no es compatible con otros sistemas operativos.

Las computadoras presentan un SMBv1 activos para compartir las impresoras y algunos archivos dentro de la red.

Los sistemas operativos no se estaban actualizados cuando se presentó la fuga de información, ya que la última fue realizada el 05 de febrero de 2017.

Se identifica el fallo de seguridad (vulnerabilidad) CV3 -2017-0144.

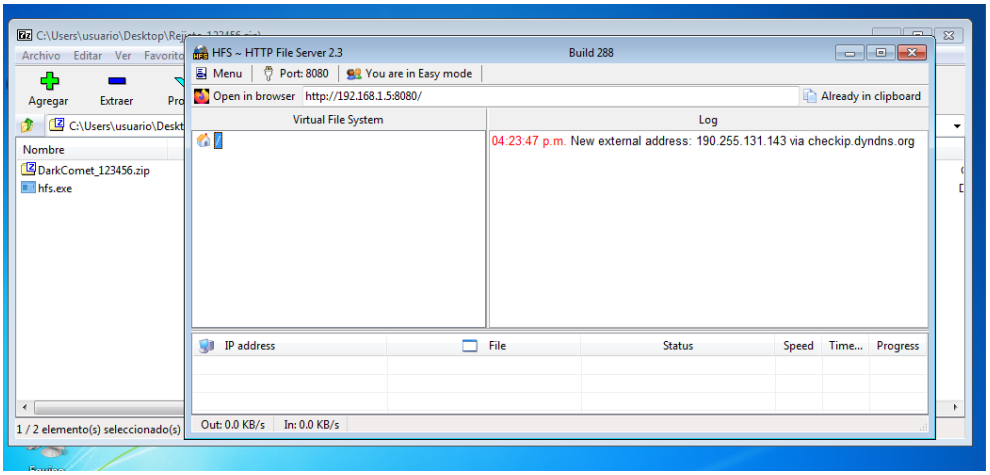
Las computadoras no presentan instalación de la actualización MS17-010.

2.3.4 Herramienta Utilizada para Identificar los Fallos de Seguridad de la “Maquina Windows 7”

La herramienta utilizada para identificar los fallos de seguridad fue Nmap, mostrando las vulnerabilidades de la máquina.

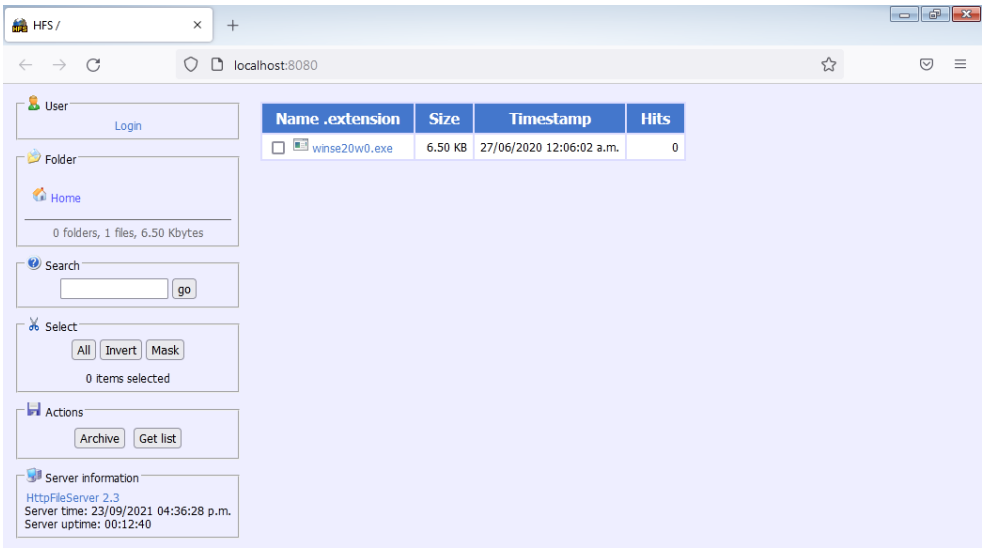
Se ejecuta mediante el puerto 8080.

Figura 32. Identificación de fallos de seguridad con Nmap



Fuente: Sandra Cortes

Figura 33. Identificación de fallos de seguridad con Nmap



Fuente: Sandra Cortes

2.3.5 Como afecta el ataque a la máquina Windows 7X64

Las vulnerabilidades de seguridad son puertas de entrada para que personas no autorizadas accedan a máquinas personales.

Dentro de las vulnerabilidades escaneadas, se encontró que la máquina tenía la vulnerabilidad MS17_010 que permite a un agente externo acceder a la máquina y efectuar cambios o robar archivos, cabe destacar que la vulnerabilidad MS17_010 es una vulnerabilidad que genera alerta al usuario debido a que se pueden ver los cambios realizados en la interfaz gráfica del sistema operativo, otro tipo de vulnerabilidades pueden permitir el robo, eliminación o modificación de archivos; instalación de software no deseado, entre otras.

2.4 ETAPA 4: CONTENCION DE ATAQUES INFORMÁTICOS

2.4.1 Escenario 4

Situación problema: Análisis Red team.

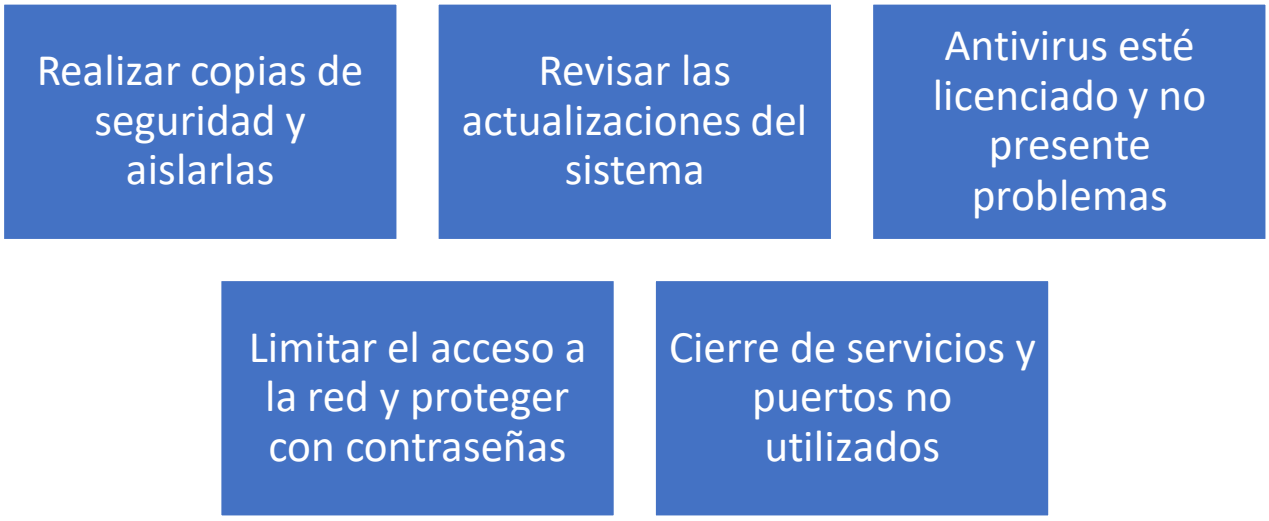
WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHouse Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

2.4.2 Análisis con acciones necesarias para contener un ataque en tiempo real

2.4.2.1 Prevención

Frente a un ataque en tiempo real el paso a seguir sería reunir la mayor cantidad posible de información sobre la seguridad de los equipos, se verifica el funcionamiento del firewall del sistema, posterior a eso se realizan los siguientes pasos:

Figura 34. Pasos a seguir para la prevención de un ataque

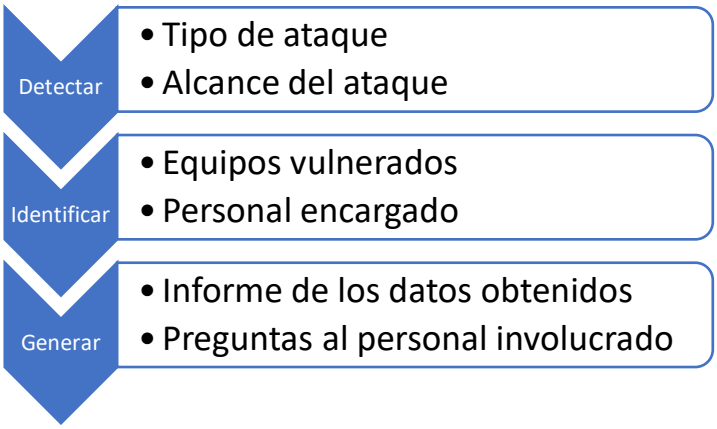


Fuente: Sandra Cortes

2.4.2.2 Detección

Al momento de detectar un ataque se empieza un momento crítico donde se debe reconocer el tipo de ataque que se está realizando, verificando la información sustraída o en casos que el ciberdelincuente revela datos del ataque, una buena gestión en esta fase puede reducir considerablemente el impacto del ataque. Se puede seguir el siguiente proceso:

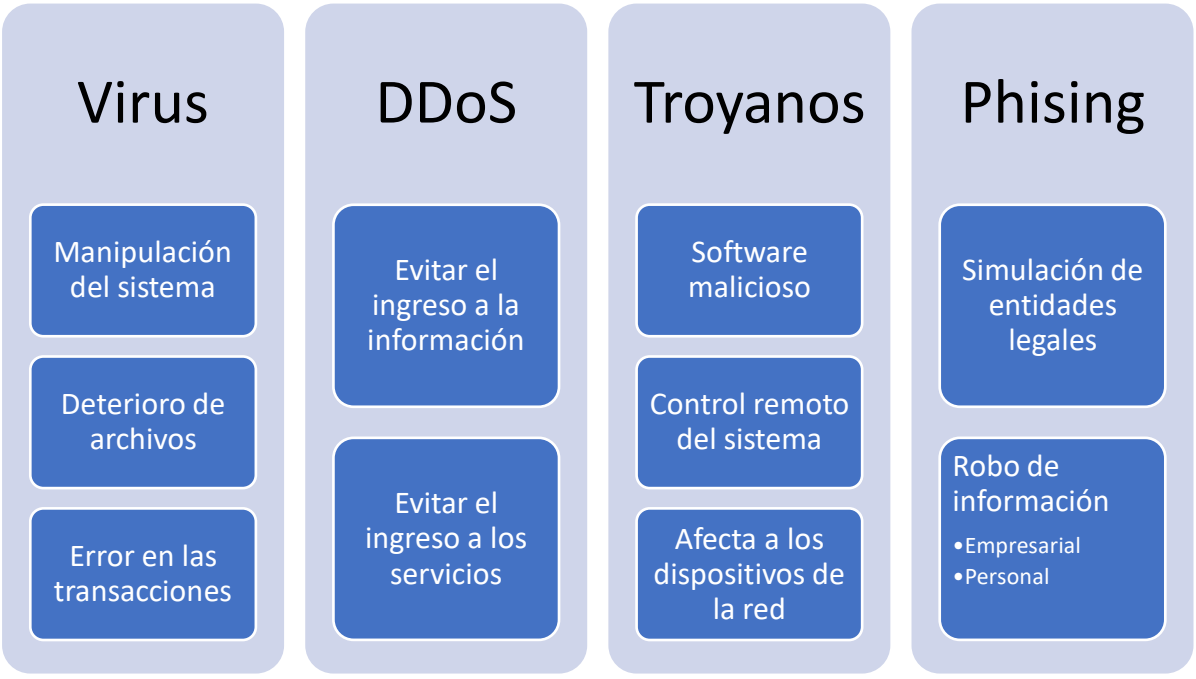
Figura 35. Pasos a seguir en el momento de la detección del ataque



Fuente: Sandra Cortes

Dentro de los tipos de ataques más comunes se tienen:

Figura 36. Tipos de ataques más comunes



Fuente: Sandra Cortes

2.4.2.3 Contención

Finalizada la fase de detección, se procede a iniciar los procesos para la contención y recuperación del sistema, en esta fase se identifican las herramientas que servirán para limitar el ataque y finalmente detenerlo, además de generar planes de contingencia para el recuperado de la información y bloqueo de cuentas o salidas del equipo.

Finalmente se retoma el funcionamiento normal, pero también, generando planes estratégicos para garantizar la seguridad frente a futuros ataques con la experiencia ya adquirida.

2.4.2.4 Comunicación

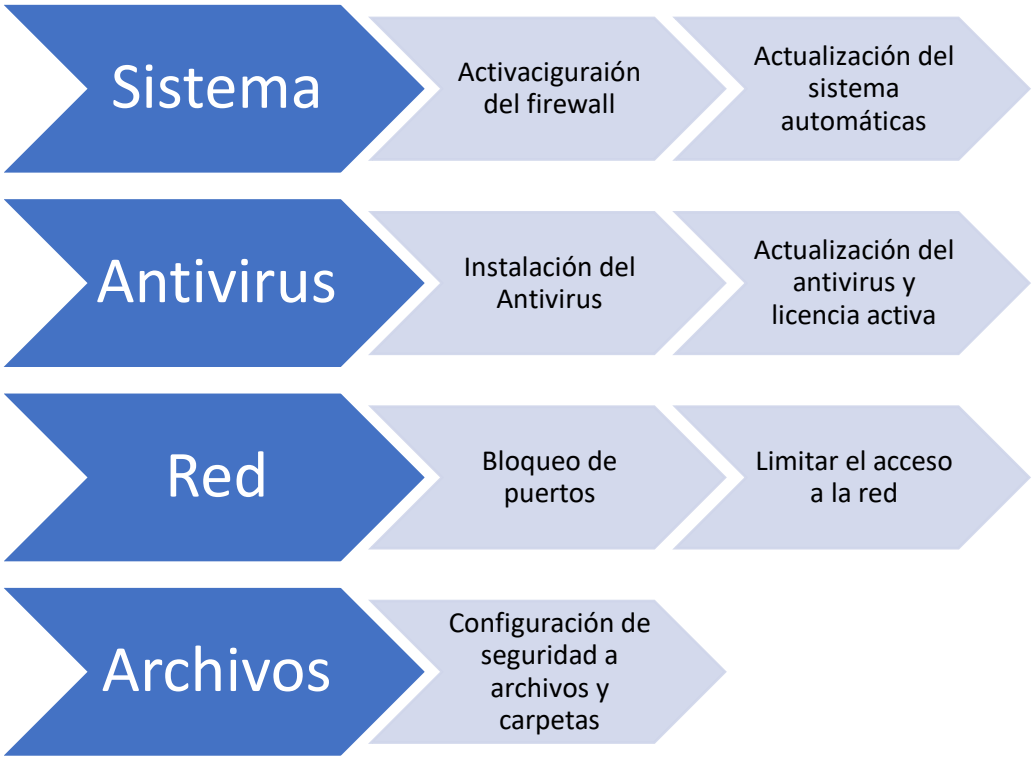
Como último paso se tiene el dar a conocer la información obtenida junto con los resultados a los interesados de la empresa, como pueden ser: clientes, trabajadores, jefe, gerentes y socios; con la finalidad de dar a conocer las consecuencias sufridas del ataque y más medidas que se adoptaron para mitigarlo.

2.4.3 Acciones de Hardenización a implementar para evitar ataques de seguridad informática

Hardening es una técnica empleada en equipos informáticos para mejorar su seguridad reduciendo las vulnerabilidades del mismo, esto se logra eliminando software innecesario, además de los servicios y usuarios que no se usan y podrían generar puertas de acceso no deseadas, también el limitar el número de puertos activos, entre otros.

Para el ejercicio realizado de Red Team, esta máquina presentó vulnerabilidades permitiendo el acceso remoto a los datos presentes en el equipo, para evitar futuros ataques se proponen las siguientes medidas que se muestran en la siguiente figura.

Figura 37. Medidas para evitar futuros ataques



Fuente: Sandra Cortes

2.4.4 Análisis Sobre las Diferencias entre el Equipo de Blue Team y el Equipo de Respuesta a Incidentes Informáticos

En la siguiente tabla, se muestra las diferencias entre Equipos Blue team y Equipos de respuestas a incidentes informáticos, con relación a sus características.

Tabla 4. Diferencias entre equipos Blue team y equipos de respuestas a incidentes informáticos

Característica	Equipos Blue team	Equipos de respuestas a incidentes informáticos
Enfoque	Se enfoca en seguridad defensiva.	Se enfoca en incidencias informáticas.
Operación	En su operación identifica comportamientos sobre el sistema y aplicaciones.	En su operación identifica causantes de incidentes y sus consecuencias.

Acciones	Actúa sobre ataques de amenazas de riesgos.	Incidentes de acciones sospechosas.
Actor	Contención de ataques, proponiendo mejoras para la entidad.	Gestiona los incidentes de una organización.
Análisis	Analiza, evalúa riesgos y soluciones (SEIM).	Analiza situaciones respondiendo a incidentes.
Vigilancia	Su vigilancia es constante, permitiendo procesos de documentación como bienestar de la entidad.	Su vigilancia es periódica, puesto que los objetivos son específicos y eficientes para nulidad de ataques.
Estado	Caracterización forense de las máquinas afectadas, proponiendo soluciones y medidas de detección.	El fortalecimiento del software reduce el número de incidentes.
Verificación	Caracteriza la efectividad de las medidas de seguridad.	Cuenta con efectividad en la respuesta y con normal funcionamiento de la entidad.
Proceso	Rastreo de incidentes de ciberseguridad.	Gestiona os respectivos incidentes.

Fuente: Sandra Cortes

2.4.5 Análisis sobre la pertinencia de trabajar con CIS "Center for Internet Security" como propuesta de aseguramiento por parte de un equipo de Blue Team

CIS es una entidad sin fines de lucro que busca aprovechar el poder de la comunidad TI a nivel global para desarrollar, promover y mantener las mejores prácticas de seguridad contra amenazas cibernéticas en organizaciones públicas y privadas, además de ofrecer soluciones para prevenir y responder rápidamente frente a los ataques.

CIS maneja un estándar de seguridad frente a atacantes que permitiría al equipo Blue team analizar las redes, monitorearlas, desarrollar evaluaciones y controles de vulnerabilidades.

Algunas de las vulnerabilidades más comunes en el estándar de CIS son:

- La ubicación de equipos desprotegidos y que se encuentran conectados a una red.
- En el momento del mal uso de los privilegios, abriendo archivos maliciosos o ingresando a páginas que tienen como finalidad acceder al sistema.
- Explotación de puertos, servicios, contraseñas inseguras, cuentas con una protección baja, instalación de software innecesario.

- Intervención en las conexiones inalámbricas para conectarse a la red de la empresa.

2.4.6 análisis sobre las funciones y características principales de un SIEM

Security Information and Event Management “SIEM” o Gestión de Eventos e Información de Seguridad tiene como objetivo otorgar a organizaciones información sobre potenciales amenazas de seguridad de sus redes cítricas de negocio y resolverlas de manera eficiente, esto es posible por medio de un banco de datos generado con análisis en tiempo real de sistemas como: antivirus, firewalls y soluciones de prevención de intrusiones.

Beneficios:

- Centralización de la información de seguridad
- Automatización de tareas
- Respuesta automática a eventos y amenazas
- Reducción en el tiempo de detección de ataques
- Análisis en tiempo real y logs actualizados automáticamente.
- Evaluación de vulnerabilidades

Funciones de SIEM:

- Resolver de manera eficaz y eficiente las amenazas a las que se puede enfrentar la organización.
- Analizar en tiempo real ataques hacia el hardware o software y alertar.
- Visualizar los procesos y procedimientos de seguridad.

Características de SIEM:

- Capaz de recolectar todos los datos debido a que en su arquitectura maneja la posibilidad de almacenar y trabajar con grandes cantidades de datos.
- Monitoreo en tiempo real, detección de amenazas, creación de indicadores y priorización de alertas.
- Análisis de eventos detectados para categorizarlos y priorizar los riesgos de mayor impacto.
- Administración en las alertas para notificar a usuarios específicos además de permitir configurar la forma como se envían las alertas.
- Informar sobre infracciones a las políticas, bloqueos y desbloqueos de cuentas, cuentas en desuso, cambios realizados, entre otras.
- Integración de varias aplicaciones para garantizar una interfaz de usuario de fácil interpretación y manejo.

Aplicaciones que implementan el sistema SIEM:

- IBM Security QRadar: es uno de los sistemas más completos con más de 400 módulos que permiten gestionar millones de eventos al día aportando soluciones inteligentes para garantizar la seguridad y evitar o reducir los ataques.
- McAfee Enterprise Security Manager: herramienta SIEM de la empresa de seguridad McAfee que permite monitorizar sistemas, recopilando, analizando y comparando los datos de incidentes de seguridad para de esta forma detectar amenazas de forma inteligente.
- LogRhythm: Solución SIEM orientada a Pymes que no pueden abordar costos de herramientas más avanzadas.

2.4.7 Elección de Herramientas que permitan Contener Ataques Informáticos

A continuación, se mencionan las tres herramientas que permiten contener ataques informáticos, teniendo en cuenta las observaciones descritas en problema escenario 4:

2.4.7.1 Openwips-ng

Es una herramienta que permite la detección y prevención de ataques en sistemas inalámbricos, la cual se compone de tres partes:

- **Sensores:** Detecta y responde a las amenazas, capturando el tráfico para el respectivo análisis y caracterización del sistema de seguridad.

- **Interfaces:** Permite analizar y mostrar en detalle, los ataques a los que pueden estar expuestas las redes inalámbricas.

- **Servidores:** Generan alertas y respuestas ante cualquier tipo de amenaza, permitiendo el análisis de los datos y la información enviada por los sensores.

2.4.7.2 Ossec

Corresponde a una herramienta gratuita, la cual permite realizar el análisis a los registros de información, verificando la integridad e información de las alertas que se presentan. Asimismo, permite administrar y realizar con facilidad el monitoreo de varios sistemas y

el registro de los diferentes dispositivos y/o formatos, debido a que esta cuenta con un motor de análisis permitiendo la detección de ataques en la mayoría de los sistemas operativos.

2.4.7.3 Snort.

Esta herramienta de código abierto permite realizar el análisis y el registro de paquetes en tiempo real, logrando identificar los ataques DOS y DDoS. De igual manera, esta es utilizada para detectar exploits, gusanos y exploración de puertos, analizando el tráfico de la red durante su ejecución y dando a conocer algún tipo de amenaza, bloqueando el ataque.

2.5 ETAPA 5: SOCIALIZACIÓN DEL INFORME TÉCNICO

2.5.1 Escenario 5

Situación problema: Análisis Final

The WhiteHose Security desea un informe técnico donde se plasme el proceso de los escenarios propuestos en cada una de las acciones como Blue team, Red team y aspectos legales que logró usted como experto en Ciberseguridad dentro del período de prueba de la organización. El informe es solicitado para ser analizado por los analistas Seniors en Seguridad con los que cuenta WhiteHouse Security, esto ayudará al proceso de selección de los expertos que harán parte de esta prestigiosa organización.

2.5.2 Enlace video informe técnico

Enlace video: https://youtu.be/Pq0x6vbYo_M

3 CONCLUSIONES

El profesional en seguridad informática debe estar actualizado, conocer y comprender sobre la legislación vigente, como son los decretos y las leyes relacionados con los delitos informáticos y protección de datos personales. Asimismo, conocer sobre el código de ética para ingeniero COPNIA, establecido en la Ley 842 de 2003, en donde el Congreso de Colombia decreta: “Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones”. De otra parte, estar actualizado con respecto a las modificaciones realizadas a dicha normatividad.

Teniendo en cuenta el acuerdo de confidencialidad y/o contrato con la empresa The WhiteHouse Security, este documentos se puede considerar como ilegal, ya que va en contra del reglamento ético y legal de los profesionales de la ingeniería; a su vez, este documento demuestra, la utilización indebida de información, el ocultamiento de procesos ilegales, entre otros, los cuales van en contra de la legislación vigente y la violación del código de ética COPNIA.

Las herramientas de análisis de vulnerabilidades como lo son Nmap, Nessus Metasploit son de gran ayuda en la implementación de un sistema de seguridad informática de una organización, por ello también es importante una buena comunicación entre el administrador de la herramienta y los administradores de los activos de la organización. Cabe resaltar que esto es un complemento de un análisis de seguridad, como lo son las pruebas de Pentest.

Para seleccionar una herramienta de contención, es importante analizar y tener en cuenta los múltiples factores de riesgo del sistema, junto con las capacidades de respuesta ante los incidentes presentados en tiempo real, esto con el fin de evaluar la capacidad del proceso desarrollado por el profesional de seguridad como la herramienta seleccionada para la ejecución del procedimiento.

4 RECOMENDACIONES

De acuerdo con el presente informe técnico, a continuación se plantean algunas recomendaciones para mejorar las estrategias utilizadas por Red Team & Blue Team:

- Contar con la continua asesoría jurídica y permanecer actualizado en los aspectos éticos y legales relacionados con la seguridad informática, a fin de evitar los conflictos legales por la desinformación. Asimismo, toda la documentación antes de ser firmada por la gerencia, esta debe estar revisada por el personal idóneo y la asesoría jurídica, para generar la legalidad de la documentación y de todos los procesos.
- Actualización permanente de firmwares a dispositivos de la organización. Las actualizaciones de los sistemas operativos deben ser automáticas, con la instalación de sistemas de seguridad como son los antivirus, parches, firewall, antispam y antispyware.
- Dentro del manual de políticas de seguridad y buenas prácticas, establecer los privilegios de administración de los equipos de cómputo, con el propósito de restringir la instalación de software sin la respectiva autorización. Igualmente, se debe establecer el bloqueo de las paginas de internet no autorizadas.
- Establecer políticas de seguridad informática, restringiendo la instalación de software sobre el sistema sin previa autorización, para minimizar el robo de información desde programas maliciosos. De igual manera, generar políticas de seguridad que permitan socializar con los empleados la importancia del sistema de seguridad informática.
- Mantener en continua capacitación y actualización a los empleados en lo referente a la normatividad vigente, procesos y procedimientos establecidos para la seguridad informática.
- Continua capacitación a los usuarios, ya que la mayoría de los ataques informáticos se presentan por la desinformación y la falta de conocimiento en los temas relacionados con las políticas de seguridad informatica y los manuales de buenas prácticas de la organización.
- Establecer el manual de políticas y buenas prácticas, sobre el manejo y uso de las computadoras, estableciéndose los ítems a que hace referencia la norma ISO 27001:2013.
- Realizar auditorías internas, que permitan identificar las vulnerabilidad, amenazas y riesgos, a fin de tomar los correctivos necesarios.
- Establecer e implementar procesos y procedimientos relacionados con el monitoreo, manejo y actualización de las herramientas que permiten el escaneo e identificación de las vulnerabilidades, para evitar la explotación y la contención de los ataques informáticos.

BIBLIOGRAFÍAS

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. Recuperado de: https://www.cisecurity.org/cis-benchmarks/

COLOMBIA.CONGRESO DE LA REPÚBLICA. Ley 842 (14, octubre, 2003). "Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones.". Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

COLOMBIA.CONGRESO DE LA REPÚBLICA. Ley 1273 (05, enero, 2009). "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado-denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que usen las tecnologías de la información y de las comunicaciones, entre otras disposiciones". Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

COLOMBIA.CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). "Por la cual se dictan disposiciones generales para la protección de datos personales.". Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Computer Science Columbia.[Sitio Web]. A Red Team/Blue Team Assessment of Functional Analysis Methods for Malicious Circuit Identification. [Consulta: 01 de septiembre de 2021]. Disponible en: http://www.cs.columbia.edu/~simha/preprint_dac14.pdf

Copnia. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [Sitio web]. [Consulta: 12 de septiembre de 2021]. Copnia. (pp. 3-26). Recuperado de: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Costes, C. (2015). Auditando con Nmap y sus scripts para escanear vulnerabilidades Welivesecurity by ESET. [En línea] Disponible en: https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

CVE. [Sitio Web]. [Consulta:01 de septiembre 2021]. Disponible en: https://cve.mitre.org/index.html

CYBERSEGURIDAD.NET. [Sitio Web]. Las fases de un test de penetración (Pentest) (Pentesting I). [Consulta:01 de septiembre 2021]. Disponible en: https://www.cyberseguridad.net/las-fases-de-un-test-de-penetracion-pentest-pentesting-i

El Espectador. De Andrómeda a los 'hackers'. [Sitio web]. [Consulta: 12 de septiembre de 2021]. Disponible en: https://www.elespectador.com/investigacion/de-andromeda-a-los-hackers-article-492933/

ENTER.CO. Detrás de Buggly: la historia de la fachada Andrómeda. [Sitio web]. [Consulta: 12 de septiembre de 2021]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Esecurityplanet.[Sitio web]. 10 Open-Source Security Breach Prevention and Detection Tools. [Consulta: 12 de septiembre de 2021]. Disponible en: https://www.esecurityplanet.com/networks/open-source-security-breach-prevention-and-detection-tools/

Exploit Database. [Sitio Web]. Exploits. [Consulta:01 de septiembre 2021]. Disponible en: https://www.exploit-db.com/

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). (p. 14 - 27) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles5482_G21_Gestion_Incidentes.pdf

Hacking Para Novatos. [Sitio Web]. Fases de una auditoría (pentesting). [Consulta:01 de septiembre 2021]. Disponible en: https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/

Homebrew Formulae. [Sitio Web]. exploitdb. [Consulta:01 de septiembre 2021]. Disponible en: https://formulae.brew.sh/formula/exploitdb

Leacock, S. (2019). Introducción al escaneo de red y vulnerabilidades con Nmap. Backtrack Academy [En línea] Disponible en: https://backtrackacademy.com/articulo/introduccion-al-escaneo-de-red-y-vulnerabilidades-con-nmap.

Metasploit actual combat-ms17-010 (eternal blue) explotación y reproducción de vulnerabilidades [En línea] Disponible en: https://programmerclick.com/article/85041358889/

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63) Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Netsparker.[Sitio web]. Red Team Vs Blue Team Testing for Cybersecurity. . [Consulta: 12 de septiembre de 2021]. Disponible en: https://www.netsparker.com/blog/web-security/red-team-vs-blue-team/

Noticias Caracol. Fiscalía interrogará a representante legal del negocio donde operaba base Andrómeda. [Sitio web]. [Consulta: 12 de septiembre de 2021]. Disponible en: https://www.youtube.com/watch?v=Gh-pw2oCo6M

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

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

Red Teams. [Sitio web]. What is a red Team. [Consulta: 01 de septiembre de 2021]. Disponible en: https://redteams.net/redteaming/2013/what-is-a-red-team

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

Security Affairs. [Sitio web]. Cyber Security: Red Team, Blue Team and Purple Team. [Consulta: 01 de septiembre de 2021]. Disponible en: https://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blueteam.html

Semana. Chuzadas: así fue la historia. [Sitio web]. [Consulta: 12 de septiembre de 2021]. Disponible en: https://www.semana.com/nacion/articulo/chuzadas-a-negociadores-de-la-paz-por-parte-del-ejercito-nacional-asi-fue-la-historia/376548/

Semana. El informe que sacudió el caso de la fachada Andrómeda. [Sitio web]. [Consulta: 12 de septiembre de 2021]. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

SPARTAN CYBERSECURITY. [Sitio Web]. Fases de un pentesting. [Consulta:01 de septiembre 2021]. Disponible en: https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/

Técnicas de Detección de ataques en un sistema SIEM "Security Information and Event Management". Internet. Disponible en: https://repositorio.usfq.edu.ec/handle/23000/4911

Universidad Nacional Autónoma de México. [Sitio Web]. Pruebas De Penetración Para Principiantes: 5 Herramientas Para Empezar. [Consulta:01 de septiembre 2021]. Disponible en: https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Wikipedia. [Sitio Web]. Common Vulnerabilities and Exposures. [Consulta:01 de septiembre 2021]. Disponible en: https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures