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

HENRY ALBERTO CALDERÓN FÉREZ

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

DIRECTOR DEL CURSO: JOHN FREDDY QUINTERO TAMAYO

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

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

En este informe se relacionan los aspectos relevantes del desarrollo de las actividades planteadas en el Seminario Especializado - Equipos Estratégicos en Ciberseguridad - Red Team & Blue Team, en el cual mediante la conceptualización y la practica virtual se logró dar cumplimiento a las competencias y propósito del curso. En la primera parte se realizó una evaluación de las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales, donde se realizó frente a un caso propuesto, el análisis de las implicaciones éticas y legales, y también en relación a la vulnerabilidad de la ley 1273; en la segunda parte realizando pasos y proceso bajo la perspectiva de Red Team, se realizó un ejercicio de pentesting donde se demostró vulnerabilidades de un sistema informático a partir del uso de metodologías y técnicas de intrusión, sobre un escenario propuesto de máquinas virtuales; en la tercera y última parte, con la perspectiva de Blue Team se propusieron medidas para la hardenización y mitigación de los fallos de seguridad encontrados en el escenario propuesto de máquinas virtuales.

GLOSARIO

Pentesting: Es una práctica en la cual se realiza un ataque a un sistema informático con la finalidad de evaluar su seguridad y así encontrar fallos, vulnerabilidades y errores de seguridad.

Red Team: Es un equipo de expertos de seguridad informática, enfocados en la seguridad ofensiva, se encargan de emular ataques informáticos para explotar vulnerabilidades en los sistemas y/o aplicaciones en una organización.

Blue Team: Es un equipo de expertos de seguridad informática, enfocados en la seguridad defensiva, se encargan evaluar los riesgos y amenazas a los que están expuesto los sistemas e infraestructura informática de una organización, y a su vez realiza procesos de contención y mitigación de ataques informáticos.

Exploit: Son programas que contienen datos o códigos maliciosos, que buscan explotar o vulnerar una falla informática para lograr tener acceso y control de un sistema informático.

Vulnerabilidad Informática: es un punto débil o un defecto de seguridad en el software o hardware que representa un riesgo de la seguridad de los sistemas y de la información.

Hardening: Es un término que se refiere al endurecimiento o aseguramiento de la seguridad de un sistema informático, para así aumentar las probabilidades de protección frente a ataques informáticos.

NMAP: Es una herramienta de código abierto bajo licencia GPL, utilizada para la exploración y auditoria de seguridad de redes TCP/IP.

METASPLOIT: Es una herramienta de código abierto, está diseñado para el desarrollo y ejecución de exploits.

OPENVAS: Es una herramienta bajo licencia GPL, de código abierto, que sirve como herramienta para el análisis y evaluación de vulnerabilidades.

INTRODUCCIÓN

Contener ataques informáticos hoy en día puede ser considerado una tarea muy difícil, porque son muchos los riesgos y amenazas a los están expuestos los sistemas, dispositivos, las redes, aplicaciones, entro otros, son muchos los vectores y modos de ataque que existen y también los que aparecen nuevos en el día a día, y dependiendo el volumen de activos, de información, dispositivos, sistemas con los que pueda contar una organización, mientras más se tenga, más complejo se vuelve bastionarlos y lograr obtener niveles de seguridad aceptables, y proteger sobre todo la información que es el activo más importante para las organizaciones.

Bajo esta necesidad surgen los equipos de seguridad Red Team & Blue Team que vienen aportar respuestas a la demanda de ciberseguridad, bajo dos enfoques, el Red Team como un esquema de revisión y aseguramiento de la seguridad informática en las organizaciones, por su capacidad para evaluar los ámbitos de seguridad de protección, detección y respuesta, a través de ejercicios de simulación de ataques reales; por otra parte los equipos de seguridad Blue Team con actividades de detección, respuesta y mitigación frente a las amenazas y ataques informáticos.

El desarrollo de presente informe es el resultado de la solución de varias actividades planteadas en el curso de Seminario Especializado - Equipos Estratégicos en Ciberseguridad - Red Team & Blue Team, donde se adquirieron conocimientos específicos para la planificación de estrategias basadas en metodologías de ciberseguridad ofensivas y defensivas, bajo los enfoques de Red Team y Blue Team, lo cual permite desarrollar competencias para hacer frente a eventos o incidentes de seguridad informática en el campo laboral, teniendo presente que para el desarrollo de estas actividades, ante todo debe darse cumplimiento a las normas éticas y legales, y desarrollar los procesos basándose en metodologías y buenas prácticas para obtener resultados efectivos que ayuden a mejorar los esquemas de ciberseguridad en una organización.

OBJETIVOS

OBJETIVO GENERAL

- Desarrollar competencias propias de los Equipos Estratégicos de Ciberseguridad Red Red Team & Blue Team, a través de la aplicación de procesos, metodologías, herramientas y marco legal, mediante la conceptualización y practicas virtuales, aplicados a escenarios planteados por la UNAD en el seminario especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

OBJETIVOS ESPECIFICOS

- Identificar la normatividad relacionada con delitos informáticos en Colombia.

- Plantear las implicaciones éticas y legales sobre el caso problema “Anexo 3 - Acuerdo”.

- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías, técnicas de intrusión y herramientas especializadas, sobre un escenario propuesto de máquinas virtuales “Anexo 4 - Escenario 3”.

- Proponer medidas para la hardenización y mitigación de los fallos de seguridad encontrados en el escenario propuesto de máquinas virtuales.

1. LEGISLACIÓN RELACIONADA CON DELITOS INFORMÁTICOS

Dentro del margen legal sobre delitos informáticos y protección en datos personales, el estado Colombiano cuenta con normatividad importante que ha venido legislando con mayor fuerza en esta última década, siempre tratando de adaptarse a la nuevas realidades propias de los avances tecnológicos que viene afrontando el país por el proceso de globalización, teniendo avances significativos en conectividad y todo lo que tiene que ver con las TIC´s, por lo que se ha visto en la necesidad de ajustar su normatividad para poder contrarrestar esos riesgos adyacentes de las nuevas tecnologías.

1.1. LEY 1273 DE 2009

A través de la ley 1273 de 2009 el congreso de la Colombia modificó el Código Penal y tipificó los delitos informáticos contra la protección de la información, los datos y los sistemas informáticos, buscando con esta "la preservación integral de los sistemas hagan uso de tecnologías de la información y las comunicaciones"[1].

En el capítulo primero (atentados contra la confidencialidad, la integridad y la disponibilidad de los Datos y sistemas informáticos) se penaliza los siguientes delitos:

- (prisión 48 a 96 meses, multa 100 a 1000 S.M.L.M.V.).

- Artículo 269B: Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación (prisión 48 a 96 meses, multa 100 a 1000 S.M.L.M.V.)

- Artículo 269C: Interceptación de Datos Informáticos (prisión 36 a 72 meses).

- Artículo 269D: Daño informático (prisión 48 a 96 meses, multa 100 a 1000 S.M.L.M.V.).

- Artículo 269E: Uso de Software Malicioso (prisión 48 a 96 meses, multa 100 a 1000 S.M.L.M.V.).

- Artículo 269F: Violación de Datos Personales (prisión 48 a 96 meses, multa 100 a 1000 S.M.L.M.V.).

- Artículo 269G: Suplantación de sitio Web para Capturar Datos Personales (prisión 48 a 96 meses, multa 100 a 1000 S.M.L.M.V.).

[1] MINTIC, 2009. LEY 1273 (5 de enero de 2009). [En línea]. [Consulta: 30 agosto 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

- Artículo 269H: Circunstancias de Agravación Punitiva (las penas se aumentan de la mitad a las tres cuartas partes si los delitos se cometen sobre: 1) redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros; 2) Por servidor público activo; 3) aprovechamiento de confianza; 4) dar a conocer información en perjuicio de otro; 5) obteniendo provecho para sí mismo o para un tercero; 6) con fines terroristas; 7) utilizando como instrumento un tercero de buena fe; 8) si es responsable de la administración, manejo o control de dicha información).

En el segundo capítulo (atentados informáticos y otras infracciones) se penaliza los siguientes delitos:

- Artículo 269I: Hurto por Medios Informáticos y Semejantes (penas señaladas en el artículo 240 del código penal entre 3 y ocho años).

- Artículo 269J: Transferencia no Consentida de Activos (prisión 48 a 96 meses, multa 100 a 1000 S.M.L.M.V.).

1.2. LEY 1928 DEL 2018

Por medio de la ley 1928 del 24 de julio de 2018, el gobierno colombiano incluye dentro de su normativa, el Convenio sobre Ciberdelincuencia, adoptado el 23 de noviembre 2001, en Budapest, del Concejo de Europa, y vigente desde el julio de 2004[2].

Con esta incorporación, el estado colombiano busca estar en sintonía con los estándares y esfuerzos conjuntos que realizan los estados suscritos en este convenio a nivel mundial, en la lucha contra la ciberdelincuencia. El estado colombiano con esta adhesión se compromete, a través de la cooperación internacional, el desarrollo de estrategias conjuntas bilaterales y multilaterales, y el fortaleciendo de sus leyes y regulaciones internas nacionales, para continuar la lucha para resguardar el espacio cibernético[3].

[2] DAPRE. 2009. LEY 1273 (24 de julio de 2018). [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

[3] MINTIC. 2020. Adhesión al Convenio de Budapest contra la ciberdelincuencia, clave para Colombia en tiempos de Coronavirus. [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126496:Adhesion-al-Convenio-de-Budapest-contra-la-ciberdelincuencia-clave-para-Colombia-en-tiempos-de-Coronavirus.

1.3. LEY 1581 DE 2012 Y DECRETO 1377 DE 2013

Por medio de la ley 1581 de 2012 y el decreto 1377 de 2013 que reglamentó esta ley, el gobierno nacional dictó las disposiciones generales para la protección de datos personales, con lo cual se desarrolló el marco jurídico que da reconocimiento de los datos e información personal como un bien jurídico tutelado.

La ley 1581 de 2012 Habeas Data, es de mucha importancia, porque desarrolla el derecho constitucional que tiene toda la ciudadanía colombiana para conocer, suprimir, actualizar y rectificar todo tipo de datos personales que estén recolectados, almacenados o que hayan surtido algún tratamiento en bases de datos en entidades públicas y privadas en el territorio colombiano[4]. Para esto, esta ley establece unos principios rectores, los derechos de los titulares de la información, los deberes que adquieren los responsables de tratamiento de los datos, el procedimiento para solicitudes de correcciones de información, entre otros. Como entidad gubernamental designada para la vigilancia y sanciones en cuanto a esta ley, está la Superintendencia de Industria y Comercio[5].

[4] ALCALDIA BOGOTÁ. 2012. Ley 1581 de 2012 Nivel Nacional. [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

[5] MINTIC. 2013. DECRETO 1377 DE 2013. [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf.

2. IMPLICACIONES ETICAS Y LEGALES DE ACUERDO CON EL CASO PROBLEMA

2.1. ANÁLISIS DESDE EL PUNTO DE VISTA LEGAL Y NO ÉTICO

De acuerdo con el análisis que se realizó a los documentos Anexo 2 – Escenario 2 y Anexo 3 – Acuerdo, en primera instancia en la revisión del primer documento Anexo 2 – Escenario 2, donde se expone la situación del problema con la Organización WhiteHouse Security, se afirma que "***este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos*"**, esta afirmación ya empieza a por lo menos, a generar interrogantes, de que algo podría estar sucediendo dentro de la organización WhiteHouse Security, y puede verse en este momento como un primer indicio de que alguna irregularidad o hecho ilegal se pueda estar llevando en esta organización.

En la revisión del segundo documento Anexo 3 – Acuerdo, que es un documento de acuerdo de confidencialidad entre la organización WhiteHouse Security y el estudiante, se observan que existen fragmentos donde se puede evidenciar irregularidades y que hay actividades ilegales que desarrolla la organización, estos fragmentos serán expuestos a continuación, con su respectivo análisis desde el punto de vista ético y legal.

La cláusula primera del acuerdo de confidencialidad, donde se indica el objeto del acuerdo, que dice "***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***", se puede apreciar que este objeto del acuerdo pretende obligar al receptor, que bajo ninguna situación, circunstancia o hecho se puede divulgar la información de la organización, sin embargo existen dos fragmentos que son irregulares, cuando indican lo siguiente, en el primero "***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***", y en el segundo "***la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados***", se deja claro en el primer fragmento que no puede ser divulgada a las autoridades legales, y en el segundo cuando hace referencia de que se dan lugar a procesos ilegales dentro de la organización. Esta cláusula pretende que se haga caso omiso a la obligación que tenemos todos los ciudadanos de denunciar a las autoridades competentes los hechos delictuosos, lo cual es también vulnera el código de ética, que tiene los ingenieros certificados por el COPNIA, que en su capítulo II, articulo

31, numeral f, tiene como deber que todo profesional tiene la obligación de denunciar los delitos[6].

En la cláusula segunda del acuerdo, estipulan cual será la información confidencial que se manejará, esta cláusula dice en el numeral 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***", da a entender que dentro de la información que va obtener la parte receptora, pueden haber datos de acciones de interceptación de información, de chuzadas, y accesos abusivos a sistemas de información, los cuales pueden estar violando la ley, sino son realizados legalmente con sus respectivas autorizaciones judiciales o por entes gubernamentales que tengan competencia. La parte receptora puede verse involucrada en un posible hecho delictivo, dado que está asumiendo el tratamiento de esta información.

En la cláusula cuarta del acuerdo, se estipulan las obligaciones de la parte receptora, dentro de las cuales existen tres clausulas con irregularidades evidentes, que hacen concordancia con los hechos analizados en la cláusula primera del objeto del acuerdo, a continuación, se hace referencia, en la obligación 3 que dice "***No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.***", en esta obligación se entiende que la parte receptora va estar involucrada en el tratamiento de información de actividades de espionaje y apropiación de información de terceros, lo cual es ilegal, y puede verse introducido en un hecho delictivo de violación de datos personales.

En la obligación 4 que dice "**Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.**", sigue reiterando que no podrá realizar denuncias cuando se tenga conocimiento de información ilegal, lo cual es un requerimiento no ético e ilegal, se está violando la ley y por otra parte viola deberes éticos y labores en la profesión de ingeniera, lo cual también llevaría a sanciones.

En la obligación 8 que dice "***Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.***", el mensaje refleja esta exigencia es muy preocupante, porque está trasladando la responsabilidad que debería asumir la organización, al receptor de la información, queriéndolo dejar a su suerte, y dando a conocer que estas situaciones de allanamiento se pueden dar, lo que da a suponer que se están llevando internamente acciones irregulares e ilegales que son sujeto de estos actos judiciales.

[6] COPNIA. Código de Ética para el servicio de la Ingeniería en general y sus profesiones a fines y auxliares. [En línea]. [Consulta: 8 de septiembre de 2020]. En linea en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

2.2. ANÁLISIS DE LOS ANEXOS, CON RELACIÓN A LA VULNERACIÓN DE LA LEY 1273 ARGUMENTANDO CUALQUIER PROCESO ILEGAL

De acuerdo al análisis realizado del documento Anexo 3 – Acuerdo, se puede deducir que dentro la organización WhiteHouse Security, se están llevando en su interior procesos ilícitos, prueba de esto se encuentra, en muchos fragmentos del documento Acuerdo de Confidencialidad, donde hace precisiones puntuales que en el desarrollo de las actividades de la organización, se obtiene información confidencial a través de actividades ilegales, como lo son, interceptaciones de información, chuzadas, espionajes, y accesos abusivos a sistemas informáticos.

Si bien dentro del documento Anexo 3 – Acuerdo, en la parte de las consideraciones se menciona en el punto 2 que "***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.***", indicando que la información se obtiene de manera legal, esto no concuerda con la obligación del acuerdo y con todas las cláusulas donde se da entender que se surten procesos ilegales, por esa razón es evidente que se toman una serie de medidas y prevenciones en el acuerdo de confidencialidad, frente a posibles escenarios donde puedan ser descubiertos, o que puedan ser allanados por alguna autoridad competente.

Frente a estas actividades ilegales, se puede estar vulnerando varios archivos artículos de la ley 1273[7], que se indicaran a continuación:

- **Artículo 269A (Acceso Abusivo a Sistema Informático)**: Este articulo lo puede estar vulnerando la organización Whitehouse Security, al indicar en el Acuerdo de Confidencialidad, en cláusula segunda, que consideran como información confidencial que ellos manejan, como datos secretos tales como "***datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos***"; más sin embargo, esto se tiene que demostrar en una investigación, pero si hay indicios por lo que se indica en el acuerdo.
- **Artículo 269E (Interceptación de Datos Informáticos**): De igual manera que como se mencionaba que vulneraba el artículo 269A, también se podría estar vulnerando este artículo 269E, al considerar dentro la información confidencial que maneja la organización "***datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos***", también se está manejando información de procesos de interceptaciones de datos, entonces, se podrían llegar a imputar cargos bajo este artículo, si se logra demostrar bajo alguna investigación.

[7] MINTIC. 2009. LEY 1273. [En línea]. [Consulta el: 8 de septiembre de 2020]. En linea en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

- **Artículo 269F (Violación de Datos Personales)**: Este es el artículo que a todas luces es el que más evidente se está violando, debido que el acuerdo de confidencialidad es reiterativo en el hecho que el receptor de la información, va tener manejo de información confidencial, que puede ser fruto de procesos de interceptaciones de información, chuzadas, espionajes, y accesos abusivos a sistemas informáticos, y en toda estas se estaría ejerciendo violación a datos personales, al aplicar estas actividades ilegalmente sin la autorización de los entes judiciales o entes gubernamentales competentes, en primera instancia la organización al sustraer información de terceros, sería el máximo responsable y también lo estaría violando el receptor de la información al manipular esta información que fue obtenida de manera ilegal.

- **Artículo 269H (Circunstancia de Agravación Punitiva)**: El receptor de la información puede ser imputado bajo este artículo, que de acuerdo al numeral 8, que dice "***Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.***", al ser el esa personal que está recibiendo la información, la controla y le da manejo, está incurriendo en este delito y puede ser inhabilitado para el ejercicio de su profesión hasta por tres años.

3. DEMOSTRACION DE VULNERABILIDADES EN UN SISTEMA INFORMÁTICO A PARTIR DEL USO DE METODOLOGIAS, TÉCNICAS DE INSTRUSIÓN Y HERRAMIENTAS ESPECIALIZADAS, SOBRE UN ESCENARIO DE MAQUINAS VIRTUALES PROPUESTO

3.1. CONFIGURACION DEL "BANCO TRABAJO" EN SU ENTORNO LOCAL

Para el desarrollo de la presente práctica se utilizó un computador de escritorio con las siguientes características:

- Procesador Ryzen 5 2600, 16 Gb de memoria Ram Ddr4, Disco de estado Solido de 256 Gb, Disco duro de 1 Tb, Tarjeta Gráfica Radeon Rx 570 de 4Gb Ddr5 y Monitor de 25" UltrawideScreen.

Para la implementación del banco de trabajo, siguiendo las indicaciones de la guía de actividades, importé las máquinas virtuales indicadas por el director del curso en el Oracle VM VirtualBox, con los sistemas operativos y estas configuraciones:

- Kali Linux, con 2048 MB de memoria ram, funcionando con un procesador con 1 CPU, 16 MB de video, Red Adaptador puente.

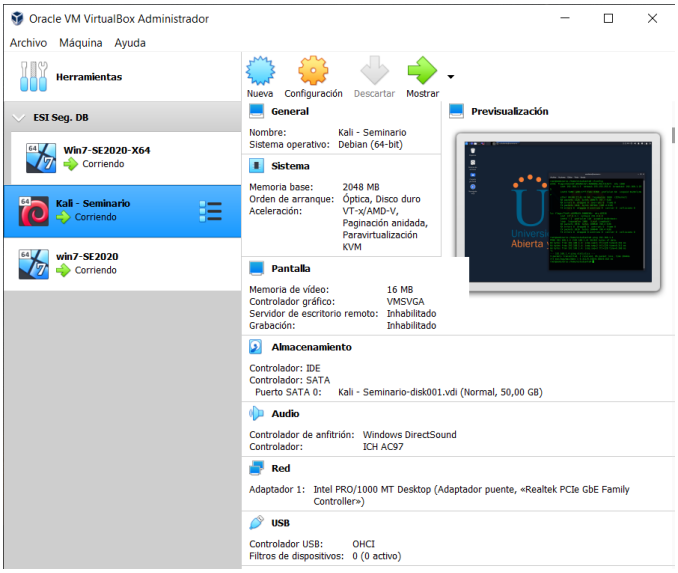
- Windows 7 - SE2020-X64, con 1775 MB de memoria ram, funcionando con un procesador con 1 CPU, 36 MB de video, Red Adaptador puente.

- Windows 7 - SE2020-X86, con 1775 MB de memoria ram, funcionando con un procesador con 1 CPU, 36 MB de video, Red Adaptador puente.

A continuación, se presentarán evidencias de la implementación.

A continuación, se evidencia la Implementación de la maquina Kali Linux:

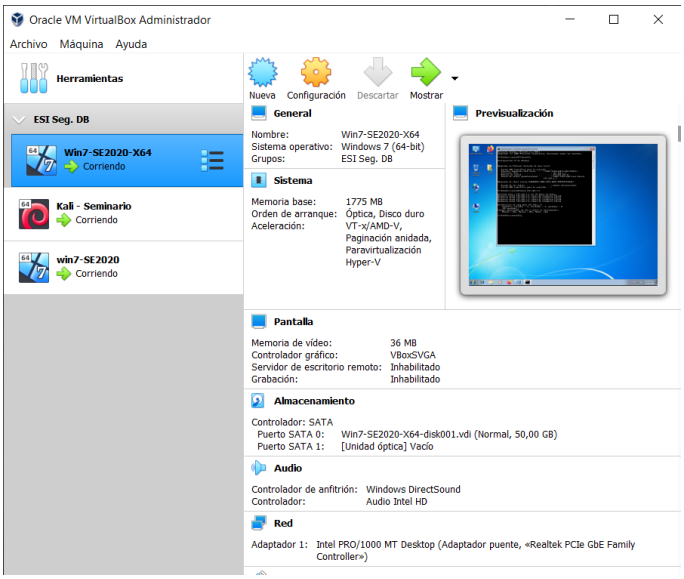
Figura 1 - Máquina Kali Linux



Fuente: El Autor.

A continuación, se evidencia la Implementación de la maquina Win7 x64:

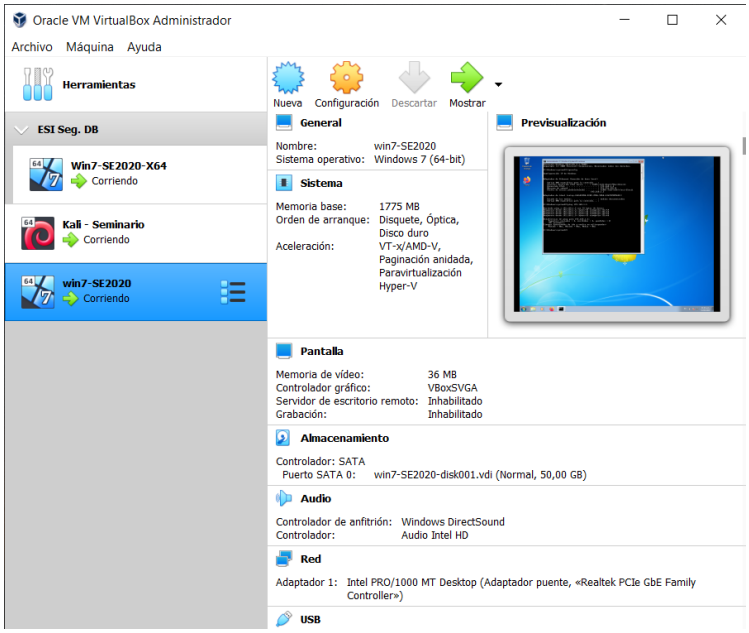
Figura 2 - Máquina Win7 x64



Fuente: El Autor.

A continuación, se evidencia la Implementación de la maquina Win7 x86:

Figura 3 - Máquina Win7 x86



Fuente: El Autor.

3.2. FASE DE RECOLECCION DE INFORMACION:

De acuerdo con el análisis de archivo suministrado “Anexo 4 – Escenario 3”, en la situación del problema se da a conocer información que es considerada importante en esta fase recolección de información, se menciona a continuación:

- Las maquinas que serán el objetivo de las pruebas de intrusión, se indica que son dos equipos con sistema operativo Windows 7, uno con arquitectura x64 y el otro con x86.

- Ambos equipos cuentan con un servicio activo SMBv1 para compartir impresoras y archivos dentro de la red, que está desactualizado.

- Los sistemas operativos se encuentren desactualizados, su última actualización fue el 5 de febrero de 2017.

- La organización reporta fuga de información y pantallazos azul recurrentes en uno de los equipos.

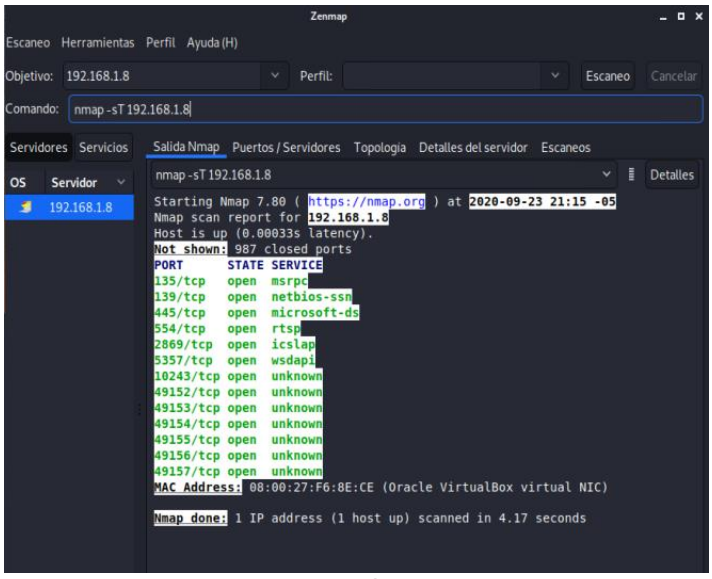
Para la práctica del proceso de pentesting, se utilizará un entorno controlado de máquinas virtuales, en este caso se hace uso de dos máquinas con sistema operativo Win 7 x64 y Win 7 x86 como víctima, y una maquina con sistema operativo Kali Linux como maquina atacante.

3.3. FASE DE ENUMERACIÓN:

Se utilizó la herramienta de código abierto Zenmap, que es la aplicación GUI oficial de Nmap Security Scanner, esta fue instalada en la maquina Kali Linux, y a través de ella se pudo identificar los servicios que se ejecutaban en las dos máquinas objetivo según el caso de estudio. Se realizó un escaneo de puertos TCP y UDP a las maquinas objetivos con IP´s 192.168.1.8 (Win 7 X64) y 192.168.1.9 (win 7 X86), para recolectar información de los puertos, servicios activos, las versiones y el sistema operativo, con la finalidad de detectar información que sirva para el estudio en esta fase.

Se utilizaron los siguientes comandos:
Con el comando “nmap -sT 192.168.1.8” se detectaron trece (13) puertos y servicios abiertos en TCP, en la maquina Win 7 X64.

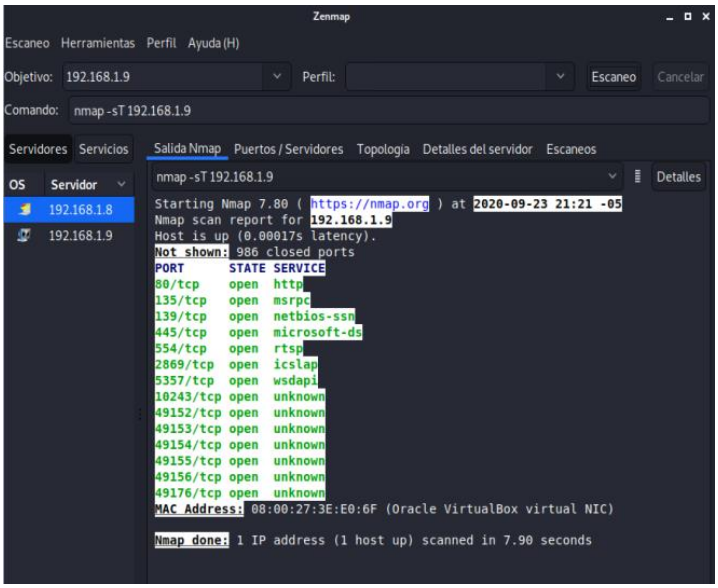
Figura 4. Escaneo de puertos TCP con Zenmap Win 7 X64



Fuente: El Autor.

Con el comando “nmap -sT 192.168.1.9” se detectaron catorce (14) puertos y servicios abiertos en TCP, en la maquina Win 7 X86.

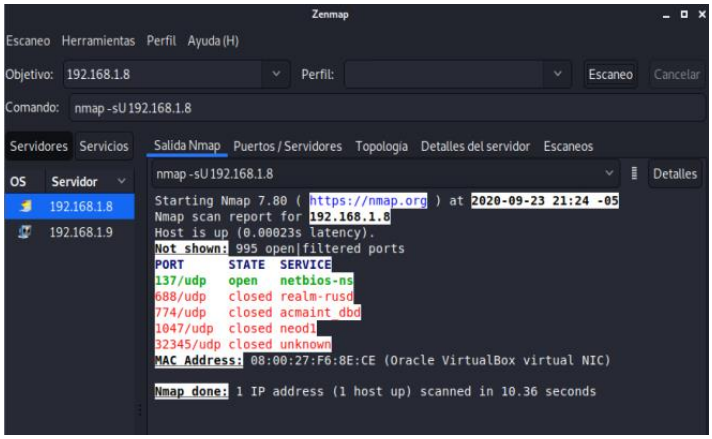
Figura 5. Escaneo de puertos TCP con Zenmap Win 7 X86



Fuente: El Autor.

Con el comando “nmap -sU 192.168.1.8” se detectaron un (1) puerto y servicios abiertos en UDP, en la maquina Win 7 X64.

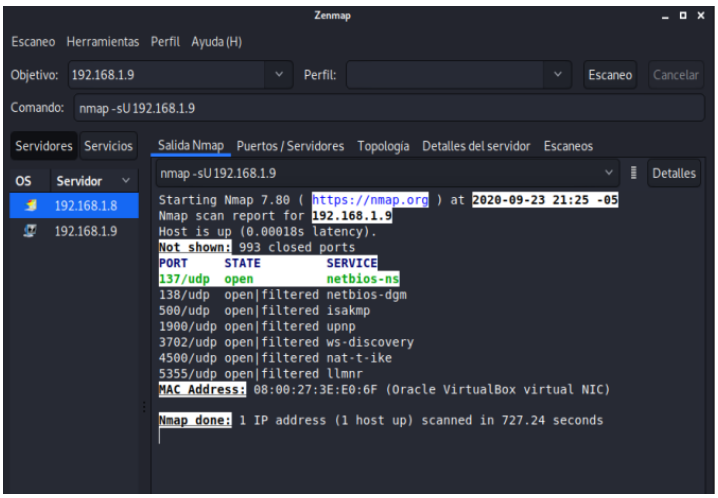
Figura 6. Escaneo de puertos UDP con Zenmap Win 7 X64



Fuente: El Autor.

Con el comando “nmap -sU 192.168.1.9” se detectaron un (1) puerto y servicio abiertos en UDP, en la maquina Win 7 X86.

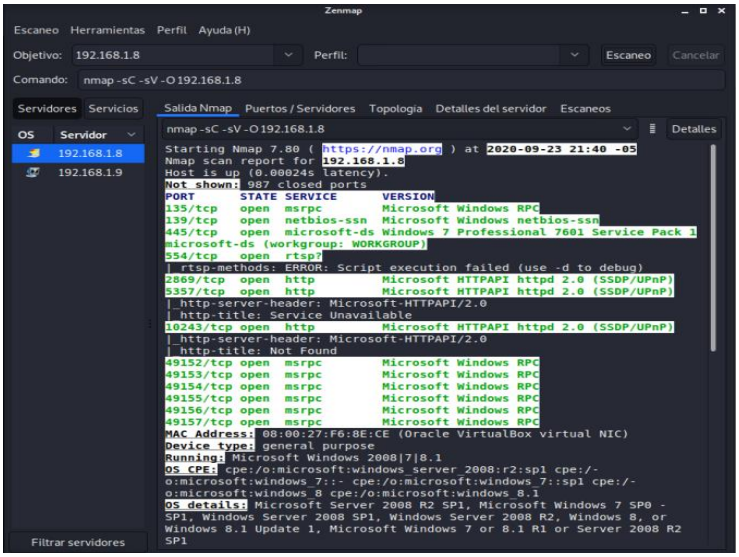
Figura 7. Escaneo de puertos UDP con Zenmap Win 7 X86



Fuente: El Autor.

Con el comando “nmap -sC -sV -O 192.168.1.8” se realizó un escaneo agresivo, utilizando los comandos para escaneo a través de scripts, detección de versiones y detección de sistema operativo, en la maquina Win 7 X64.

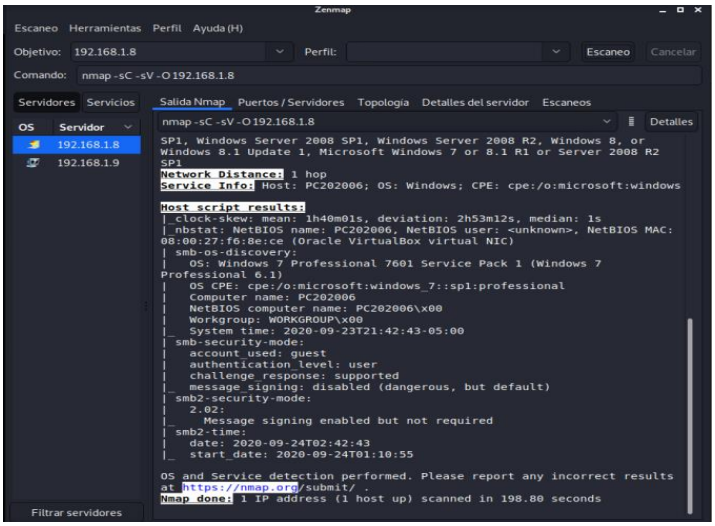
Figura 8. Escaneo agresivo con Zenmap Win 7 X64



Fuente: El Autor.

A continuación, la segunda parte del reporte del escaneo agresivo en Win7 X64:

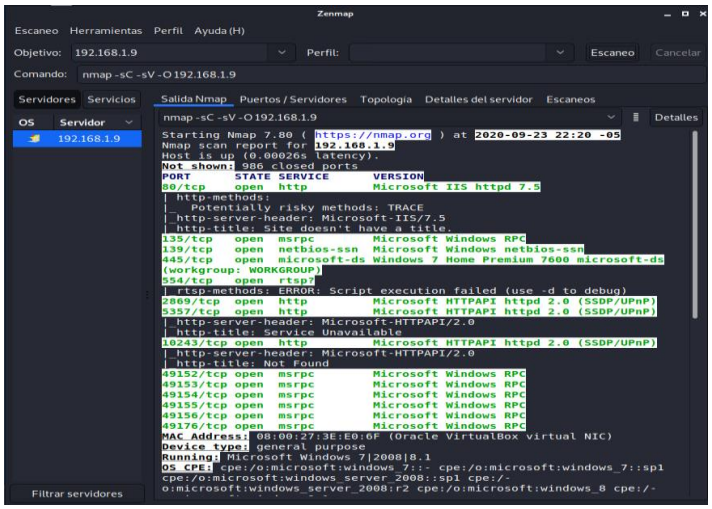
Figura 9. Escaneo agresivo parte 2 con Zenmap Win 7 X64



Fuente: El Autor.

Con el comando “nmap -sC -sV -O 192.168.1.9” se realizó un escaneo agresivo, utilizando los comandos para escaneo a través de scripts, detección de versiones y detección de sistema operativo, en la maquina Win 7 X86.

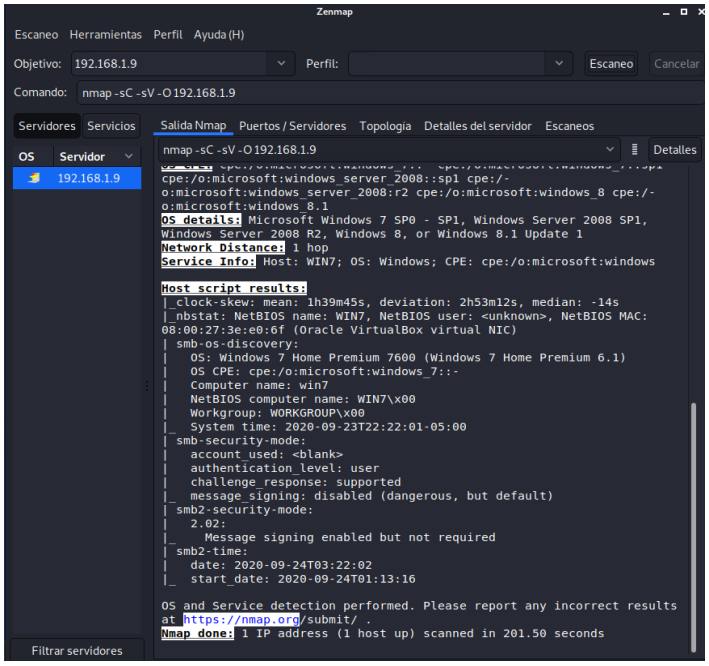
Figura 10. Escaneo agresivo con Zenmap Win 7 X86



Fuente: El Autor

A continuación, la evidencia de la segunda parte del escaneo agresivo sobre Win7 X86:

Figura 11. Escaneo agresivo parte 2 con Zenmap Win 7 X86



Fuente: El Autor.

A continuación, se evidencia en las siguientes tablas, el resumen de los puertos, servicios y versiones encontradas en el puerto TCP en las maquinas Win 7 X64 con IP 192.168.1.8 y Win 7 X86 con IP 192.168.1.9, de acuerdo con los procedimientos descritos que fueron realizados:

Tabla 1. Resumen escaneo de puertos TCP con NMAP en Win 7 X64

Puerto	Estado	Servicio	Versión
135/tcp	Abierto	msrpc	Microsoft Windows RPC
139/tcp	Abierto	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	Abierto	Microsoft-ds	Windows 7 Professional 7601 Service Pack 1
554/tcp	Abierto	rtsp	
2869/tcp	Abierto	http	Microsoft HTTPAPI httdp 2.0 (SSDP/UPnP)

5357/tcp	Abierto	http	Microsoft HTTPAPI httdp 2.0 (SSDP/UPnP)
10243/tcp	Abierto	http	Microsoft HTTPAPI httdp 2.0 (SSDP/UPnP)
49152/tcp	Abierto	msrpc	Microsoft Windows RPC
49153/tcp	Abierto	msrpc	Microsoft Windows RPC
49154/tcp	Abierto	msrpc	Microsoft Windows RPC
49155/tcp	Abierto	msrpc	Microsoft Windows RPC
49156/tcp	Abierto	msrpc	Microsoft Windows RPC
49157/tcp	Abierto	msrpc	Microsoft Windows RPC

Tabla 2. Resumen escaneo de puertos TCP con NMAP en Win 7 X86

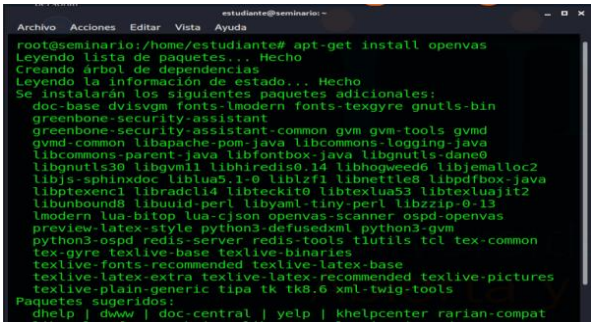
Puerto	**Estado**	**Servicio**	**Versión**
80/tcp	Abierto	http	Microsoft IIS httpd 7.5
135/tcp	Abierto	msrpc	Microsoft Windows RPC
445/tcp	Abierto	Microsoft-ds	Windows 7 Home Premiun 7600 microsoft-ds
554/tcp	Abierto	rtsp	
2869/tcp	Abierto	http	Microsoft HTTPAPI httdp 2.0 (SSDP/UPnP)
5357/tcp	Abierto	http	Microsoft HTTPAPI httdp 2.0 (SSDP/UPnP)
10243/tcp	Abierto	http	Microsoft HTTPAPI httdp 2.0 (SSDP/UPnP)
49152/tcp	Abierto	msrpc	Microsoft Windows RPC
49153/tcp	Abierto	msrpc	Microsoft Windows RPC
49154/tcp	Abierto	msrpc	Microsoft Windows RPC
49155/tcp	Abierto	msrpc	Microsoft Windows RPC
49156/tcp	Abierto	msrpc	Microsoft Windows RPC
49157/tcp	Abierto	msrpc	Microsoft Windows RPC

3.4. FASE DE ANÁLISIS DE VULNERABILIADES:

Se utilizó la herramienta de código abierto OpenVas, que es un escáner de vulnerabilidades muy popular, que sirve para la identificación de fallas de seguridad.
Se realizó un escaneo a las maquinas objetivos con IP´s 192.168.1.8 (Win 7 X64) y 192.168.1.9 (win 7 X86), con la finalidad de que identificaran las vulnerabilidades en ambas maquinas, y que de estos resultados sirvieran para poder explotar alguna vulnerabilidad conocida.

Para la instalación de la herramienta OpenVAS, se necesitó tener completamente actualizado el sistema operativo Kali Linux, para ellos previamente se utilizaron los comandos “apt-get update”, “apt-get upgrade” y “apt-get dist-upgrade”. Una vez el sistema operativo actualizado, se procedió a la instalación de la herramienta OpenVas a nivel de consola por medio del comando “apt-get install openvas”.

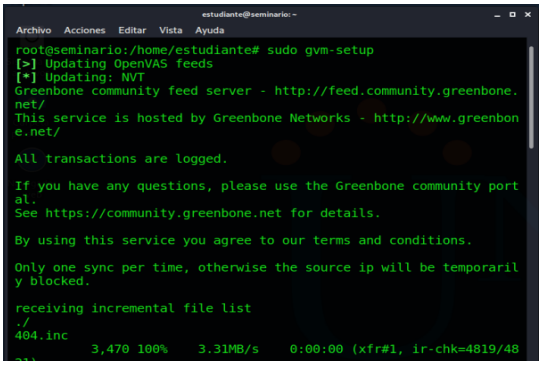
Figura 12. Instalación OpenVas.



Fuente: El Autor.

Después de su instalación, se procedió a su configuración con el comando “sudo gvm-setup”

Figura 13. Configuración OpenVas.

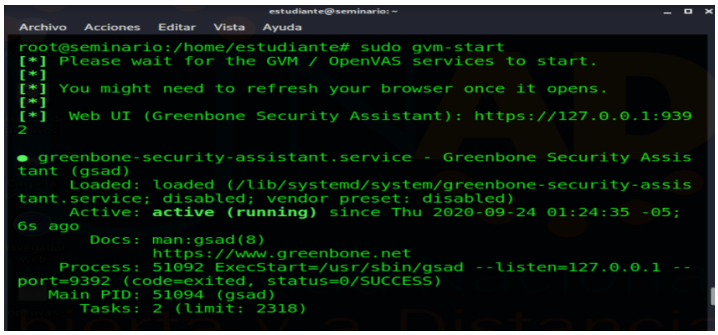


Fuente: El Autor.

Dentro del proceso de configuración, la aplicación arroja los datos de usuario: “admin” y password: “3dbcca68-18b8-44ª9-8be6-4067ee0c72e0”.

Posteriormente se hizo arranque al OpenVas por medio del comando “sudo gvm-start”, en el cual se dio a conocer la URL para abrir la interfaz gráfica de la herramienta: “https://127.0.0.1:9392”.

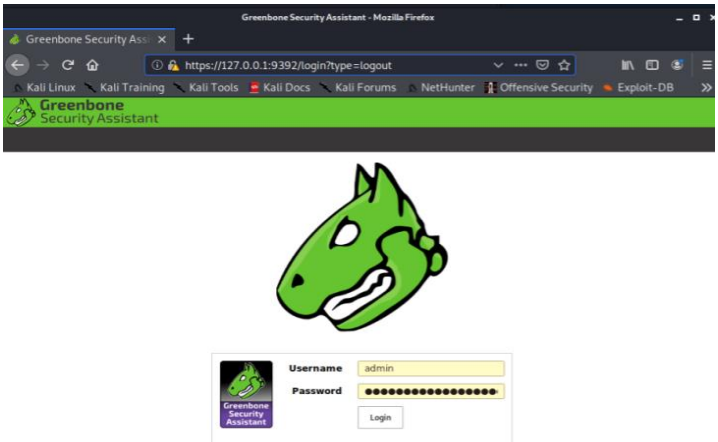
Figura 14. Arranque del OpenVas.



Fuente: El Autor.

A continuación, se evidencia el inicio de la interfaz gráfica del OpenVas:

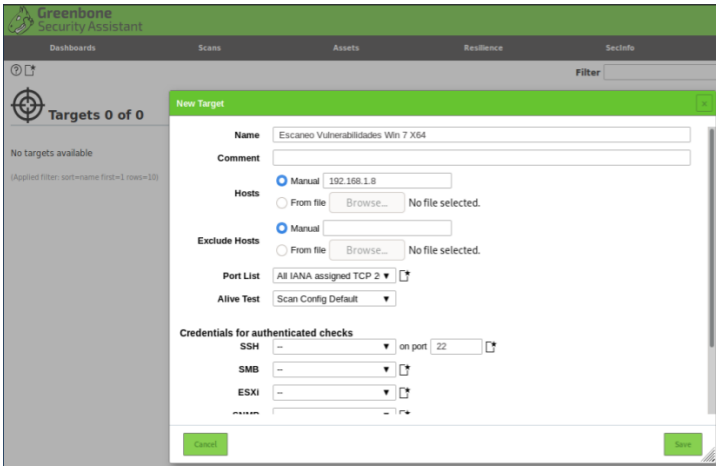
Figura 15. Inicio interfaz gráfica del OpenVas en navegador web.



Fuente: El Autor.

Como siguiente paso se procedió a registrar los Targets por la opción “Configurations” y después en “New Target”, se incluyeron los dos objetivos a escanear, con IP´s 192.168.1.8 (Win 7 X64) y 192.168.1.9 (win 7 X86).

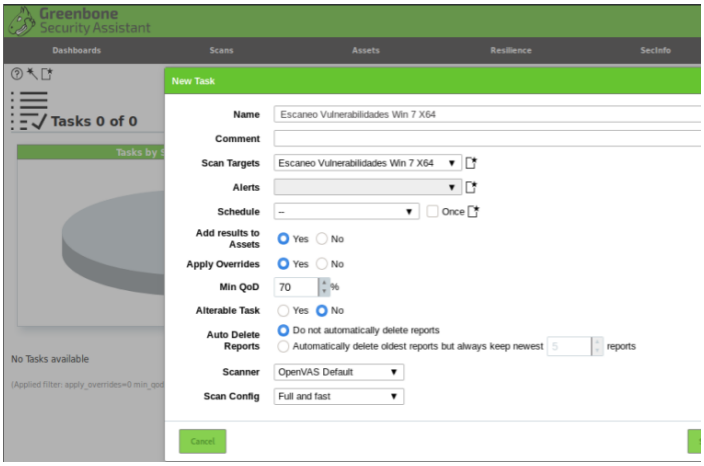
Figura 16. Registro de New Targets en OpenVas.



Fuente: El Autor.

Se registraron las tareas de escaneo a ambas maquinas con IP´s 192.168.1.8 (Win 7 X64) y 192.168.1.9 (win 7 X86), estableciéndose tipo de escaneo “OpenVAS Default”.

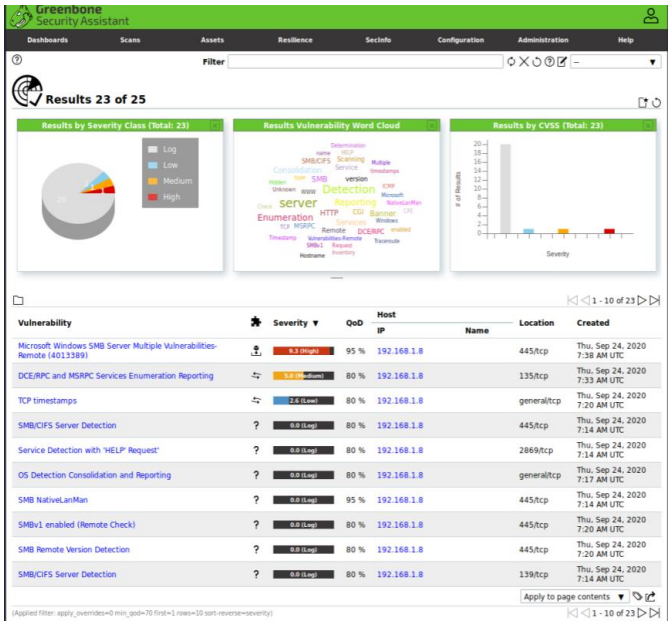
Figura 17. Registro de New Task en OpenVas.



Fuente: El Autor.

Una vez creado los “Targets” y las “Task”, se realizó los escaneos a las maquinas, arrojando los siguientes resultados para la maquina Win 7 X64 con IP 192.168.1.8:

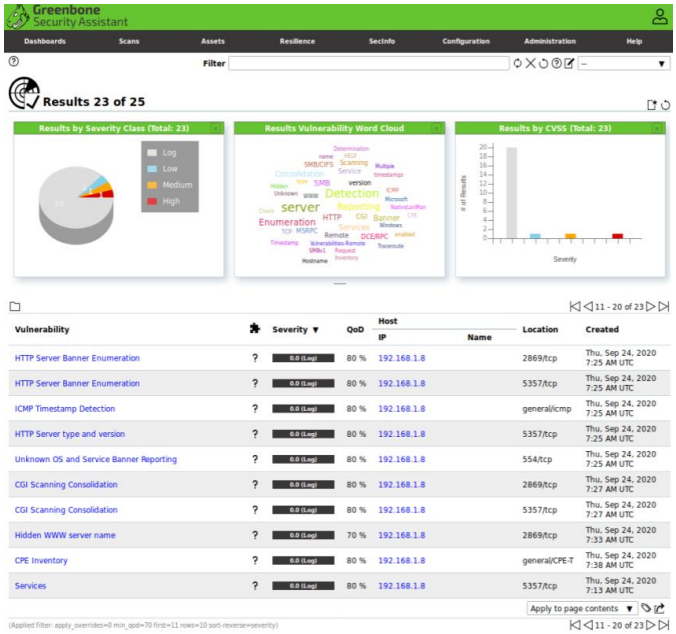
Figura 18. Resultado parte 1 escaneo OpenVas a Win 7 X64.



Fuente: El Autor.

A continuación, la segunda parte del resultado del escaneo a Win 7 X64:

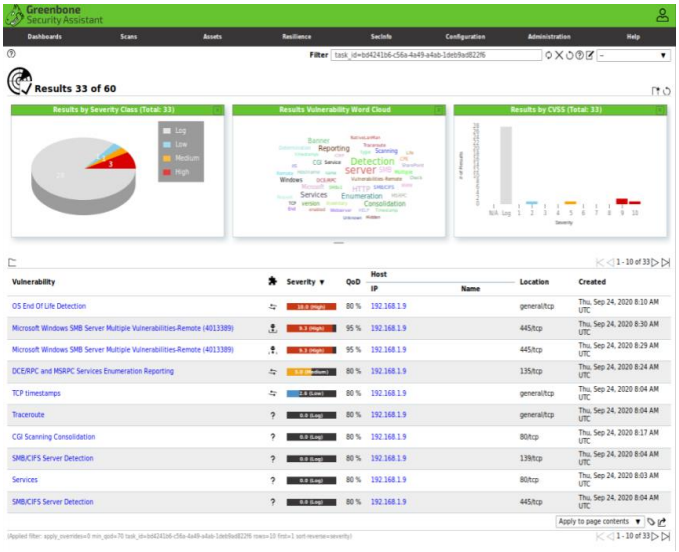
Figura 19. Resultado parte 2 escaneo OpenVas a Win 7 X64.



Fuente: El Autor.

Y para la maquina la maquina Win 7 X86 con IP 192.168.1.9, arrojó los siguientes resultados:

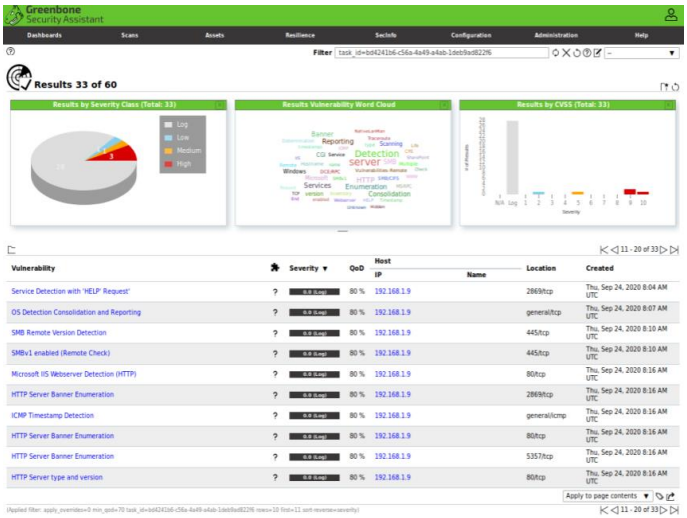
Figura 20. Resultado parte 1 escaneo OpenVas a Win 7 X86.



Fuente: El Autor.

A continuación, la segunda parte del resultado del escaneo a Win 7 X86:

Figura 21. Resultado parte 2 escaneo OpenVas a Win 7 X86.



Fuente: El Autor.

En la siguiente tabla se encuentran los principales fallos encontrados en ambas maquinas Windows 7:

Tabla 3. Fallos encontrados en Escaneos con OpenVas.

No.	Vulnerabilidad	Hosts	Localización	Severidad	Descripción
1	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	192.168.1.8 192.168.1.9	445 / tcp	ALTO (9.3)	Esta vulnerabilidad es de un impacto muy grave, y permite la ejecución remota de código, por medio de ataques al servidor Microsoft Message Block 1.0 (SMBv1), afecta al sistema operativo de las maquinas en estudio, con el sistema operativo Windows 7 x64 y x86 Service pack 1, entre muchas otras versiones de Windows. La vulnerabilidad puede ser encontrada con los siguientes ID en el CVE: (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-148). La explotación de esta vulnerabilidad le permitiría al atacante a través de un ataque con Exploits (ejemplo: Eternalblue, Doublepulsar), iniciar sesión con privilegios asociados con el usuario y poder ver, modificar, eliminar datos, instalar programas, crear cuentas de usuarios, etc. Para dar solución a esta vulnerabilidad, se requiere actualizar el sistema operativo con la actualización MS17-010, o también se podría bloquear el puerto 445.

2	OS end Of Life Detection	192.168.1.9	general / tcp	ALTO (10.0)	Esta vulnerabilidad es de impacto alto, se refiere a que el sistema operativo del host escaneado (Windows 7), ha llegado al final de vida útil, esto tiene muchas implicaciones, ya que un sistema operativo EOL, cuando pierde soporte de actualizaciones y parches de seguridad, se vuelve muy vulnerable a las fallas de seguridad que sean detectadas en la actualidad, y también puede ir perdiendo compatibilidad con programas, además de generar altos costos operativos para mantener estos sistemas antiguos. Para dar solución a este tipo de vulnerabilidad, se hace necesario que se realice actualización de las estaciones de trabajo y se haga migración de hardware y software a versiones actuales, que puedan garantizar un soporte en el tiempo.
3	DCE/RPC and MSRPC Services Enumerations Reporting	192.168.1.8 192.168.1.9	135 / tcp	MEDIO (5.0)	Esta vulnerabilidad es de impacto medio, que permite realizar consultas a través de la conexión al puerto 135, aprovechando fallas de los servicios DCE/RPC y MSRPC, lo cual le permitiría al atacante recabar información del Host remoto, para encontrar otras vulnerabilidades. Esta vulnerabilidad puede ser mitigada aplicando filtrado de tráfico entrante en el puerto 135.

4	TCP timestamps	192.168.1.8 192.168.1.9	general / tcp	BAJO (2.6)	Esta vulnerabilidad es de un impacto muy bajo, se refiere a que un atacante podría tratar de calcular el tiempo de actividad del host remoto, y con esta información servirle de insumo para futuros ataques. Esta vulnerabilidad podría mitigarse, inhabilitando el TCP Timestamps, sin embargo, se deben analizar en cada caso particular, ya que el Timestamps cumple una función importante, y deshabilitarlo podría generar inconvenientes con procesos asociados al protocolo TCP.

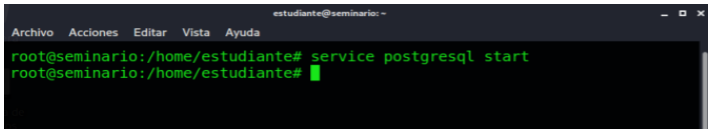
3.5. FASE DE EXPLOTACIÓN:

Se utilizó la herramienta Metasploit Framework, que es de código abierto, y es un software muy popular, utilizado para la ejecución de exploits, contando con una base de datos con una gran cantidad de exploits y payloads, los cuales son usados para realizar pentesting.

En el desarrollo de la fase Anterior, con el programa OpenVas se logró identificar una vulnerabilidad común en ambas maquinas Win 7 X64 y Win 7 X86, encontrándose que CVE-2017-0144, la cual explota una vulnerabilidad critica en el puerto 445, en el servidor SMBv1.

Como primer paso, antes de que se ejecutara el Metasploit Framework, se dio inicio al servicio Postgresql, a través del comando “service postgresql start”:

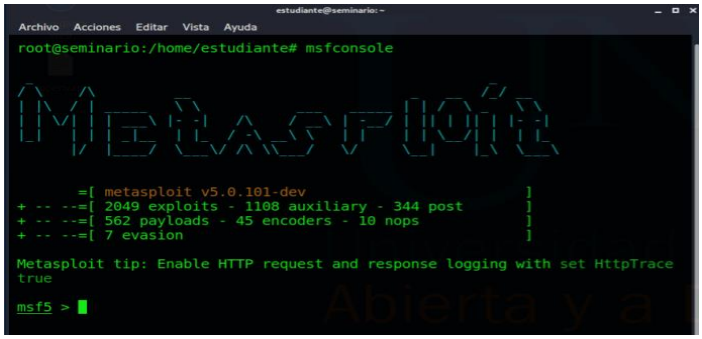
Figura 22. Arranque del servicio postgresql.



Fuente: El Autor.

Se ejecutó el Metasploit Framework por medio del comando “msfconsole”:

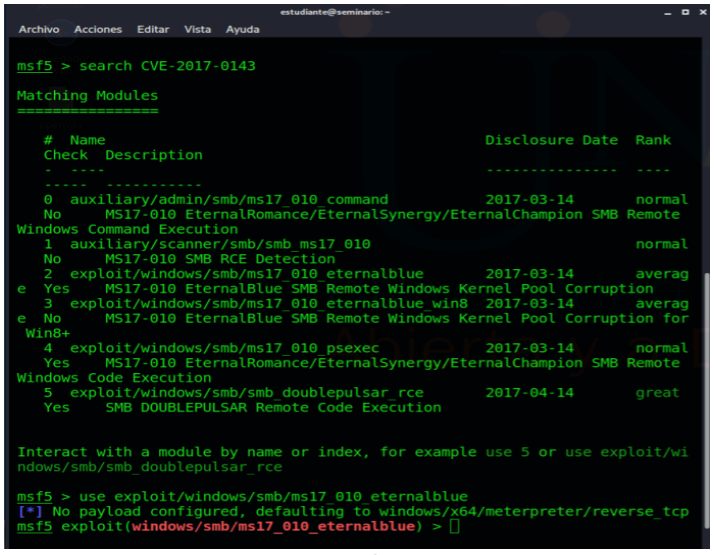
Figura 23. Ejecución de Msfconsole.



Fuente: El Autor.

Se realizó la búsqueda del exploit relacionado con CVE-2017-0144, por medio del comando “search CVE-2017-0144”. Una vez identificado el exploit a utilizar, se procedió a seleccionar el exploit, para esto se utilizó el comando “use exploit/windows/smb/ms17_10_eternalblue”, y automáticamente el programa asigna el Payload por default “windows/x64/meterpreter/reverse_tcp”:

Figura 24. Comandos Search y Use.



Fuente: El Autor.

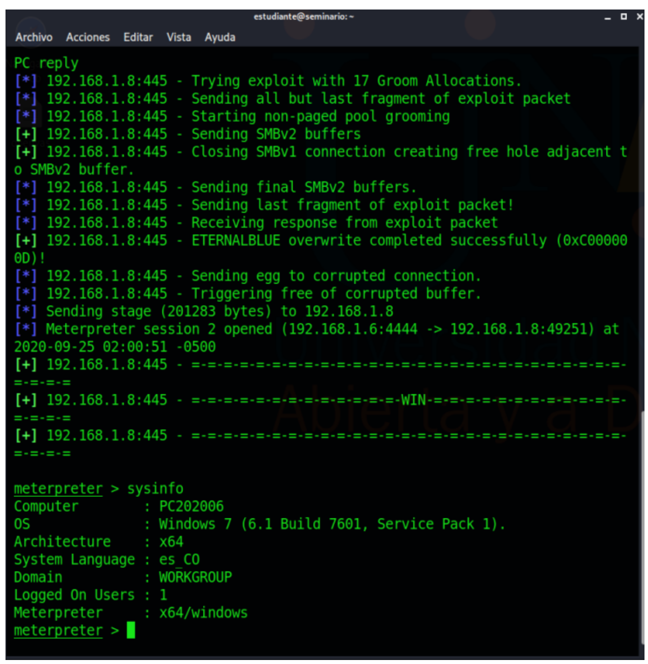
se estableció a configurar la IP de la maquina atacada, en primera instancia se atacó la maquina Win 7 X64, a través de los comandos “set RHOST 192.168.1.8”:

Figura 25. Set RHOST.

Fuente: El Autor.

Se ejecutó el exploit con el comando “**exploit**”, y se logró de manera exitosa iniciar sesión con el meterpreter. Una vez dentro de la sesión, con el comando “**sysinfo**”, se verificó la información de la maquina vulnerada.

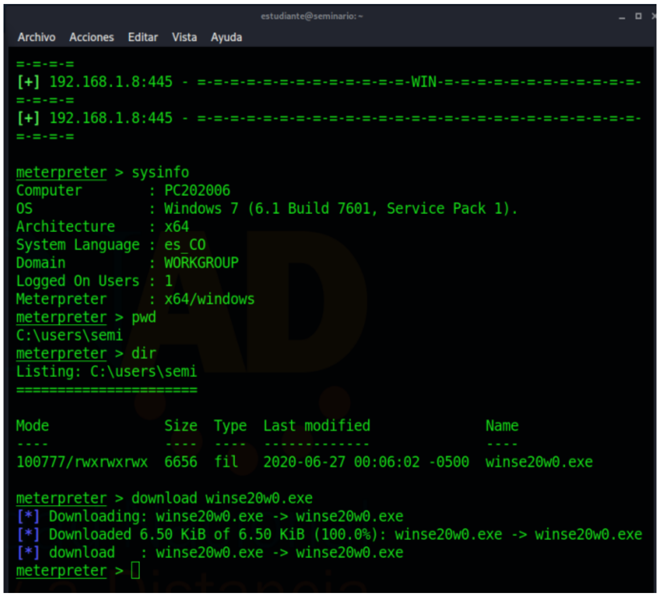
Figura 26. Ejecución Exploit y Sysinfo.



Fuente: El Autor.

Se realizó la búsqueda del archivo “winse20w0.exe”, ubicándose en la carpeta “C:/users/semi”.

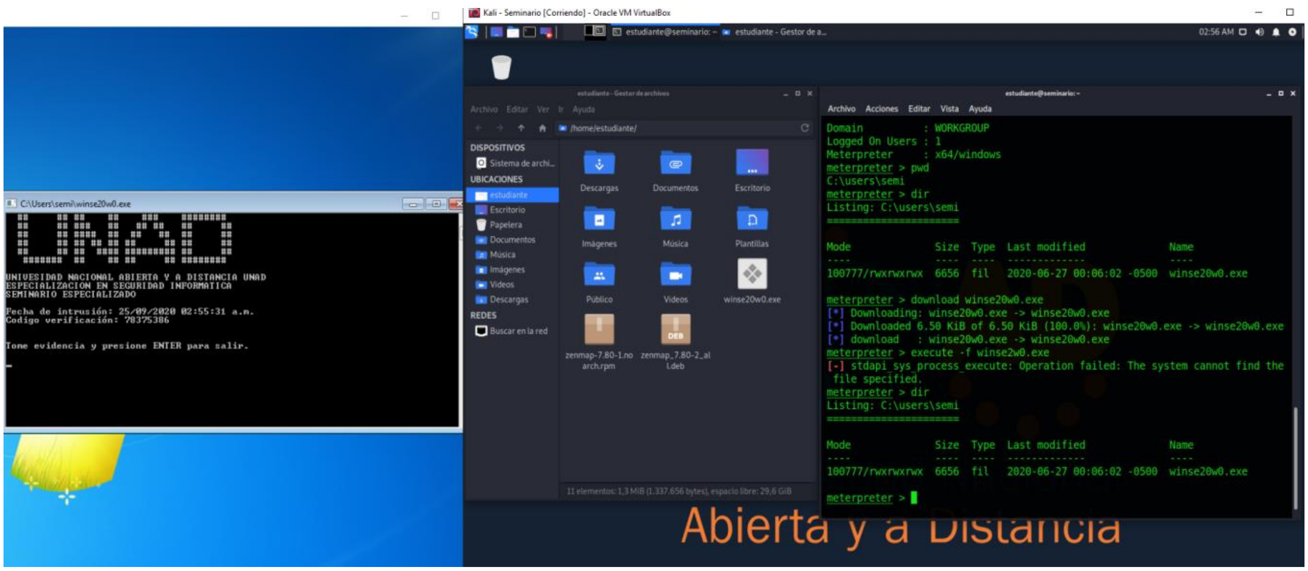
Figura 27. Ubicación y descargar archivo winse20w0.exe.



Fuente: El Autor.

Y se descargó el archivo con el comando “**download winse20w0.exe**”:

Figura 28. Evidencia archivo winse20w0.exe descargado.



Fuente: El Autor.

Encontrando la siguiente información al ejecutar el archivo:

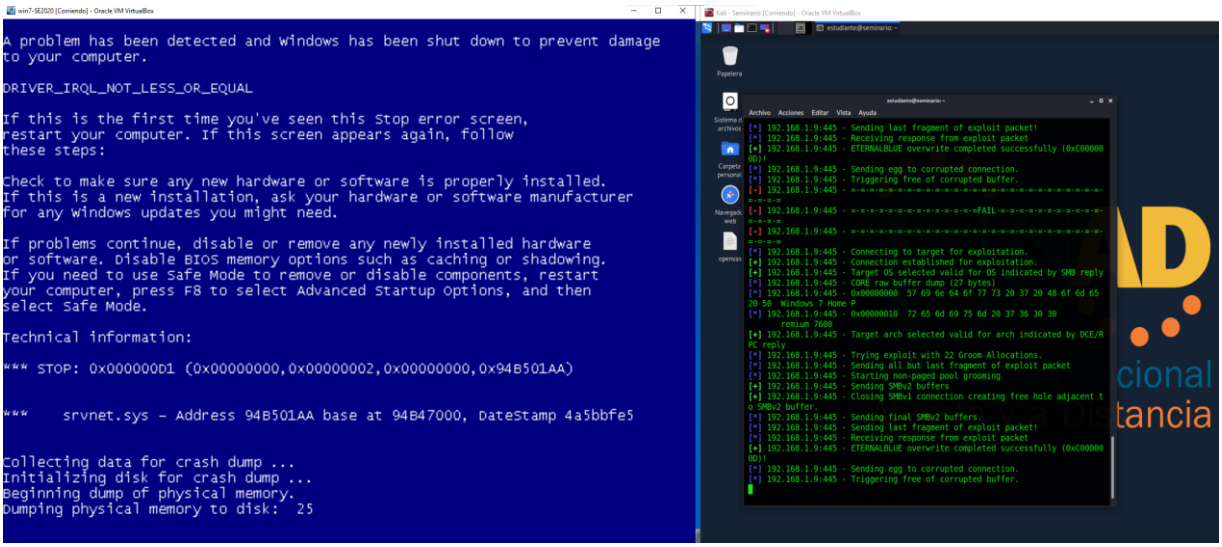
“UNAD
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION EN SEGURIDAD INFORMMATICA
SEMINARIO ESPECIALIZADO

Fecha de intrusión: 25/09/2020 02:55:31 a.m.
Código de verificación: 78375386”

Continuando el proceso de explotación, utilizando nuevamente el Metasploit Framework, se procedió a explotar la misma vulnerabilidad CVE-2017-0144 en Win 7 X86 con IP 192.168.1.9, atacando el puerto 445, en el servidor SMBv1.

Se utilizan los mismos comandos usados para la explotación de la maquina anterior, y al llegar al momento de ejecutar el exploit “exploit/windows/smb/ms17_10_eternalblue”, en el desarrollo del procedimiento, la maquina objetivo arroja pantalla azul, sin embargo, el exploit no logra establecer sesión, y realiza nuevamente otro intento y sucede lo mismo, como se muestra a continuación:

Figura 29. Ejecución de exploit y pantallazo azul



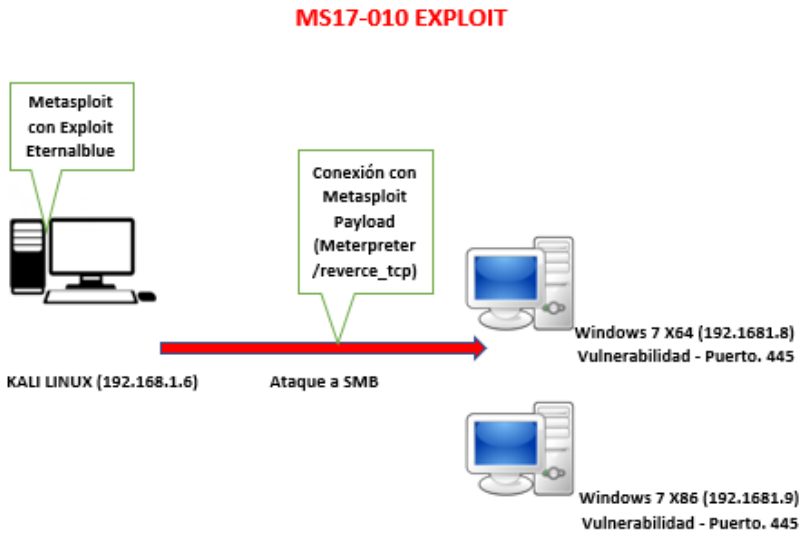
Fuente: El Autor.

El ataque con el exploit “exploit/windows/smb/ms17_10_eternalblue”, realiza un desbordamiento de buffer en la maquina objetivo para sobrescribir el búfer SMBv1, y así establecer la conexión del atacante.

Este ataque cuando se realiza en una maquina compatible con arquitectura X64, si la vulnerabilidad está presente, y se dan las condiciones, este se realiza de manera exitosa, sin embargo, en este caso se puede apreciar que al realizar el proceso en una maquina victima con arquitectura X86, el ataque está generando que el sistema operativo presente pantalla azul, esto muy posiblemente a la no compatibilidad del exploit eternalblue con esta arquitectura X86.

Debido a lo anterior, se puede deducir que esta era la razón por la que la organización reportaba que una de sus máquinas (Win 7 x86), presentaba reiteradamente pantallazos azules. Esto quiere decir que para explotar esta máquina Win 7 X86, se requiere la utilización de otro exploit diferente que ataque esta misma vulnerabilidad, pero que, si sea compatible con la arquitectura X64.

Figura 29. Exploit MS17-010.



Fuente: El Autor.

4. MEDIDAS PARA LA HARDENIZACIÓN Y MITIGACION DE LOS FALLOS DE SEGURIDAD ENCONTRADOS EN EL ESCENARIO DE MAQUINAS VIRTUALES

Teniendo en cuenta el trabajo presentado anteriormente correspondiente a la unidad 2 - Etapa 3, donde se realizó un ejercicio Red Team de ataque de intrusión a dos máquinas Windows 7 x86 y x64, en el cual se explotó una vulnerabilidad común en ambas maquinas, en el servicio SMBv1, específicamente el fallo identificado como CVE-2017-0144, aprovechando que no tenían aplicados los parches de seguridad MS17-010, se pudo a través de la herramienta Metasploit Framework, utilizando el exploit “eternalblue”, se logró la intrusión.

Para evitar que sucedan los ataques de seguridad informática que fueron objeto de estudio en el ejercicio de Red Team, se propone la aplicación de una serie de medidas de hardenización, tanto de software como en hardware, que ayuden a mitigar las fallas que se identificaron a nivel en los sistemas operativos y en la red.

- Implementar una política de actualizaciones para los sistemas operativos y el software utilizado en los equipos de la empresa, que permita mantener y hacer seguimiento para que los sistemas operativos y el software se encuentren siempre actualizados y debidamente configurados para este fin.

- Deshabilitar protocolo SMBv1 en el sistema operativo o través del bloqueo de los puertos en el firewall todas las conexiones SMB salientes del puerto TCP 445 y sus relacionados en los puertos UDP 137-138 y TCP 139.

- Se hace necesario la implementación de software antivirus en los equipos de la empresa, recomendablemente alguna solución empresarial de antivirus endpoint, que permita prevenir, detectar y remediar software malicioso.

- Se propone la implementación de un Firewall para la protección de la red de la empresa, que permita bloquear el tráfico no deseado. También se sugiere la activación y configuración de firewall en todos los equipos de la empresa.

- Se propone la implementación de un servidor para realizar monitorización de la red de la empresa, utilizando la herramienta SNORT, le permitirá hacer seguimiento al tráfico y detectar ataques en la red.

- Implementar una política de copias de seguridad para los equipos de la empresa, que permita recuperar la información en caso de ser necesario ante algún incidente o desastre. También se sugiere la adquisición e implementación de software especializado para la realización de las copias de seguridad de manera automática y programada.

- Se requiere que la empresa realice de manera urgente la migración y actualización de la versión del sistema operativo utilizado en sus equipos de trabajo, ya que se está utilizando actualmente una versión de Windows que ha llegado al final de su vida útil y ya no cuenta con soporte de actualizaciones.

- Se recomienda la deshabilitación del acceso remoto en los sistemas operativos de las maquinas, en caso de requerir el control remoto de una máquina, se debe configurar para que restrinja el acceso a un número muy limitado de usuarios, al mínimo las conexiones concurrentes, estableciendo canal cifrado utilizando SSH.

5. CONCLUSIONES

- La implementación de equipos Red Team & Blue Team dentro de las organizaciones permite desarrollar dentro de estas, procesos de mejoras continuas en la seguridad informática a corto y a largo plazo, a partir de dos perspectivas conjuntas, con Red Team con un enfoque de seguridad ofensiva, realizando emulación de ataques informáticos para explotar vulnerabilidades existentes en los sistemas y/o aplicaciones y con Bluen Team con un enfoque de seguridad defensiva, a través de la prevención, vigilancia y la defensa ante ataques informáticos.

- Se concluye que la falla de seguridad (CVE-2017-0144) mencionada en el planteamiento del problema “Anexo 4 - Escenario 3” era real y muy grave, esto se pudo comprobar en las fases de enumeración y análisis de vulnerabilidades, y debido a que no estaba parchada, pudo ser explotada a través del exploit “eternalblue”, otorgando al atacante acceso a las maquinas objetivo; en la maquina Win 7 x64 el exploit fue efectivo, en cambio en la maquina Win 7 x86 el exploit se pudo comprobar que no era compatible con la arquitectura de 64 bits, por esta razón generaba que esta máquina atacada arrojara pantallazos azules.

- Hoy en día la realización de pruebas de pentesting son muy viables realizarlas requiriendo inversiones bajas, apoyándose en software libre, ya que existen una serie de herramientas de seguridad especializadas de código abierto que permiten desarrollar estos procesos de manera eficaz, si se cuenta con el conocimiento necesario, sin embargo es fundamental tener en cuenta las metodologías y técnicas de intrusión, ya que esto permite poder desarrollar estos tipos de procesos de manera ordenada, de acuerdo con unas fases y momentos, que permitan obtener resultados evidenciables.

- Los profesionales encargados de seguridad informática tienen una gran responsabilidad al ser ellos los que administran y protegen la información; esta responsabilidad los expone a innumerables situaciones, donde por diferentes intereses, se pretenda vulnerar contra la confidencialidad, integridad y disponibilidad de la información, y frente a esto el profesional debe apelar a esos lineamientos éticos y morales apropiados en el transcurso de la vida, teniendo como base desde el hogar y continuando con los adquiridos durante sus estudios de educación media y superior, los cuales debe saber utilizar en su desarrollo profesional y laboral para no atentar contras las leyes, los intereses de las empresas y los derechos de la personas.

6. RECOMENDACIONES

- Para contener ataques informáticos en las organizaciones, se hace necesario ejercer, aplicar e implementar todas las medidas de prevención posibles, por lo que se requiere además de contar con las herramientas de hardware y software para este tema, como base se debería contar con políticas claras y con sistemas de gestión de seguridad de la información para poder identificar y gestionar los riesgos y amenazas, todo esto para poder tener claridad sobre los controles y procedimientos a aplicar para mitigar los ataques informáticos a los que están expuestos las organizaciones.

  Las siguientes son recomendaciones que podrían aplicar en las organizaciones para prevenir y mitigar ataques informáticos:

  - Mantener actualizado los sistemas (sistemas operativos, aplicaciones, servicios).
  - Aplicación de buenas configuraciones en los sistemas, aplicaciones, sistemas operativos, a nivel de software y hardware.
  - Utilización de software legal licenciado con soporte.
  - Vigilar y controlar el tráfico de las redes a través de la implementación de soluciones como el Firewall, IDS/IPS, UTM, SIEM, etc.
  - Aplicar segmentación de las redes de acuerdo con la necesidad de la organización.
  - Aplicación de políticas y planes de copias de seguridad de toda la información y bases de datos importantes para el negocio en la organización.
  - Implementar sistemas de control de acceso tanto en las instalaciones físicas como en las instalaciones informáticas (ordenadores, sistemas de comunicación, redes).
  - Utilización de contraseñas seguras.
  - Proteger los equipos endpoint con software especializado con funciones de firewall, antivirus EPP-EDR, antimalware, antirasonware, antispam, entre otros.
  - Sensibilización y capacitación de los usuarios en cuanto al uso responsable y aplicación de buenas prácticas de las tecnologías de la información.
  - Capacitación constante a los responsables de los sistemas y seguridad de los activos informáticos.
  - Contar con planes de contingencia.
  - Adquisición de pólizas para la protección de la infraestructura informática.

- En las actividades realizadas por los Equipos Red Team & Blue Team, cabe la pertinencia del trabajo conjunto con entidades como en CIS (Center of Internet Securtiy), ya que puede reforzar los procesos aplicados de sus actividades dentro de las organizaciones, con la utilización de sus herramientas, el soporte de su comunidad y la aplicación de los CIS Controls, que vendría a reforzar los procesos

del Blue Team, ya que los CIS Control son considerados como un conjunto de mejores prácticas para mitigar los ataques más comunes contra los sistemas y redes.

BIBLIOGRAFÍA

ALCALDIA BOGOTÁ. 2012. Ley 1581 de 2012 Nivel Nacional. [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

ALLEN, Mateus. 2017. Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. [En línea]. [Consulta: 20 de 09 de 2020]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf.

ASTUDILLO, Karina. 2019. Aprende a usar el Metasploit Framework. [En línea]. [Consulta: 20 de 09 de 2020]. Disponible en: https://academia-hacker.com/metasploit-framework/.

BERREIRO SANCHEZ, Pablo. 2010. CÓMO ESTRUCTURAR UNINFORME TÉCNICO COMO UN VERDADERO INGENIERO. *Universidad de Cantabria.* [En línea]. [Consulta el: 10 de 10 de 2020]. Disponible en: https://ocw.unican.es/pluginfile.php/1408/course/section/1805/tema10-comoEstructurarUnInformeTecnico.pdf.

CIS. Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution. [En línea]. [Consulta: 20 de 09 de 2020]. Disponible en: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/.

COPNIA. Código de Ética para el servicio de la Ingeniería en general y sus profesiones a fines y auxliares. [En línea]. [Consulta: 8 de septiembre de 2020]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

CVE. CVE-2017-0144. [En línea]. [Consulta: 20 de 09 de 2020]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144.

DAPRE. 2018. LEY 1928. [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf.

ESCRIVA GASCO, Gema, ROMERO SERRANO, Rosa y RAMANDA, David. 2013. Seguridad Informática. s.l. : Madrid , ES: Macmillan Iberia, S.A., 2013. pág. 173.

FERNANDEZ MIRANDA, Henry. 2019. ANÁLISISDELA SEGURIDAD DEL SITIO WEB DEL MINISTERIO DEL TRABAJO APLICANDO PRUEBAS DE PENTESTING EN LA SEDE PRINCIPAL DELA CIUDAD DE BOGOTÁ. *Repositorio UNAD.* [En línea]. [Consulta: 20 de 09 de 2020]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/27059/hafernandezm.pdf?sequence=1&isAllowed=y.

GAVIRIA, Raúl. 2015. Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. [En línea]. [Conssulta: 20 de 09 de 2020]. Disponible en: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1.

IBILI, Raul. 2019. Vulnerabilidades: OpenVas. *Security Labs.* [En línea]. [Conssulta: 21 de 09 de 2020]. Disponible en: https://securitylabs.es/elementor-1138-2-2-2-3-2-2-2/.

IPAUDITA. Top 30 de Nmap ejemplos de comandos para SYS / Red Admins. [En línea]. [Consulta: 31 de agosto de 2020.] https://ipaudita.wordpress.com/2013/02/13/top-30-de-nmap-ejemplos-de-comandos-para-sys-red-admins/.

MEJIA, Robin. 2008. Red Team Versus Blue Team: How to Run anEffective Simulation. *CSO.* [En línea]. [Consulta: 5 de 10 de 2020]. Disponible en: http://aldeilis.net/mumbai/0682.pdf.

MINTIC. 2020. Adhesión al Convenio de Budapest contra la ciberdelincuencia, clave para Colombia en tiempos de Coronavirus. [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126496:Adhesion-al-Convenio-de-Budapest-contra-la-ciberdelincuencia-clave-para-Colombia-en-tiempos-de-Coronavirus.

MINCIT. 2013. DECRETO 1377 DE 2013. [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf.

CONGRESO DE LA REPUBLICA. 2009. LEY 1273. [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

OPENVAS. OpenVAS - Open Vulnerability Assessment Scanner. [En línea]. [Consulta: 30 de agosto de 2020]. Disponible en: https://www.openvas.org/.

RAMIREZ RESTREPO, Jorge y AVILA PARDO, Williams. 2018. ESCANEO DE VULNERABILIDADES AL SERVIDOR PRINCIPAL DE LA EMPRESA CASO DE ESTUDIO. [En línea]. [Consulta: 20 de 09 de 2020]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/18321/1121877957.pdf?sequence=1&isAllowed=y.

REVISTA SEGURIDAD. 2018. Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. [En línea]. [Consulta: 20 de 09 de 2020]. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra.

SANZ MERCADO, Pablo. 2008. Seguridad en linux: guía práctica. Madrid : Universidad Autonoma de Madrid, 2008. págs. 86-88.

The Bluebox. ¿Que es un Blue Team? The BlueBox – Ethical Hacker Community. [En línea]. [Consulta: 3 de 10 de 2020]. Disponible en: https://thebluebox.wordpress.com/que-es-un-blue-team/.