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

DANIEL FELIPE VIERA QUEBRADA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CALI

2022

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

DANIEL FELIPE VIERA QUEBRADA

DIRECTOR DEL CURSO

JHON FREDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CALI

2022

CONTENIDO

pág.

Contenido

1 GLOSARIO 5

2 INTRODUCCIÓN 8

3 DEFINICIÓN DEL PROBLEMA 9

4 JUSTIFICACIÓN 10

5 OBJETIVOS 11

5.1 OBJETIVO GENERAL 11

5.2 OBJETIVOS ESPECÍFICOS 11

6 MARCO TEÓRICO 13

6.1 MARCO LEGAL EN COLOMBIA ASOCIADO A LOS DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES 13

6.2 PRUEBAS DE PENETRACIÓN (PENTESTIN) DEFINICÓN DE ETAPAS Y HERRAMIENTAS 16

2- Fase de recolección de información 18

Herramientas: 18

3- Fase de modelado de amenaza 18

Herramientas: 18

4- Fase de Analisis de vulnerabilidades 18

Herramientas: 19

5- Fase de Explotación 19

6.3 DEFINICIÓN Y EXPLICACÓN DE ALGUNAS HERRAMIENTAS DE CIBERSEGURIDAD ... 20

6.4 IMPLEMENTACIÓN DEL BANCO DE TRABAJO 29

7 ANALISIS DE LOS ANEXOS ESCENARIO 2 Y ACUERDO DESDE EL PUNTO DE VISTA LEGAL Y NO ÉTICO 35

8 ANALISIS DE LOS ANEXOS, CON RELACION A LA VULNERACION DE LA LEY 1273 ARGUMENTANDO CUALQUIER PROCESO ILEGAL 39

9 ANALISIS DE LA PROPUESTA LABORAL, TENIENDO PRESENTE EN CUENTA LA REVISIÓN DESDE EL PUNTO DE VISTA LEGAL Y ÉTICO 40

10 ANALISIS DEL CASO "OPERACIÓN ADROMEDA BUGGLY" DESDE SU POSICÓN TENIENDO EN CUENTA LOS ASPESTOS LEGALES Y ÉTICOS 43

11 HERRAMIENTAS Y PROCEDIMIENTOS ESTABLECIDOS PARA DAR SOLUCIÓN AL ANEXO 4 ESCENARIO 3..... 45

12 DATOS E INFORMACIÓN DEL ANEXO 4 -ESCENARIO 3..... 49

12.1 ANÁLISIS DE LA VULNERABILIDAD. 53

12.2 Caracterización de los procesos anteriormente mecionados:.....59

12.3 EXPLOTACION DE REJETTO CON METAEXPLOIT 60

12.4 CREANDO USUARIO APROVECHANDO LA VULNERABILIDAD.....67

12.5 EXPLICACIÓN DE LA AFECTACIÓN DEL ATAQUE A LA MAQUINA WINDOWS 7 X64 .70

12.6 ACCIONES PARA TOMAR FRENTE A UN CASO DE ATAQUE INFORMÁTICO EN TIEMPO REAL 71

13 Hardenización para minimizar o mitigar ataques de seguridad informática .. 78

14 DIFERENCIA ENTRE UN BLUE TEAM Y EQUIPO DE RESPUESTA A INCIDENTES . 85

15 ANÁLISIS DE TRABAJAR CON CIS "CENTER FOR INTERNET SECURITY" PARA ROPUESTA DEL BLUE TEAM 86

16 FUNCIONES Y CARACTERISTICAS DE UN SIEM..... 87

17 .HERRAMIENTAS PARA LA CONTEÓN DE ATAQUES INFORMÁTICOS..... 88

18 RECOMENDACIONES 94

CONCLUSIONES 95

BIBLIOGRAFÍA 96

1 GLOSARIO

Vulnerabilidad: Es un punto débil que tiene un sistema a nivel de software o hardware computacional que permite que sea vulnerado y no cuenta con las configuraciones necesarias para evitar ser vulnerado.

Seguridad: Son el conjunto de herramientas, procedimientos y estrategias que tienen como propósito garantizar la integridad, disponibilidad y confidencialidad de un sistema informático.

Red Team: Es el equipo rojo el cual está conformado por profesionales especializados o en su defecto hacker éticos con altos conocimientos técnicos en seguridad informática que emulan ataques informáticos que intentan superar y penetrar los controles de seguridad implementados en las organizaciones y ellos evalúan la seguridad del sistema de manera objetiva.

Blue Team: Es el equipo azul y esta está formado Es el equipo rojo el cual está conformado por profesionales especializados o en su defecto hacker éticos con altos conocimientos técnicos en seguridad informática por profesionales de la seguridad que tienen un amplio conocimiento de la empresa de adentro hacia fuera, su tarea es monitorear, analizar malware, ransomware y cazar amenazas, otra labor importante es proteger los activos de la organización de cualquier amenaza interna o externa que intente penetrar los sistemas de protección.

Ataques: es la forma en la que un hacker intenta explotar una vulnerabilidad o indisponer un servicio al intentar exponer, alterar, desestabilizar, destruir información y obtener acceso no autorizado a un activo.

Malware: programa mal intencionado que fue creado para infiltrarse en sistemas o dispositivos sin su consentimiento.

Routers: Es un dispositivo de la capa de red que conecta redes con ordenadores.

Amenaza: Es la posibilidad potencial de que un incidente de seguridad suceda con el potencial necesario para generar un daño informático.

Confidencialidad: Es el pilar de la seguridad informática que se enfoca en garantizar que la información sea accesible únicamente por el personal autorizado para los propósitos establecidos.

Disponibilidad: Es uno de los pilares que busca garantizar la disponibilidad de la información y al momento de acezarla esté disponible sin interrupciones.

Integridad: Garantiza que la información gestionada no sea modificada, alterada por una persona no autorizada que afecte el flujo de los procesos de la seguridad de la información.

Riesgo: Materialización de una amenaza informática que haya aprovechado una vulnerabilidad.

IoC: por sus siglas en inglés es un dato que permite identificar comportamientos maliciosos en direcciones IP, dominios, urls, hash que tienen unas características o descripción de una amenaza lo cual permite confirmar con certeza que nuestro equipo fue comprometido con un virus, ransomware, malware, pero también es información que puede ser utilizada para prevenir futuros ataques

Auditoria caja negra: Por lo general la realiza una empresa o persona externa a la empresa o un equipo de red team que no conoce nada de la empresa y su infraestructura. Una de las fases que se utiliza es Footprinting, el cual le permite al equipo de red team o pentestert recopilar información externa y en comparación con el Fingerprinting es otra fase donde recopila y enumeran los datos de la empresa.

Auditoria caja blanca: En esta auditoria el equipo de red team o pentetert conoce la infraestructura por dentro con el fin de tener ganar acceso a toda la información y saltándose los controles de seguridad. Esta etapa del ataque se llama Fingerprinting y permite recopilar información de la organización rápidamente y permite aplicar planes de remediación.

Auditoria caja gris: Esta prueba combina fases de ambas pruebas tanto de caja negra como de caja blanca lo que permite a un equipo de red team, hacer fases de reconocimiento previas con información básica de la empresa y desde ese punto comenzar a escalar privilegios en la red desde diferentes puntos, redes inalámbricas, red Lan y desde internet.

Ransomware: Este malware utiliza como vector de ataque el correo electrónico por el cual las victimas descaran el malware que permite la explotación de la vulnerabilidad SMB V1 CVE-2017-0144 que se encuentra en sistemas operativos Microsoft en todos sus sistemas operativos uno de los ataques más conocidos a nivel mundial fueron wannacry o ethernalblue" y una de sus características es que solicita dinero para rescatar la información robada a sus víctimas.

APT: Amenaza Avanzada Persistente, los grupos de APTs son muy comunes en la actualidad realizan ataques coordinados que duran meses lo que les permite explotar los sistemas sin ser detectados por lo general dejan una puerta trasera que les permite comunicarse con el C2 (Comando y control) que es donde el grupo almacenar la información recopilada para ser vendida o en su defecto desplegar un ransomware para pedir rescate.

2 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.

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.

3 DEFINICIÓN 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.

¿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?

4 JUSTIFICACIÓN

Hoy en día es de suma importancia tener equipos de seguridad que generen sinergia al interior de las empresas y tener claros los roles que deben apoyar estas gestiones a nivel táctico y estratégico que estén en pro de la misión de la empresa y tener procedimientos claros frente a in ciberataque, tener procedimientos de incidentes, procedimiento de crisis y plan de continuidad que permita brindar la operación de la empresa bajo un incidente de ciberseguridad y poder tener claro el mapa de ruta que deben seguir para garantizar la continuidad de negocio el talento humano.

5 OBJETIVOS

5.1 OBJETIVO GENERAL

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

5.2 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 y 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.

- Indicar las medidas de hardenización que se implementarían a un sistema vulnerable como el presentado en el anexo 5 - escenario 4.
- Identificar las diferencias entre un equipo BlueTeam y un equipo de respuesta a incidentes informáticos.
- Identificar el objetivo de CIS "Center For Internet Security" al interior de Blue team.
- Explicar y redactar las características y funciones principales de un SIEM.
- Definir tres herramientas de contención de ataques informáticos

6 MARCO TEÓRICO

6.1 MARCO LEGAL EN COLOMBIA ASOCIADO A LOS DELITOS INFORMÁTICOS 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.

LEY 1273 DE 2009

A través de la ley 1273 de 2009 el congreso de la Colombia modificó el Código Penal y tipifico 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.).

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

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

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

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

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

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

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

Artículo 269I: Hurto por medios informáticos y semejantes (penas señaladas en el artículo 240 del código penal entre 3 y 8 años)

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

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.

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 reglamento esta ley, el gobierno nacional dicto 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 u' bien jurídico tutelado.

La ley 1581 de 2012 Habeas Data, es de mucha importancia, porque desarrolla el derecho constitucional que tiene toda la ciudadanía colombiana para conocer, suprimir, actualizar y rectificar todo tipo de datos personales que estén recolectados, almacenados o que hayan surtido algún tratamiento en bases de datos en entidades públicas y privadas en el territorio colombiano. 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.

6.2 PRUEBAS DE PENETRACIÓN (PENTESTIN) DEFINICÓN 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 información puestos a prueba para identificar y posteriormente corregir posibles vulnerabilidades y los peligros asociados a las mismas. Esta auditoria representa para el cliente una importante fuente de información ya que el pentester actuara 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 variara 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 cual 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 cual 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 critica 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 permitiran 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 (analisis 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, Cuales 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 seria 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 (analisis de metadatos)

4- Fase de Analisis de vulnerabilidades

Llegados a este punto se debe valorar el posible éxito de fas estrategias de penetración a través de la identificación proactiva de vulnerabilidades. En este momento es cuando la habilidad del pentester se pone de manifestó 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 Negado el momento de intentar conseguir acceso a los sistemas objetivo de nuestro test de penetración, para él lo 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 maquina 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 auditoria 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 per una parte el informe ejecutivo y el informe técnico.

6.3 DEFINICIÓN Y EXPLICACÓN DE ALGUNAS HERRAMIENTAS DE CIBERSEGURIDAD

Las herramientas de analisis 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 analisis de vulnerabilidades que pueden ser aplicadas durante el desarrollo de seminario especializado: Equipos Estratégicos en Ciberseguridad: Red Team & 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 información 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

Estaciones de trabajo, servicios y sistemas operativos con las vulnerabilidades encontradas por las herramientas.

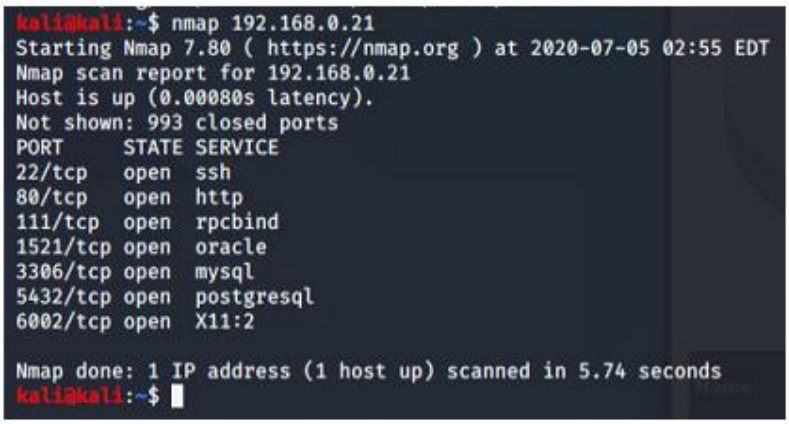
Nmap viene por defecto en Kali Linux, para verificar si está instalada y en que versión se puede utilizar el comando nmap --versión

Figura 1. Nmap

Fuente: Autor

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

Figura 2. Escaneo con Nmap



Fuente: Autor

La salida del comando permite identificar los puertos por los cuales se ha configurado los servicios de base de datos, esta información es un insumo que puede ser utilizada por un atacante generando un SLQ Inyección o DDos (Ataque de denegación de servicio).

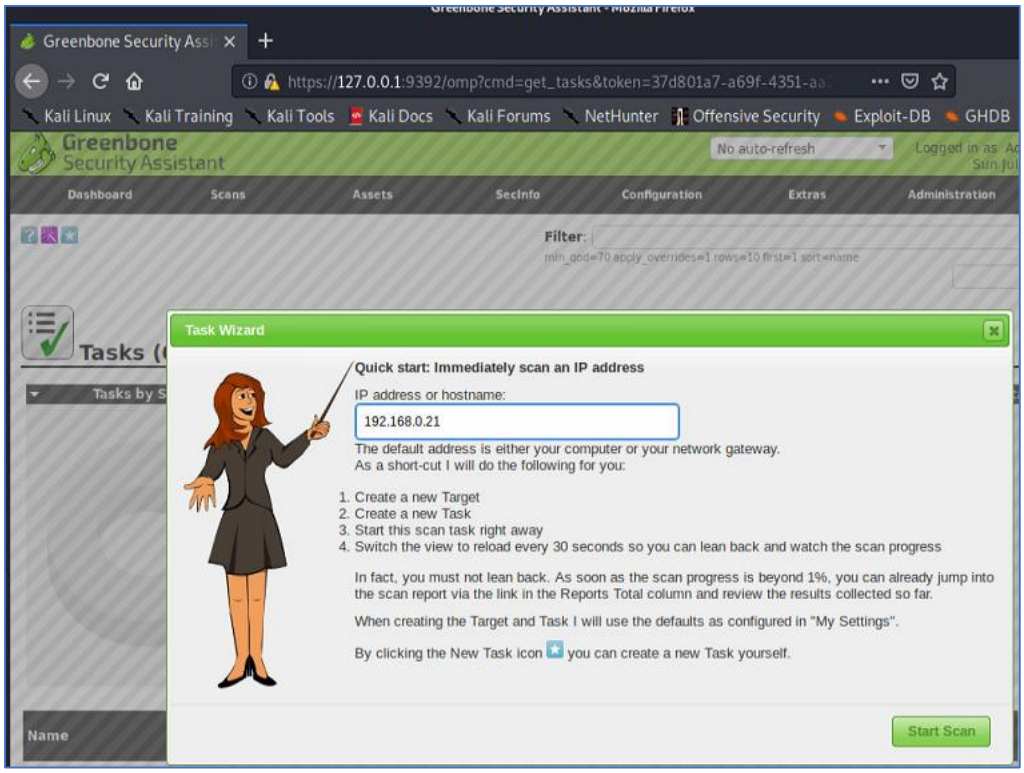
- **OpenVas**

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:

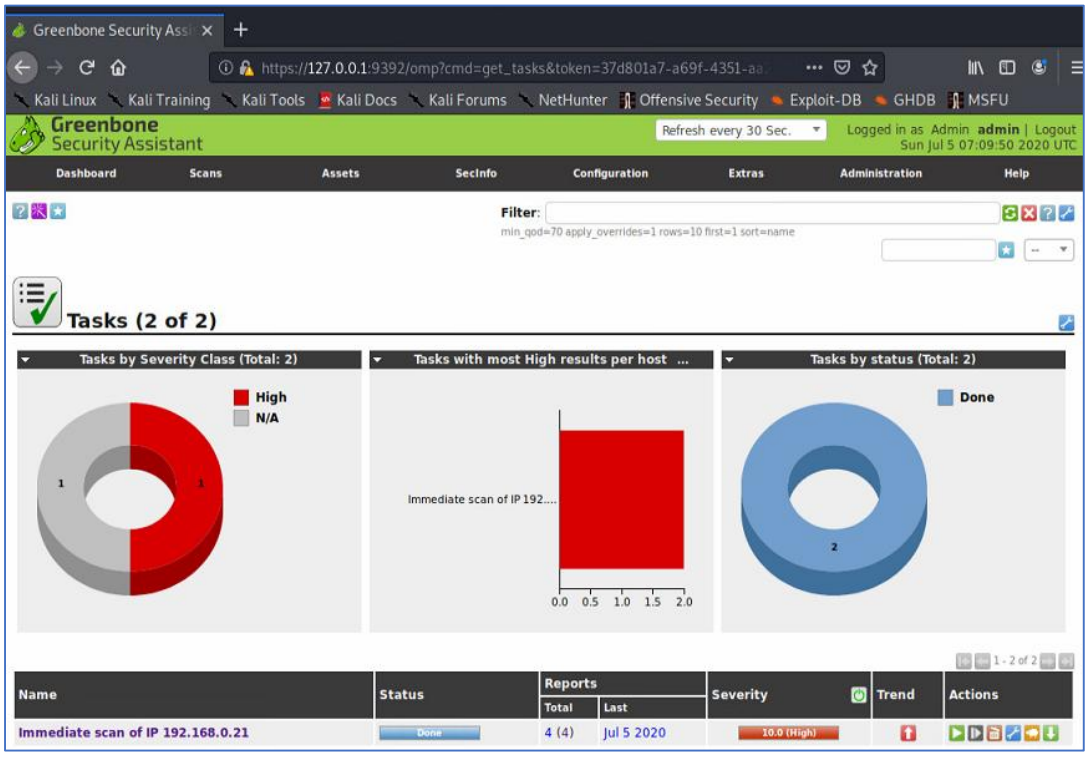
Figura 3. Escaneo con Openvas



Fuente: Autor

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

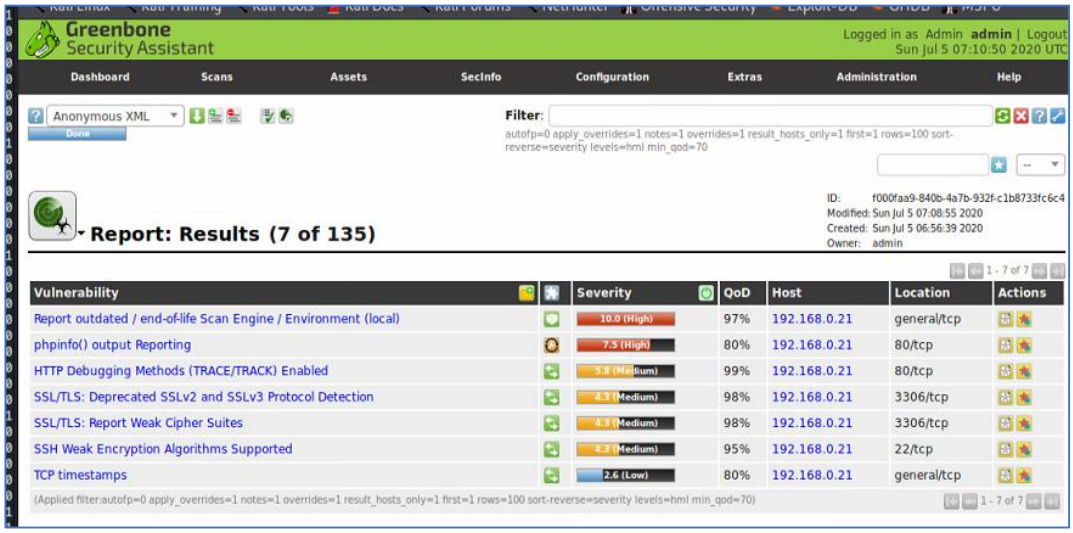
Figura 4. Resultados del escaneo



Fuente: Autor

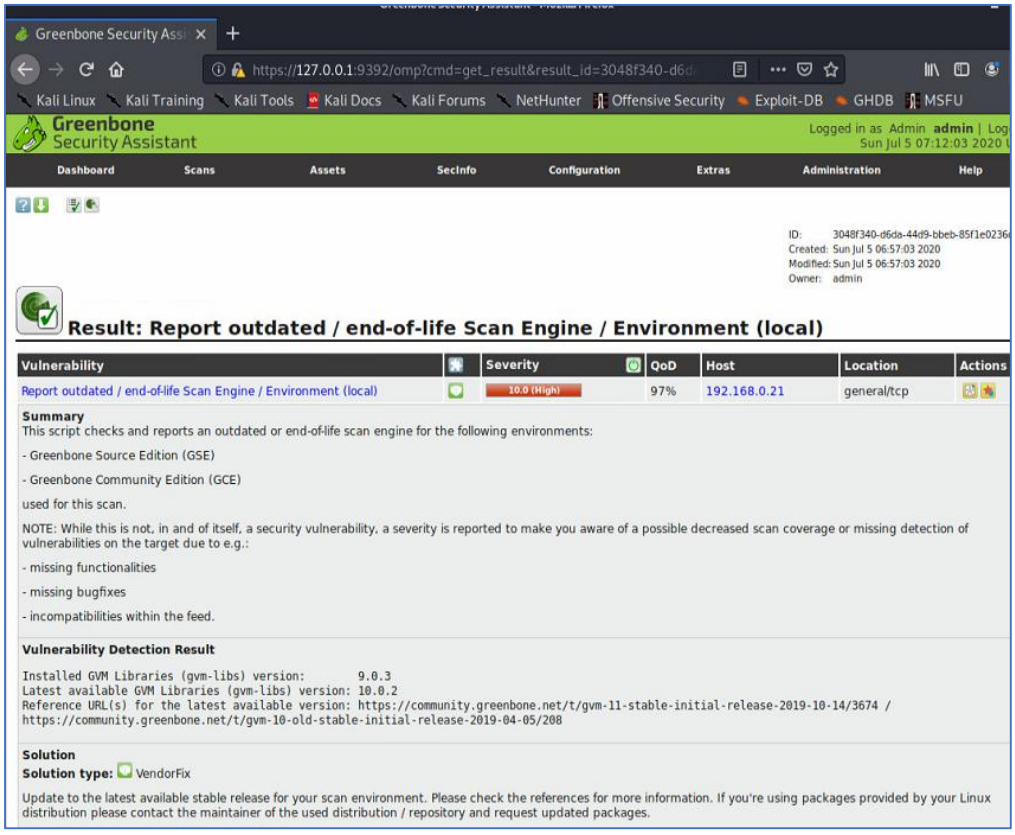
Se da clic en Done para ingresar al reporte, luego se le secciona una de las vulnerabilidades detectadas para analizarla, así se continua con cada una de las vulnerabilidades.

Figura 5. Resultados del escaneo



Fuente: Autor

Figura 6. Vulnerabilidad encontrada



Fuente: Autor

El reporte entregado por la herramienta brinda una solución para corregir la vulnerabilidad detectada.

Servicios en línea:

- **ExploitDB**

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

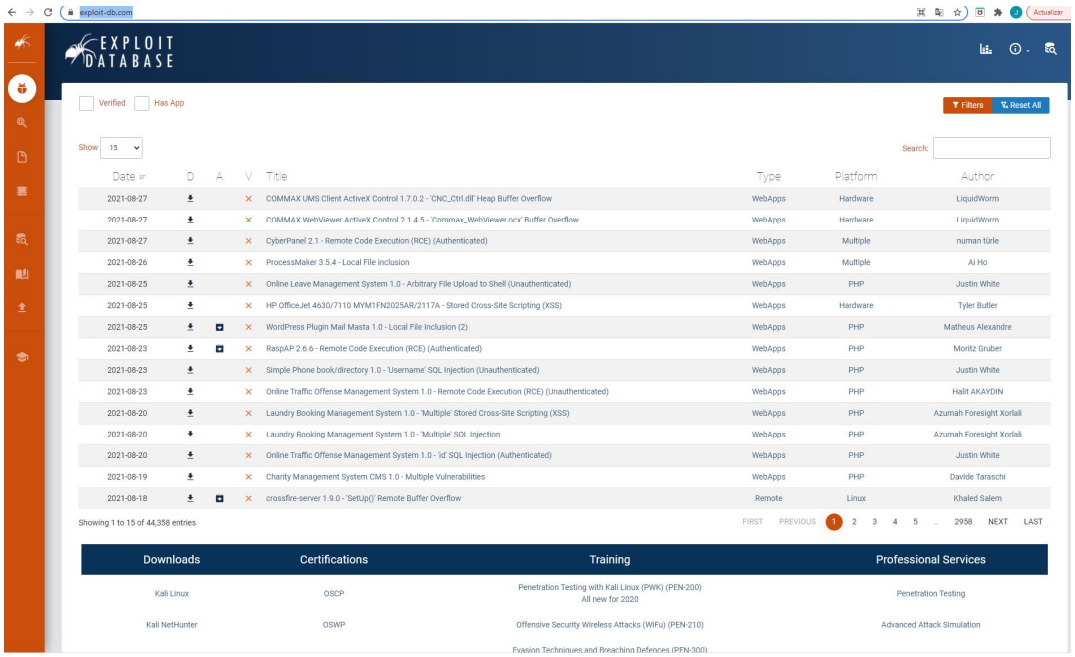
Cada día aparecen nuevas y es un lugar donde se puede aprender mucho, pero también se puede hacer daño a terceros si hacemos un mal uso de sus instrucciones y lo hacemos con fines malévolos.

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.

[1] https://www.exploit-db.com/,

Figura 7. Herramienta Exploit Database



Fuente: https://www.exploit-db.com/,

- **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 Récords para asegurarse de que están discutiendo el mismo problema y para coordinar sus esfuerzos para priorizar y abordar las vulnerabilidades.

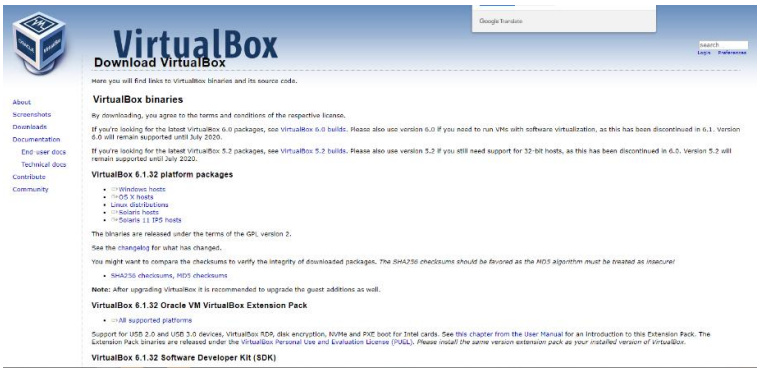
6.4 IMPLEMENTACIÓN DEL BANCO DE TRABAJO

A continuación, se analiza y configura el "banco de trabajo" de acuerdo con 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 :

Figura 8. Virtual box

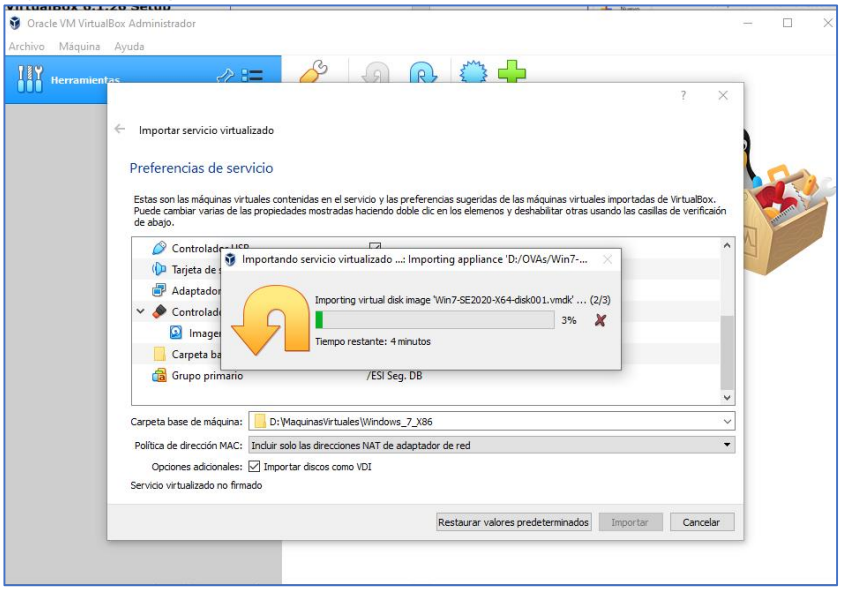


Fuente: https://www.virtualbox.org/

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.

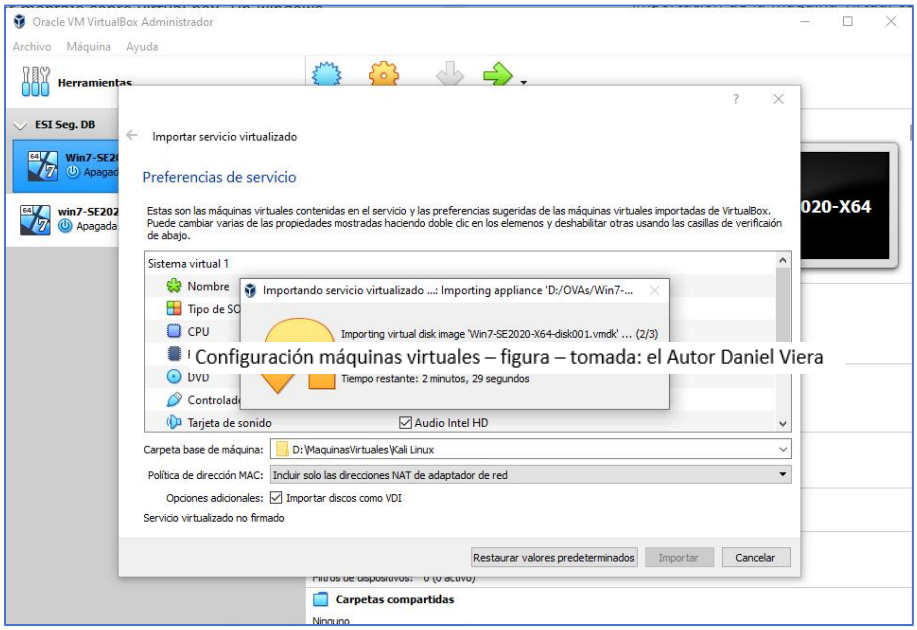
Figura 9. Máquina virtual windows7



Fuente: Autor

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

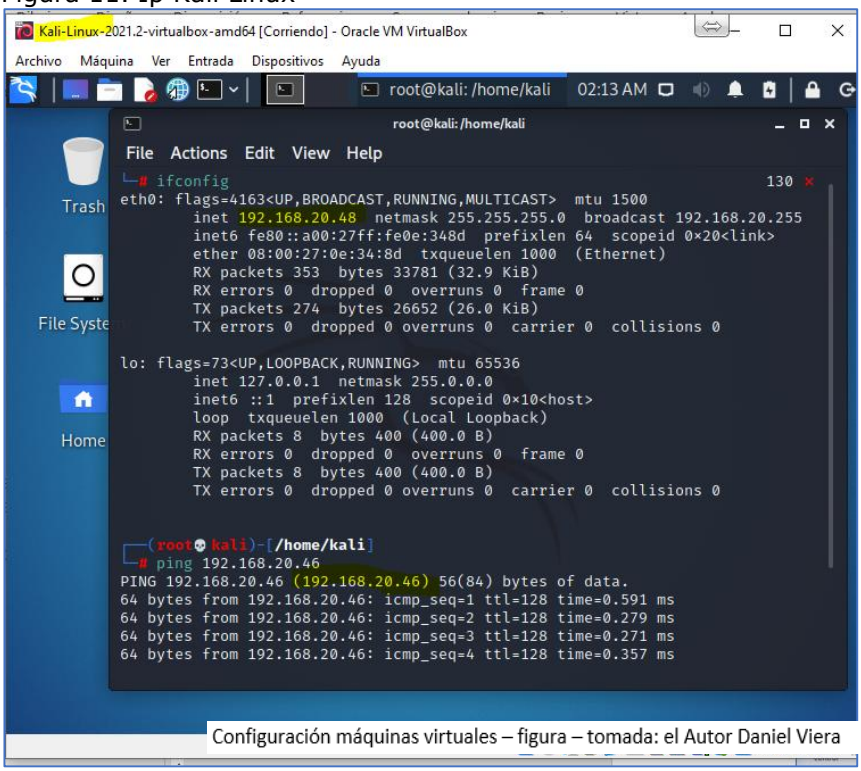
Figura 10. Máquina virtual Kali Linux



Fuente: Autor

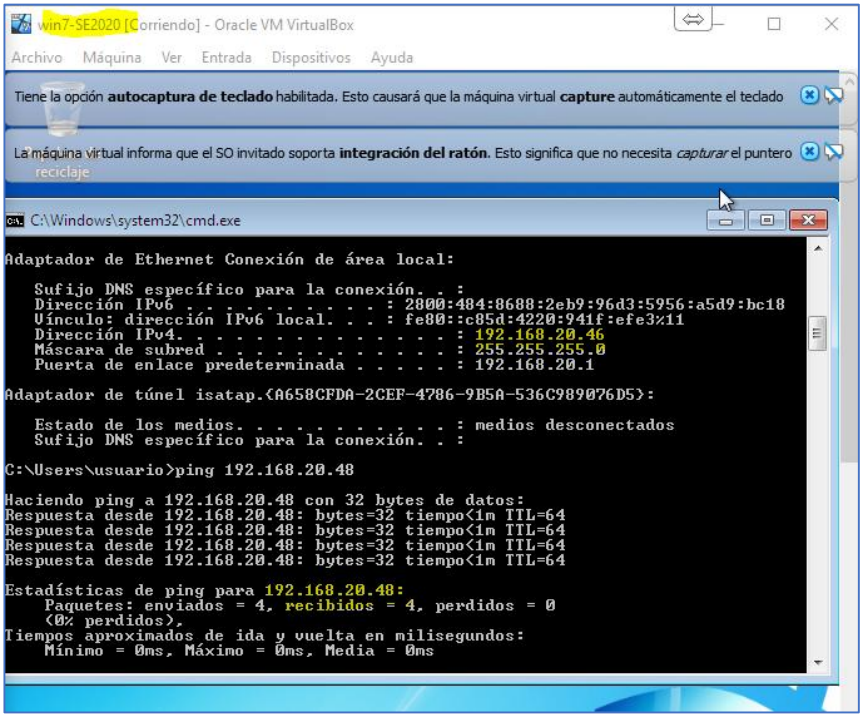
Se verifica comunicación entre la maquina Windows 7 X86 y Kali Linux para lo cual se identifica la IP de cada una y con la función ping sobre un terminal de comandos se alcanza la IP contraria.

Figura 11. Ip Kali Linux



Fuente: Autor

Figura 11. Ip Windows y ping a Kali linux



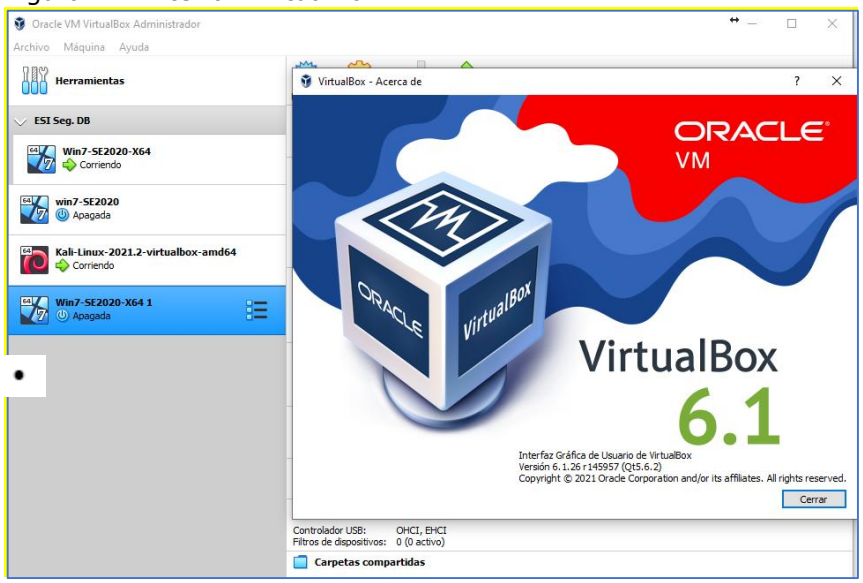
Fuente: Autor

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.

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

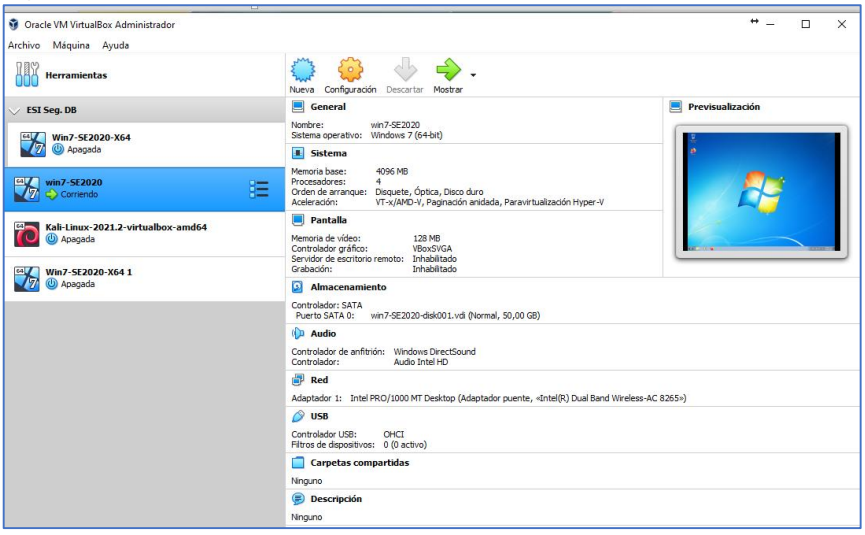
Figura 12. Interfaz VirtualBox



Fuente: Autor

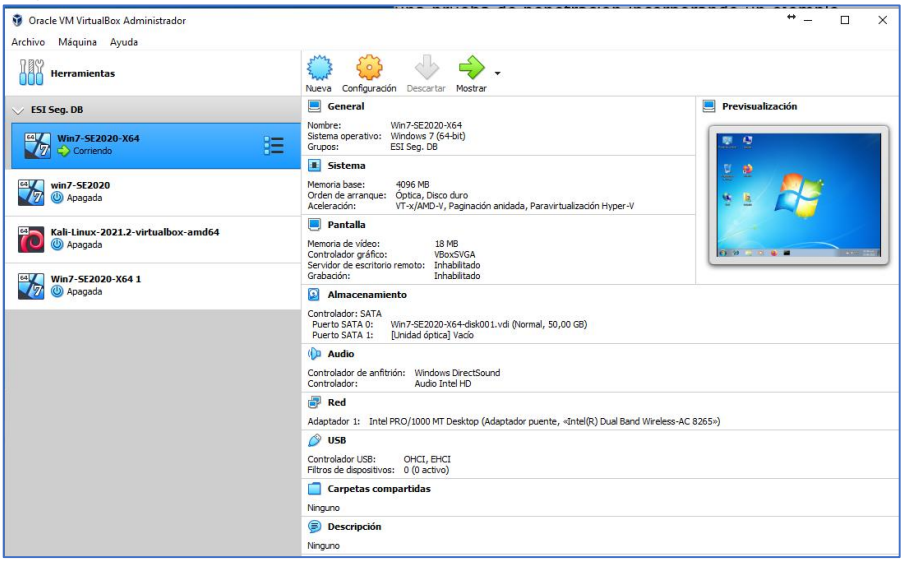
- Características técnicas de hardware para Windows 7 X86

Figura 13. Características Windows x86



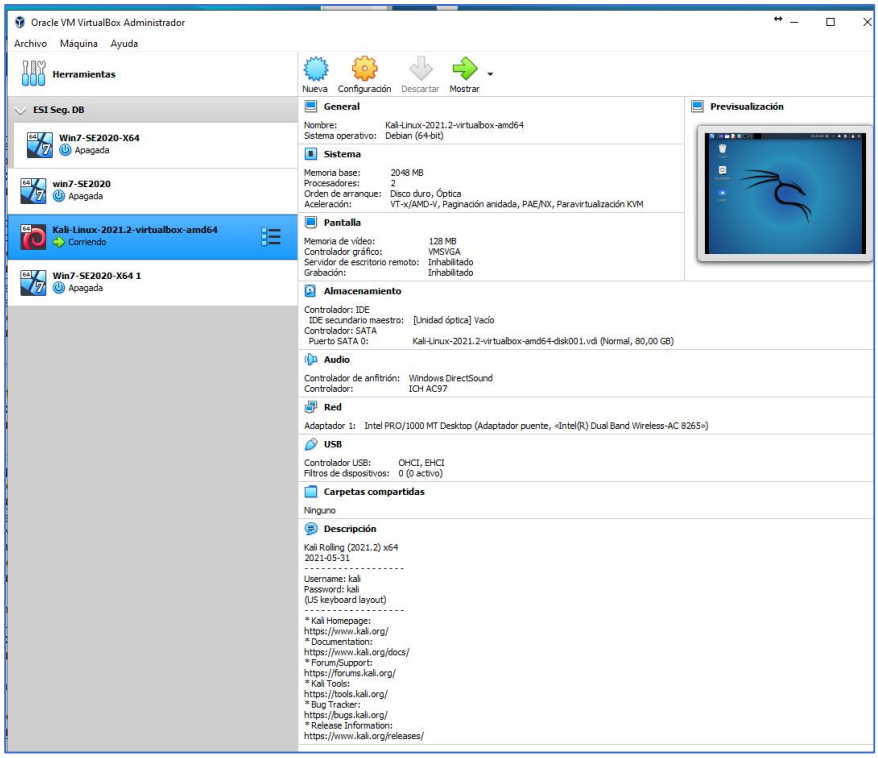
Fuente: Autor

Figura 14. Características Windows x86



Fuente: Autor

Figura 15. Características Kali Linux



Fuente: Autor

Con esto damos por concluido la etapa 1 del seminario donde se detalla el marco legal colombiano frente a los delitos informáticos y protección de datos personales y se deja listo el banco de trabajo para seguir con la etapa 2.

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

A continuación, se realiza el análisis de los anexos descritos en la etapa 2 del seminario de especialización de equipos Red Team y Blue Team de acuerdo lo que plante plantea establecer un contrato con la empresa White House Security un candidato que sería un posible alumno que haría parte de los equipos de seguridad Red Team & Blue Team, donde evidenciara las debilidades que presenta la empresa y que podrían llevar a hechos ilícitos.
De esta forma se van a enumerar las cláusulas de acuerdo con las leyes colombianas que están considerando que están incumpliendo con la normativa de las leyes y el código de ética aplicable para los ingenieros especialista en seguridad informática.

- "**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**: La información es de origen confidencial: La información vendrá de documentos clasificados por la empresa del área de recursos humanos que es la encargada de seleccionar al personal que ingresa a la empresa y aporta con la creación de intelecto para formar a los colaboradores en la venta de productos, comercialización de productos, la forma de distribuir la mercancía que debe ser de una forma visual, verbal o escrita plasmada en los documentos bien sea electrónicos, correo, discos ópticos, películas, cortometrajes USB u otros similares que se presenten de forma tangible o intangible, sin

importar la fuente o soporte de la información, sin que se requiera informar a la parte contratada se le informa que debe tener la mayor discreción debido que es suma confidencialidad."

- **Cuarta**: Deber del contratante 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 del contrato: de acuerdo con el presente contrato estipulado por la empresa y su contratante se informa a la parte el acuerdo de confidencialidad de la parte receptora se le informa de una forma clara y concisa de no divulgar directa o indirectamente la información compartida por ningún medio físico o digital u otra persona, compañero, contratista subalterno o tras personas ajenas a la empresa incluyendo autoridades legales, asesores, entidad relacionada con la información. Sobre los procesos que se llevan a cabo dentro de la empresa entro de Whitehouse Security no podrán ser divulgados." Se debe tener presente que en la primera clausula mocionada en el documento, aparece la palabra "procesos legales" me genera la inquietud que, en la cláusula mencionada, aparece el término "procesos ilegales", lo que se puede llegar a concluir que si se realizan procesos pocos convencionales que estén fuera de la normativa legal para realizar el trabajo solicitado.

En la cláusula tercera, La procedencia de la información es confidencial: La información vendrá de documentos clasificados por la empresa del área de recursos humanos que es la encargada de seleccionar al personal que ingresa a la empresa y contratación de personal aporta valor con las nuevas contrataciones y ayuda a formar a los colaboradores en la venta de productos, comercialización de productos, la forma de distribuir la mercancía que debe ser de una forma visual, verbal o escrita descrita en documentos correo electrónico, discos duros y discos ópticos, películas, cortometrajes USB u otros similares que se presenten de forma tangible o intangible, sin importar la fuente o soporte de la información sin que se requiere informar que es de suma confidencialidad."

Al parecer es una cláusula clara que indica de donde proviene la información, pero esta cláusula no hace menciona la forma o los procesos específicos que se realizan para poder obtener la información y desde ese punto se pueda incurrir en las faltas que las Leyes Colombianas tipifican como delitos informáticos, se debe dar un poco más de claridad.

En la cuarta cláusula, le expone a la parte receptora de cumplir con el inciso 7, "responder por el mal uso que le den sus representantes a la información confidencial", desde mi percepción me genera inquietud, porque a la hora de firmar un contrato se debe leer detalladamente lo que está escrito y se debe asumir que se cumplirá con lo plasmado ahí y lo que implica de una forma legal; si se llegara a presentar un problema de tipo legal la responsabilidad puede ser compartida no solo del empelado y las consecuencias que se pueden originar desde una situación legal como lo que podría ser la detección y privación de la libertad que llegara a incurrir en una falta legal por incumplir lo contratado. 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 con la falta cometida.

En la cláusula cuarta, obligaciones de la parte que acepta el contrato, inciso 3, ser cómplice u omitir sucesos, eventos que estén atentando contra la confidencialidad de la información por no denunciar actividades de espionaje o cualquier otro proceso que este en contra de lo pactado en el cual sea involucrado el buen nombre de la empresa debido a que esto puedo ocasionar daños reputacionales a la marca y la fuga de información que se puede prestar para hacer sobornos o mal uso de ella en hechos delictivos como secuestros, asesinatos y extorsiones entre otros y el no denunciarlos implica que se es cómplice de estos actos ilícitos.

En la cláusula cuarta, las obligaciones de la parte contratada, inciso 9, La Debe asumir la responsabilidad de no compartir información por ningún medio digital sin consentimiento de la empresa Whitehouse Security.” En esta cláusula se habla de manera explícita que sería una falta grave y seria motivo para entrar en procesos legales.

8 ANALISIS DE LOS ANEXOS, CON RELACION A LA VULNERACION 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 del caso de estudio:

- "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".

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

Un profesional o estudiante de ingeniería informática con especialicen en seguridad informática debería declinar por esta oferta laboral, ya que tiene que tiene cláusulas muy ambiguas que no aclaran o especifican de manera clara y concisa los procesos legales cuando se lleguen a presentar generando desconfianza al momento que suceda algún incidente que estén catalogados como delitos informáticos que la ley considera infracciones contra los pilares de la seguridad de la información que son confidencialidad, la integridad y la disponibilidad de los datos de una organización y de los sistemas de información, consignados de forma explícita en la Ley 1273 de 2009. Por otra parte, cabe mencionar que la toma de esta decisión también está influenciada por los principios éticos del profesional, para el caso de estudio se subraya que en el código de ética y valores que se deben tener para ejercer la profesión de ingeniería en general y sus pares; se puede detallar las conductas profesionales que se deben tener a la hora de ejercer esta profesión, se podría llegar a supleción definitiva para ejercer o inhabilitación temporal de la tarjeta profesional. 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 y 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 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.

Brindar la mejor actitud para prestar 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 los beneficios que ofrecen en la organización de salario y contrato "vitalicio", es llamativa esta oferta laboral, pero se debe hacer un análisis muy minucioso y crítico frente a las propuestas de este tipo estudiando a fondo las cláusulas dado el caso de llegarse a presentar un incidente informático como se le dará manejo a la cláusulas que se estipulan en un contrato laboral a un profesional de seguridad informática, analizando todas las posibles situaciones que se pudieran presentar en un momento dado cuáles podrían ser las posibles consecuencias pensando en lo anteriormente mencionado, que afecten lo pactado contractualmente.

En la sociedad en la que vivimos actualmente prima mucho el tema monetario, pero a veces no se valora el recurso humano y la paz que te puede traer laborar en una empresa que no te comprometa a tal grado de poder llegar a quedar privado de la libertad, pero como profesionales con principios éticos e íntegros y trabajando de manera correcta colocando por encima los valores y principios, que aquel que se vale de mañas y

artimañas para lograr sus objetivos y puede que tenga su cuenta con dinero, pero a que costo, sin tener tranquilidad de no saber en qué momento lo puede perder todo que obtuvo de forma dudosa.

Lo más importante es ser una persona integra con valores y contar con conocimientos que aporten a la sociedad que permitan generar valor y ayuda al pro de mejorar una sociedad bajo unos principios éticos y legales que transformen la sociedad desde el trabajo como profesional que generen impacto positivo conociendo sus deberes como ciudadano y eviten que se caiga en hechos ilícitos.

10 ANALISIS DEL CASO "OPERACIÓN ADROMEDA BUGGLY" DESDE SU POSICÓN TENIENDO EN CUENTA LOS ASPESTOS 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 Buggly 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 ciber 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, rompen 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".

Con esto podemos comprender las implicaciones legales de los delitos informáticos realizados, en el caso de estudio corresponde a: al acceso abusivo a la información y a un sistema computacional, por lo cual puede ser judicializado por penas de cárcel entre 48 a 96 meses de presión

sumándole una multa entre 100 a 1000 salarios mensuales mínimos vigentes por interceptación de datos informáticos, será sancionado con una pena de entre 36 a 72 meses de presión; Uso de software malicioso malware podrá ser encarcelado con 48 a 96 meses y una multa entre 100 a 1000 salarios mínimos mensuales legales vigentes y 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 lo que implica a los valores éticos y legales que están descritos en el código de ética para el ejercicio y el área de ciberseguridad y ciberdefensa de

la Ingeniera, se puede suspender la actividad de ejercer por 5 años o en el peor de los casos retirarle la tarjeta profesional y dejar de ejercer de

forma definitiva la profesión de especialista en seguridad informática y no volver a tener contacto con un sistema de sistema informático.

11 HERRAMIENTAS Y PROCEDIMIENTOS ESTABLECIDOS PARA DAR SOLUCIÓN AL ANEXO 4 ESCENARIO 3

Herramientas:

- **Metasploit**

  Es una herramienta que se muy completa que se caracteriza por tener bastantes exploit en su base de datos para poder explotar las vulnerabilidades conocidas la cual cuenta con módulos y uno llamado payloads, que básicamente es el código que permita explotar las debilidades de los sistemas.

  También cuenta con un módulo muy potente que permite evadir la heurística de los antivirus llamada encoders, la cual cifra el código malicioso para baypasear los sistemas de seguridad a nivel de Endpoint y perimetral.

  Otra bondad de esta herramienta es su frameworks que permite la integración con otras soluciones de auditoria externar como lo son Nmap y Nessus, lo cual visualizaremos en el curso de Metasploit.

  Una de las cualidades más importantes es una herramienta OpenSource y se puede descargar desde su página principal y permite importar malware para los diferentes sistemas operativos que existen y tiene todas las vulnerabilidades publicas conocidas.

- **Nmap**

  Nmap es una herramienta Open Source multiplataforma es una de las más utilizadas por los expertos en ciberseguridad para realizar escaneos de reconocimiento y fase de escaneo de vulnerabilidades en

la actualidad por la cantidad de información que puede extraer de sus objetivos.

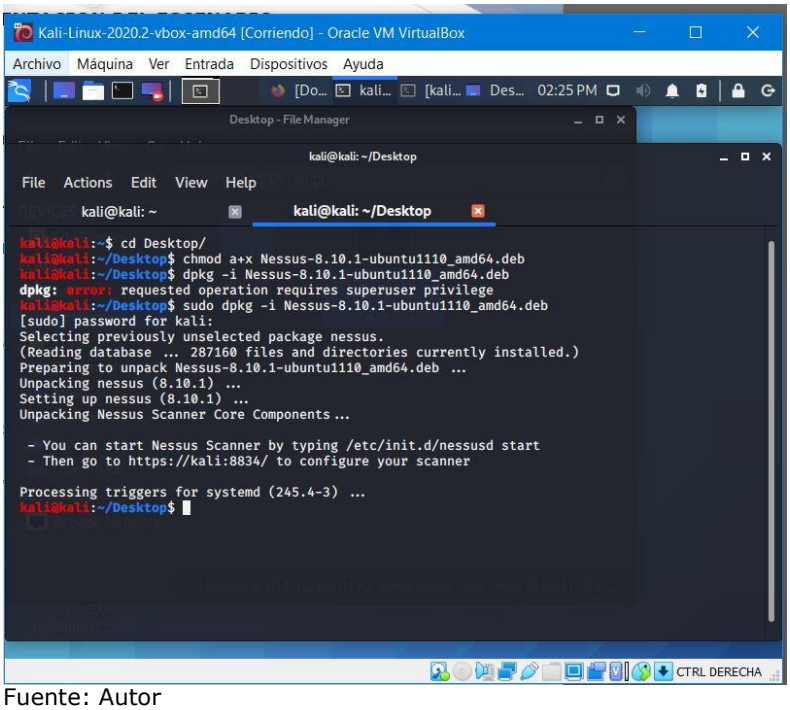
Nmap es una herramienta muy potente la cual tiene muchas opciones para realizar escaneos profundos en redes informáticas con la ayuda de scripts que identifican los equipos conectaos a la red, el sistema operativo, vulnerabilidades y servicios o puertos sensibles.
Nmap es una herramienta que sirve para realizar escaneos y se puede descargar de forma individual y también viene implícita en la solución de seguridad Kali Linux.

- **Nessus**

Nessus es una solución de seguridad muy conocida por realizar escaneo de vulnerabilidades sobre la red, la cual permite identificar vulnerabilidades en un sinfín de sistemas operativos, aplicaciones, y también permite ver los puertos abiertos en los sistemas escaneados. Se pueden obtener informes muy detallados de los escaneos realizada donde indica la criticidad de las vulnerabilidades encontradas y los exploit que se pueden utilizar para ser explotadas pero adicional también indica los planes de remediación que se le pueden aplicar a las vulnerabilidades encontrada y los parches de seguridad que se le pueden aplicar para mitigarlas. Se debe tener presente que la función "unsafe test" (pruebas no seguras) se recomienda desactivarse debido que puede generar indisponibilidad en los servicios.
Nessus permite tener dos opciones para elegir son dos versiones "Home" y "Work", una es gratuita y la otra es de paga o cual limita algunas funciones.

Para descargar la herramienta Nessus a nuestro Kali Linux debemos ingresar al repositorio principal de Nessus y procedemos a su instalación con usuario root como vemos en la imagen.

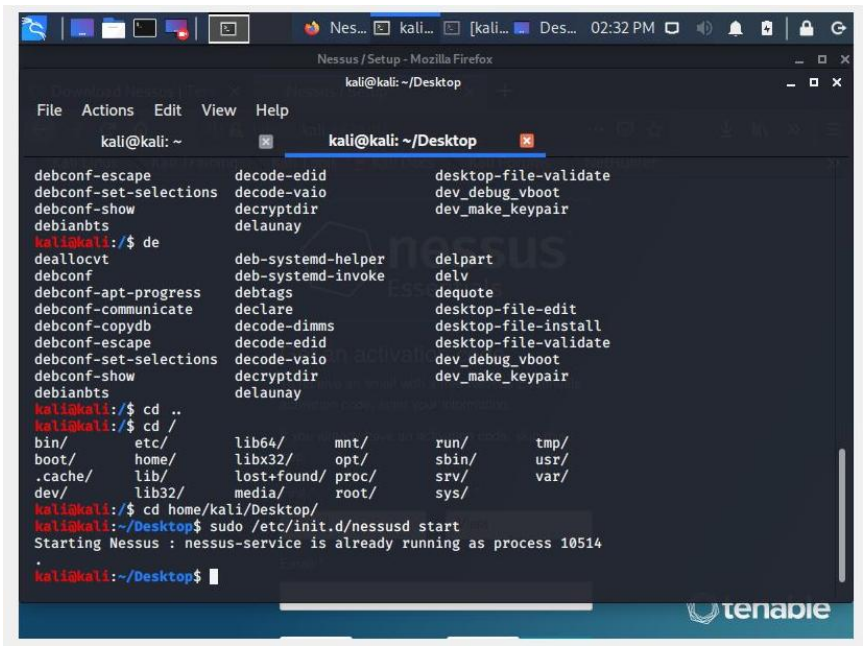
Figura 16. Instalación Nessus



Fuente: Autor

Para iniciar el servicio de Nessus debemos iniciar el servicio debemos ejecutar el siguiente comando /etc/init.d/nessusd start

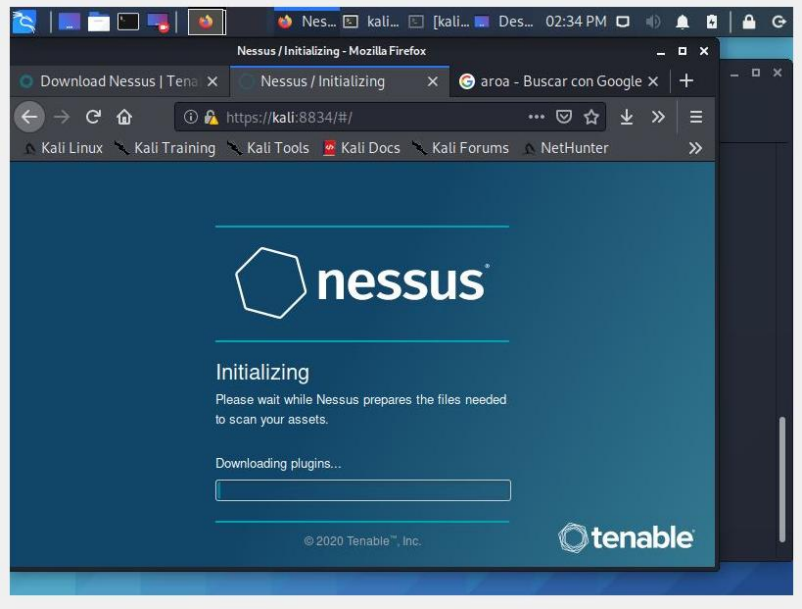
Figura 17. Iniciando Nessus



Fuente: Autor

Para ingresar al entorno web digitamos Kali:8834 en el navegador para continuar con el procese de instalación y configuración el cual nos solicitara los datos para avanzar en el proceso.

Figura 18. Interface Nessus

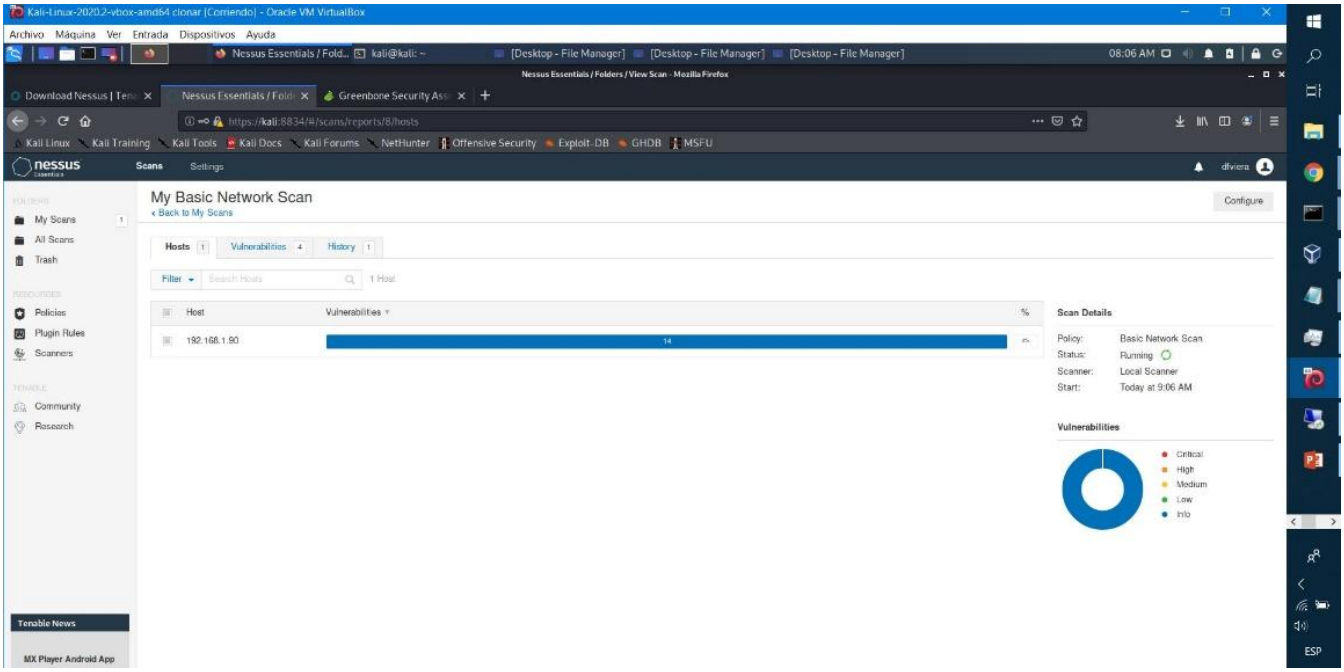


Fuente: Autor

Luego de completar el paso anterior debemos actualizarlo y puede tardar varios minutos dependiendo de la conexión del internet que se tenga.

Cuando ya este actualizado, podremos ingresar al entorno web, y podremos hacer el escaneo a las maquinas víctimas, pero primero se hace un escaneo de prueba y se puede observar que si funciona la herramienta como vemos en la imagen:

Figura 19. Escaneó básico



Fuente: Autor

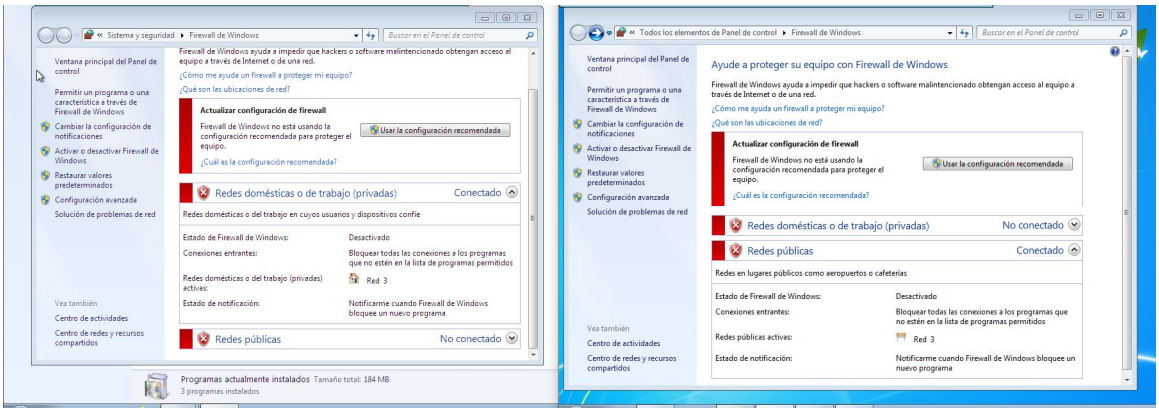
12 DATOS E INFORMACIÓN DEL ANEXO 4 -ESCENARIO 3

De acuerdo con la guía se procede a configurar el ambiente donde se realizarán las pruebas de penetración y se detallan toda la información el anexo 4 y escenario 3 que permitirán el análisis de riesgos y vulnerabilidades para identificar las fallas en los sistemas de seguridad en la maquina con sistema operativo Windows 7 version 64X.

- Es recomendable antes de iniciar con las pruebas validar que el firewall de Windows este desactivado para garantizar que los escaneos sean más efectivos y se pueda obtener toda la información de la fase de

reconocimiento este proceso se debe hacer para las dos máquinas virtuales:

Figura 20. Desactivación del firewall

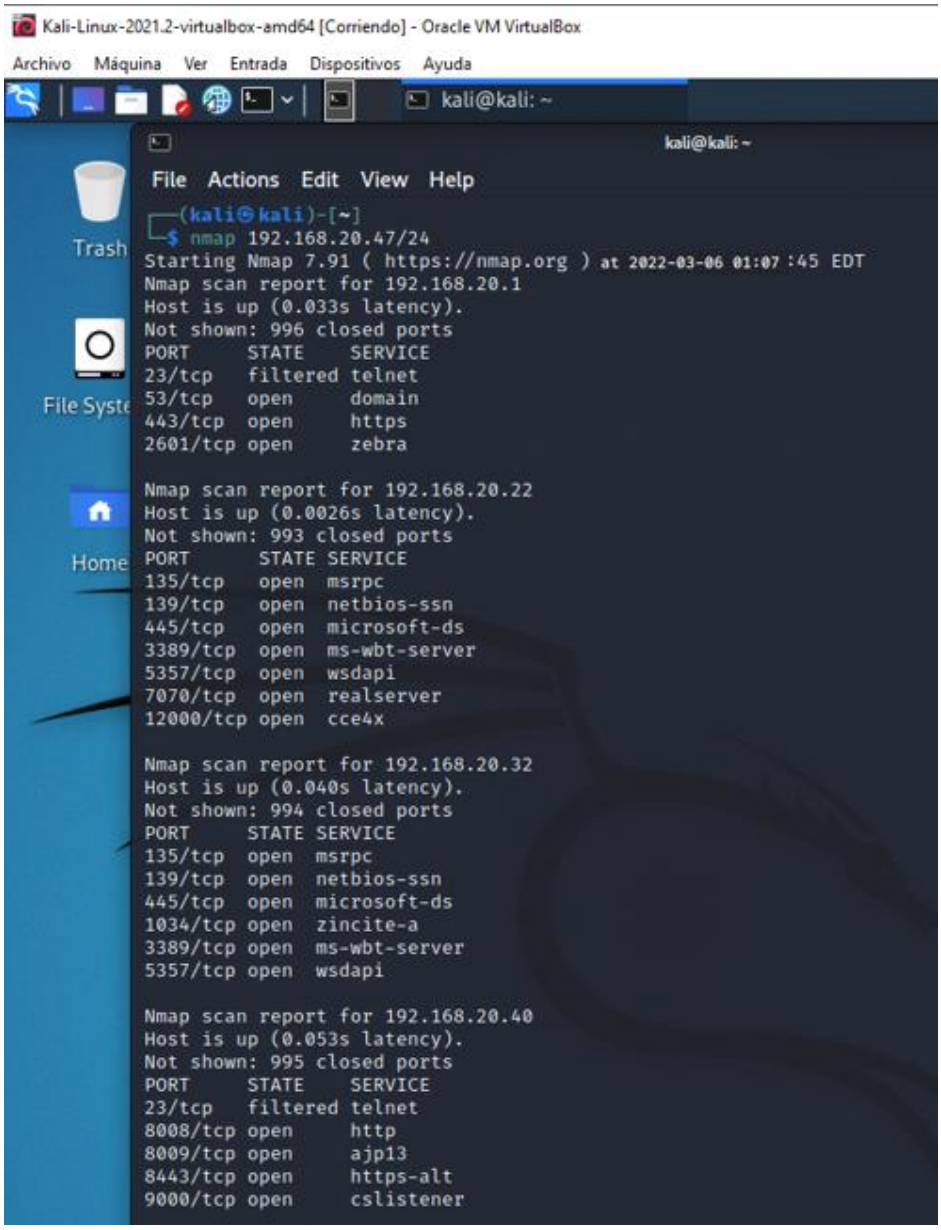


Fuente: Autor

- Se valida con el comando IP/CONFIG las direcciones IP's que tienen las máquinas virtuales y es muy importante que estén en el mismo segmento de red para que puedan verse y responder a PING

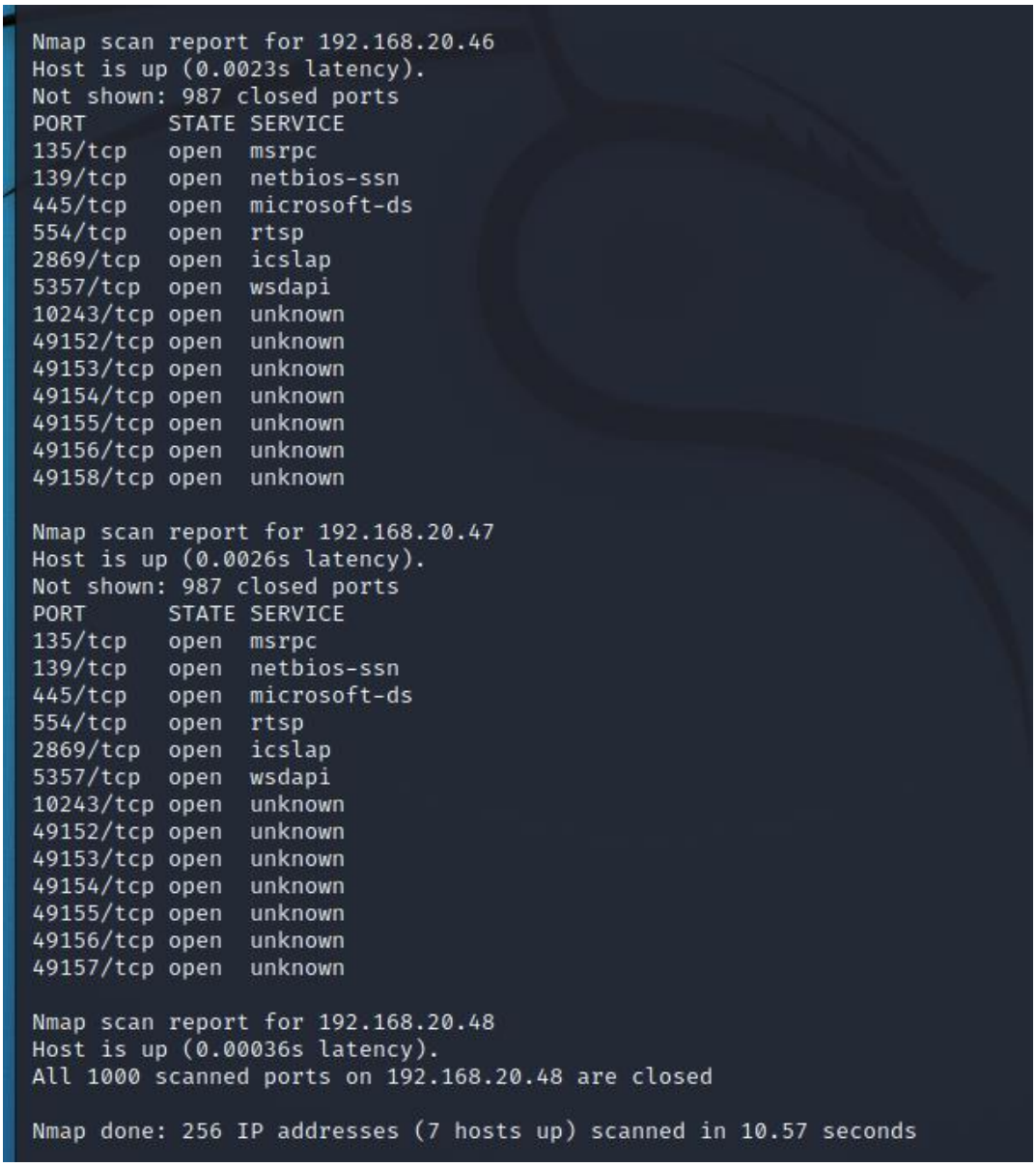
- Se procede a realizar un escaneo de reconocimiento de puertos desde la máquina virtual que tiene el Kali Linux con la herramienta Nmap se realizara un reconocimiento de la red con un escaneo de puertos desde la máquina virtual con Kali Linux con IP 192.168.20.48 hacia las IP's, y las maquinas con sistemas operativos Windows 7 y Windows 7 x64 tienen las direcciones IP's asignadas la 192.168.20.46 y 192.168.20.47 posteriormente, se procede a realizar el análisis con Nmap con el comando: nmap 192.168.20.0/24 luego se procede a dar enter para escanear el segmento de red especificado en el comando y detecte todas las direcciones IP que se encuentren en el segmento de red pero nos enfocaremos en especial en las dos direcciones IP's que tiene los sistemas operativos Windows 7 con direcciones IP's: 192.168.20.46 y 192.168.20.47 como vemos en las siguientes imágenes:

Figura 21. Escaneo de puertos con nmap



Fuente: Autor

Figura 22. Resultados del escaneo



Fuente: Autor

12.1 ANÁLISIS DE LA VULNERABILIDAD.

- **Nessus**

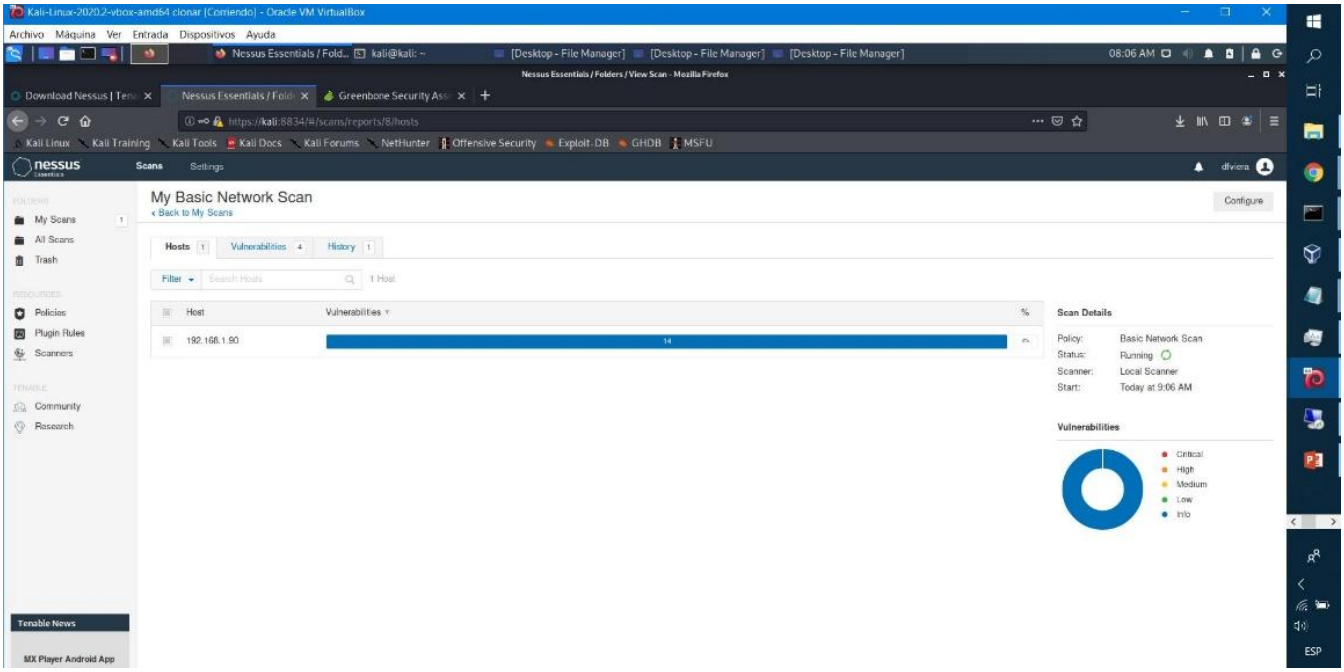
Nessus es una solución de seguridad muy conocida por realizar escaneo de vulnerabilidades sobre la red, la cual permite identificar vulnerabilidades en un sinfín de sistemas operativos, aplicaciones, y también permite ver los puertos abiertos en los sistemas escaneados. Se pueden obtener informes muy detallados de los escaneos realizada donde indica la criticidad de las vulnerabilidades encontradas y los exploit que se pueden utilizar para ser explotadas pero adicional también indica los planes de remediación que se le pueden aplicar a las vulnerabilidades encontrada y los parches de seguridad que se le pueden aplicar para mitigarlas. Se debe tener presente que la función "unsafe test" (pruebas no seguras) se recomienda desactivarse debido que puede generar indisponibilidad en los servicios.
Nessus permite tener dos opciones para elegir son dos versiones "Home" y "Work", una es gratuita y la otra es de paga o cual limita algunas funciones.

Para ingresar al entorno web digitamos Kali:8834 en el navegador para continuar con el procese de instalación y configuración el cual nos solicitara los datos para avanzar en el proceso.

Cuando ya este actualizado, podremos ingresar al entorno web, y podremos hacer el escaneo a las maquinas víctimas, pero primero se hace un escaneo de prueba y se puede observar que si funciona la herramienta como vemos

en la imagen:

Figura 23. Analisis Básico

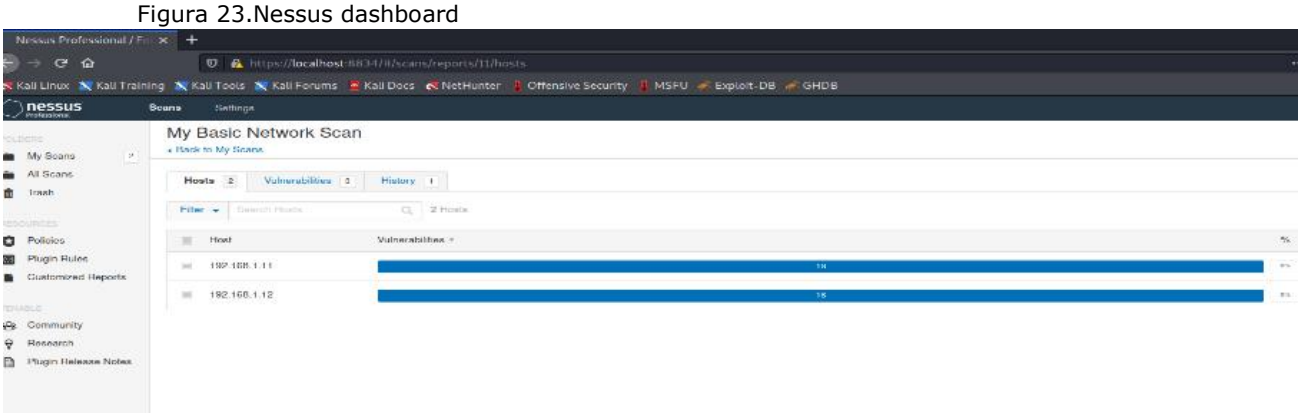


Fuente: Autor

Para la siguiente fase del laboratorio y habiendo descubierto los puertos sensibles en las maquinas víctimas y teniendo en cuenta el punto anterior, realizaremos un escaneo para las maquinas con sistema operativo Windows 7.

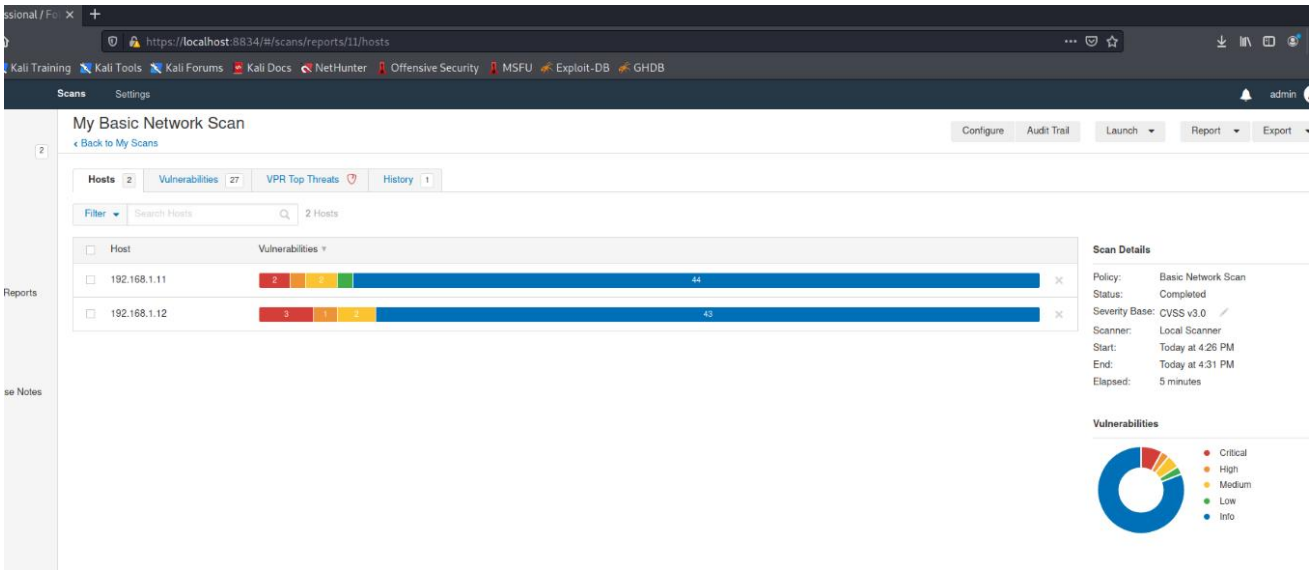
Por medio del tablero de la herramienta Nessus nos permitirá ver detalladamente el alcance que tiene en la red y el avance con el análisis de las vulnerabilidades halladas en los sistemas que se utilizaron para el laboratorio.

Figura 23.Nessus dashboard



Fuente: Autor

Figura 24. Resultado Análisis Nessus



Fuente: Autor

Con base al análisis se identificaron los dos hosts y poseen muchas vulnerabilidades

El servidor virtual x64 tiene 50 Vulnerabilidades (192.168.1.12)

4% de Vulnerabilidades Criticas (2)

2% de Vulnerabilidades Altas (1)

4% de Vulnerabilidades Medias (2)

2% De vulnerabilidades Bajas (1)

88% Informativas (44)

Servidor 32 Bits tiene 49 Vulnerabilidades (192.168.1.11)

6% de Vulnerabilidades Criticas (3)

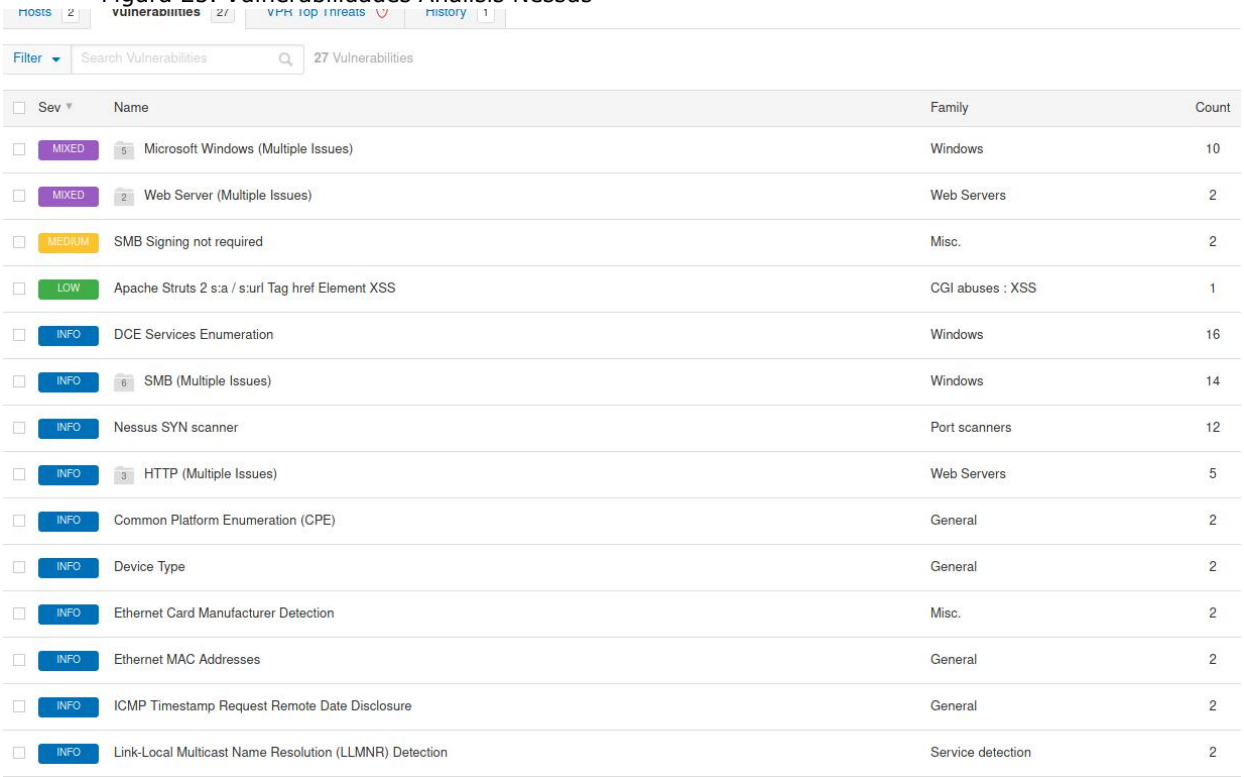
2% de Vulnerabilidades Altas (1)

4% de Vulnerabilidades Medias (2)

88% Informativas (43)

Luego se extrae un informe con todas las vulnerabilidades de los sistemas analizados y definido con las siguientes calificaciones: Critica, Alta Media y baja. Identificando cuantas computadoras o servidores tienen la urgencia de ser parchados.

Figura 25. Vulnerabilidades Análisis Nessus



Hosts 2 | Vulnerabilities 27 | VPR Top Threats | History 1

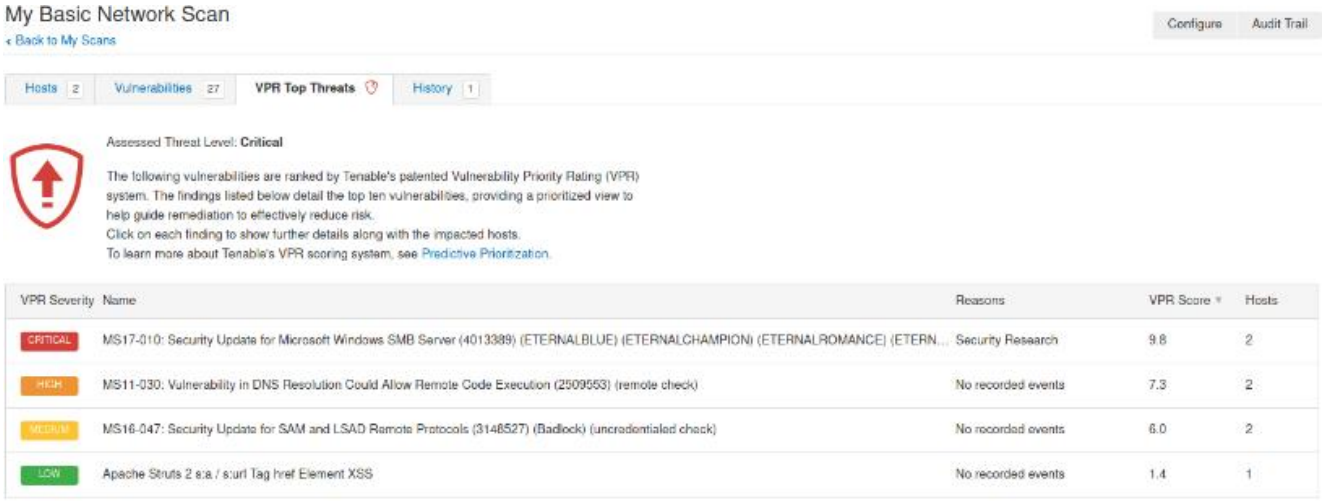
Filter | Search Vulnerabilities | 27 Vulnerabilities

Sev	Name	Family	Count
MIXED	Microsoft Windows (Multiple Issues)	Windows	10
MIXED	Web Server (Multiple Issues)	Web Servers	2
MEDIUM	SMB Signing not required	Misc.	2
LOW	Apache Struts 2 s:a / s:url Tag href Element XSS	CGI abuses : XSS	1
INFO	DCE Services Enumeration	Windows	16
INFO	SMB (Multiple Issues)	Windows	14
INFO	Nessus SYN scanner	Port scanners	12
INFO	HTTP (Multiple Issues)	Web Servers	5
INFO	Common Platform Enumeration (CPE)	General	2
INFO	Device Type	General	2
INFO	Ethernet Card Manufacturer Detection	Misc.	2
INFO	Ethernet MAC Addresses	General	2
INFO	ICMP Timestamp Request Remote Date Disclosure	General	2
INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	2

Fuente: Autor

Las vulnerabilidades encontradas en el análisis se clasifican en Criticas, Altas y Medias y bajas existen otras de carácter informativo que por lo general no se tienen mucho en cuenta debido que ya están implícitas en los equipos por tener habilitados servicios necesarios para su funcionamiento con base en esto se recomienda aplicar el plan de remediación para las vulnerabilidades Críticas, Altas, Medias y altas que por lo general a las críticas se deben solucionar en un periodo máximo de un mes y las altas en dos meses y para las medias de 3 a 6 meses para su corrección.

Figura 26. Vulnerabilidades Ranking



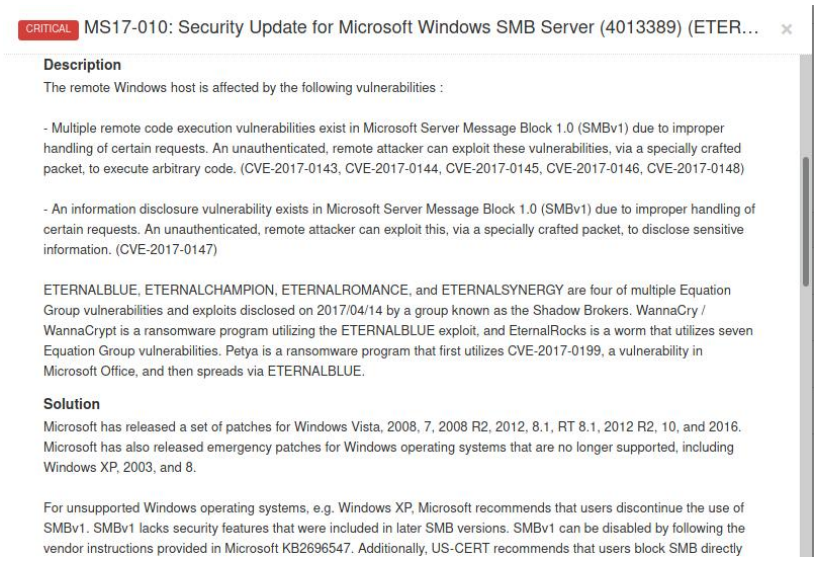
Fuente: Autor

Luego de analizar las vulnerabilidades detectadas por la herramienta Nessus Scan las vulnerabilidades críticas son las primeras que se deben trabajar de forma inmediata por el impacto que pueden llegar a tener sobre los equipos, en este caso podemos observar una de las vulnerabilidades más críticas hoy en día y es la del puerto 445 abierto la cual puede permitir a un atacante o una APT realizar un ataque por ransomware.

Figura 27. Ms17-010 Descripción

Fuente: Autor

Figura 28. Descripción Vulnerabilidad



Fuente: Autor

12.2 CARACTERIZACIÓN DE LOS PROCESOS ANTERIORMENTE MECIONADOS:

• MS17-010 (crítica): 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.

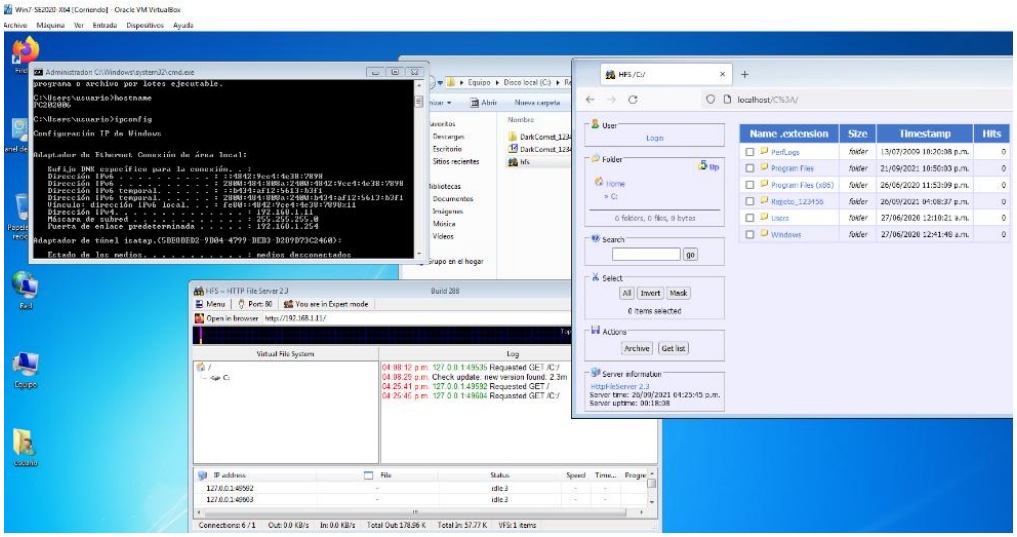
• MS11-030 (Alta): Idéntica las fallas en la característica de forma del DNS de Windows, permite realizar las consultas de resolución de nombres de multidifusión del enlace, los cuales se pueden aprovechar para ejecutar códigos arbitrarios en contextos de cuentas Network Service.

• MS16-047 (Medium): 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.

12.3 EXPLOTACION DE REJETTO CON METAEXPLOIT

Lo que se debe hacer primero es seleccionar el servidor anfitrión donde estará la aplicación en este caso vamos a utilizar un windows7 64, para alojar la aplicación Rejetto con el propósito de analizar los puertos que utiliza la aplicación por medio de Nmap desde la máquina virtual con Kali Linux.

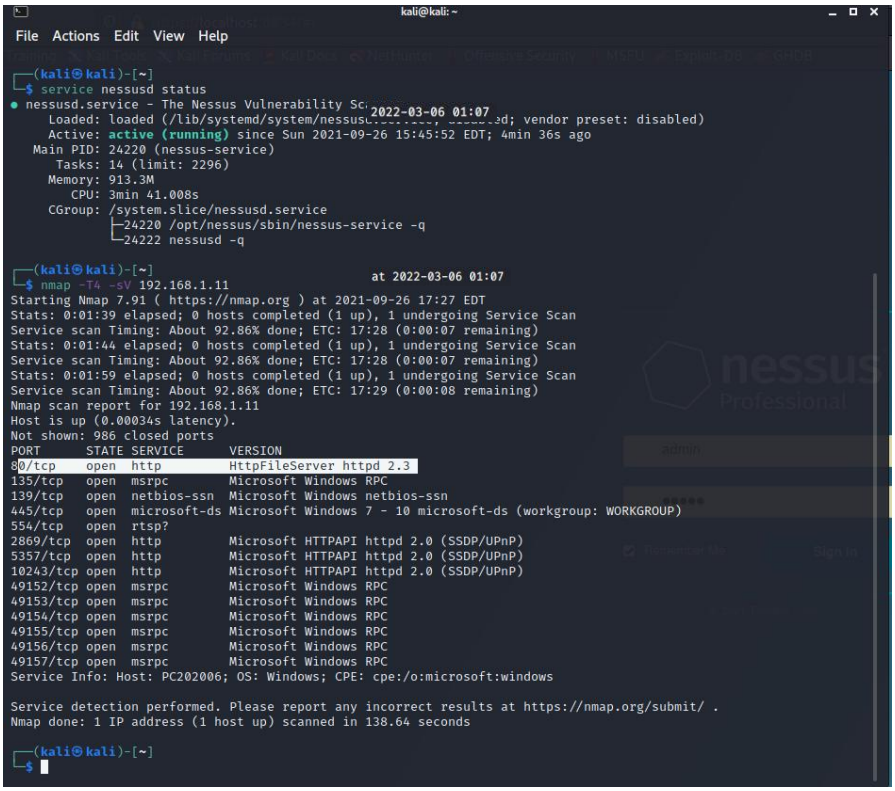
Figura 29. Ejecución rejjeto



Fuente: Autor

Desde la máquina virtual con Kali Linux ejecutaremos la herramienta Nmap con el siguiente comando: nmap -T4 -sV 192.168.1.11(IP maquina Windows 7 64 Bits) el cual nos permitirá saber los puertos abiertos el cual nos muestra: 80: HTTP y la version del 2.3 que es la versión del Rejjeto.

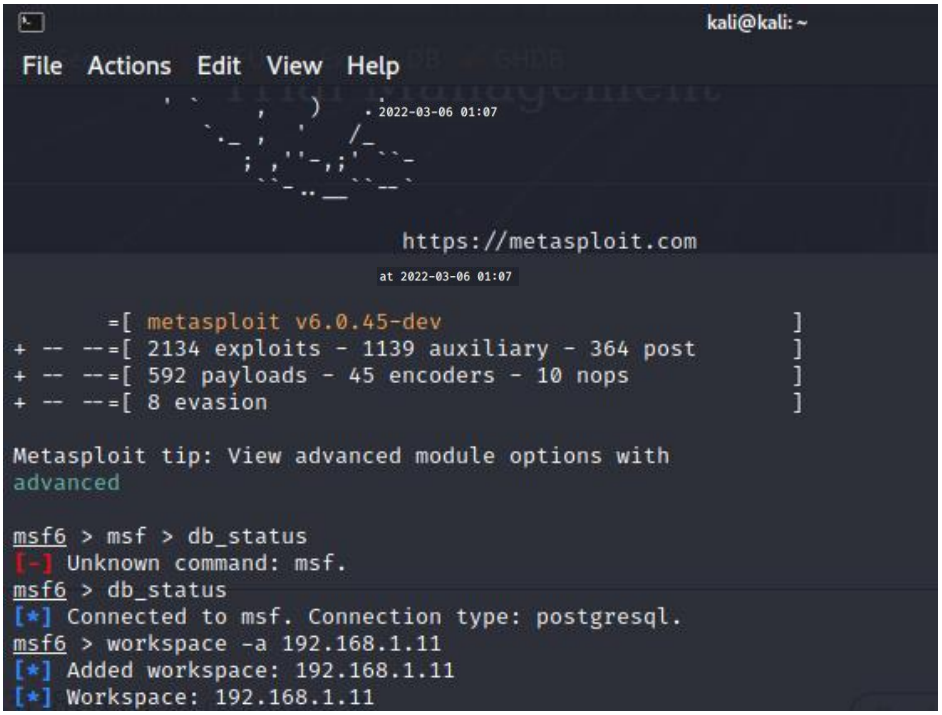
Figura 30. puertos abiertos windows7



Fuente: Autor

Luego crearemos el espacio de trabajo para ejecutar la consola de metaesploit con el Servidor victima al cual vamos a atacar.

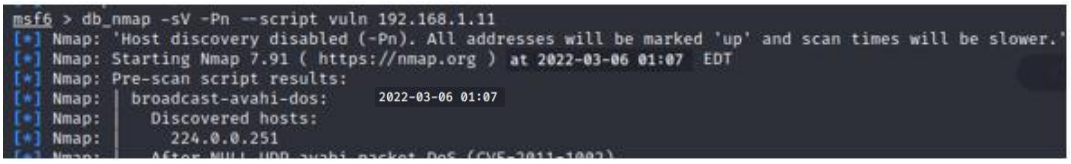
Figura 31. Ejecución del exlpoit



Fuente: Autor

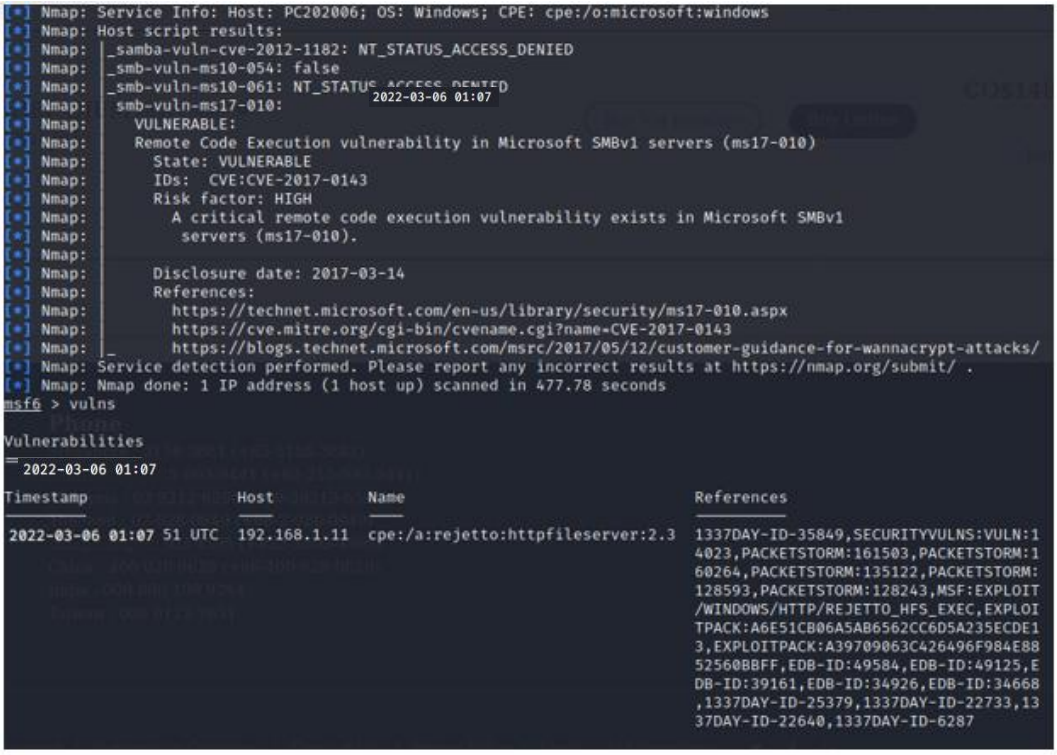
Luego ejecutamos el análisis de la vulnerabilidad para identificar las brechas de seguridad que tiene el servidor que vamos a explotar:

Figura 32. vulnerabilidades con Metasploit



Fuente: Autor

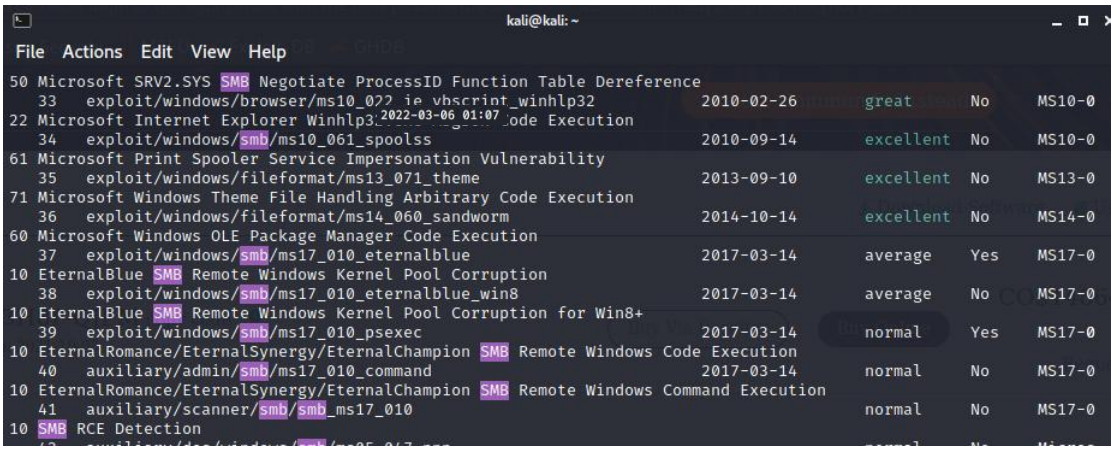
Figura 33. Resumen Vulnerabilidades metasploit



Fuente: Autor

Luego nos aparece la opción de search y buscaremos la vulnerabilidad del puerto 445 SMB que en este caso sería el puerto vulnerable que vamos a explotar. Luego de esto nos aparecerán los exploit que permiten explotar esta vulnerabilidad del SMB.

Figura 34. Search Metaexploit



Fuente: Autor

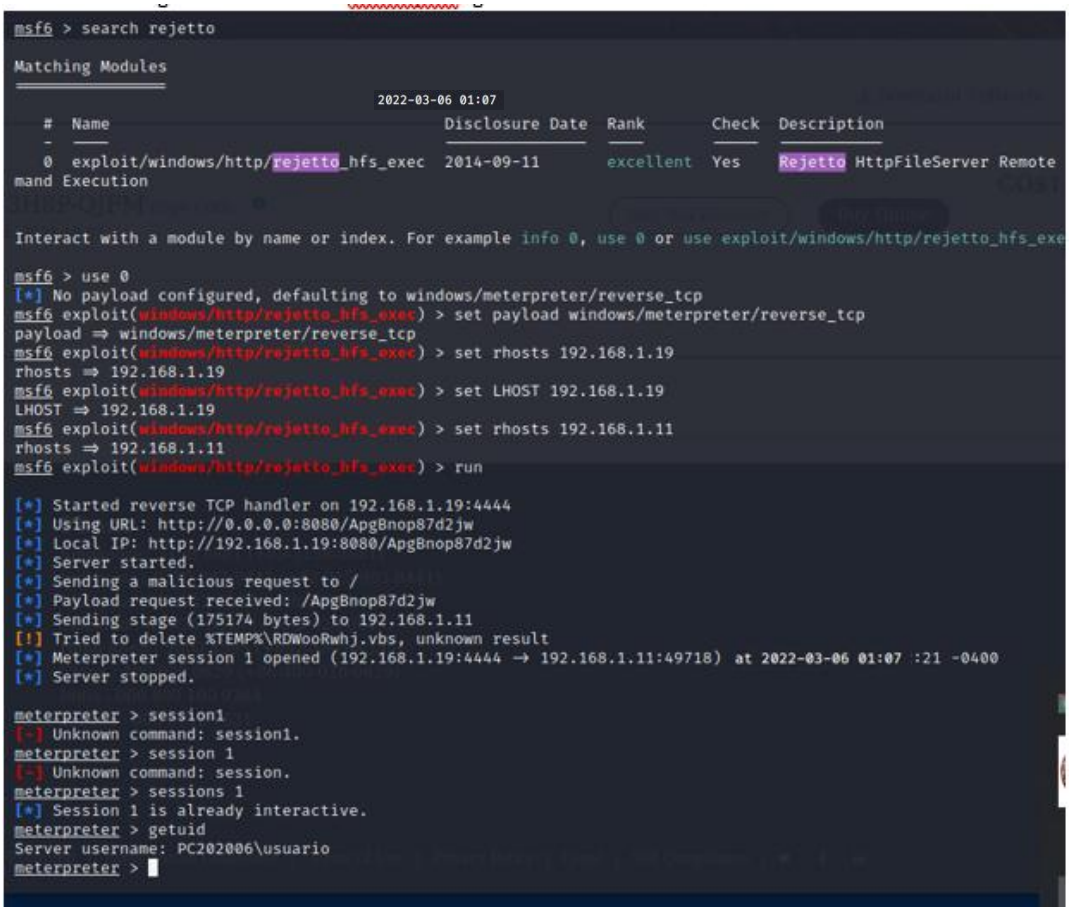
Utilizaremos el código “0” para este caso Use 0

Vamos a utilizar y configurar el Payload: set payload Windows/meterpreter

Vamos a configurar el host remoto: set rhosts

Vamos a configurar el Host Local: set LHOST KALI

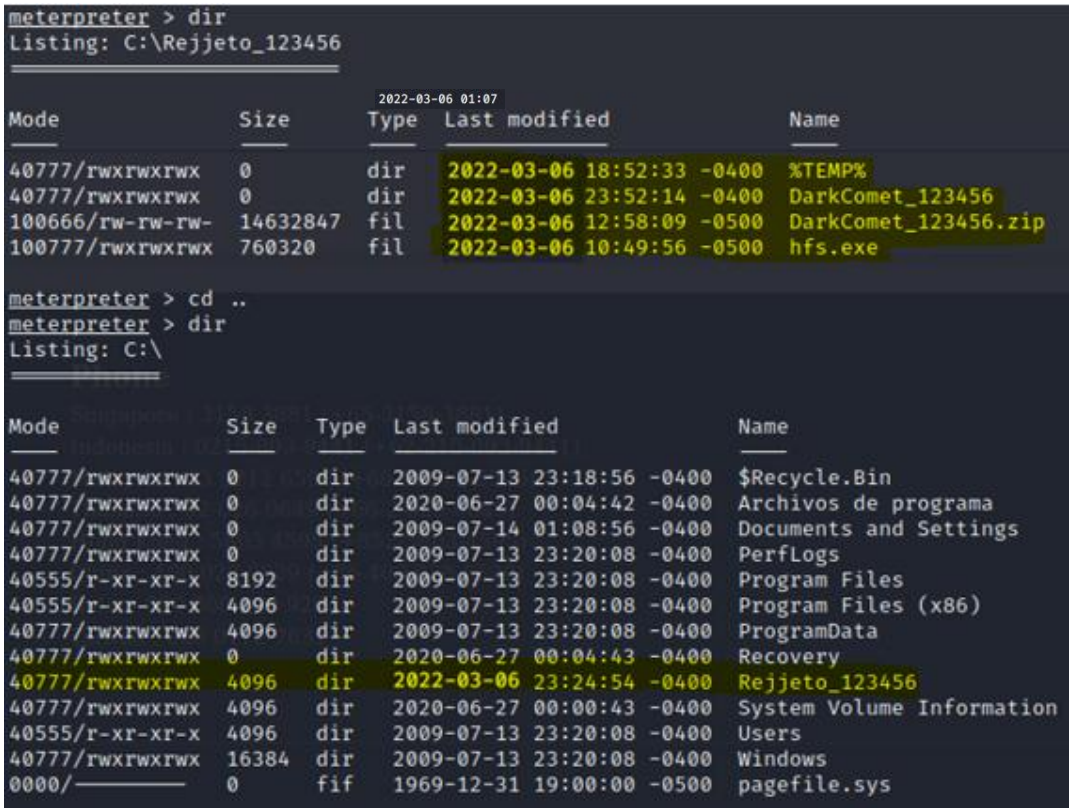
Figura 35. Utilizando el código de Vulnerabilidad Metaexploit



Fuente: Autor

Luego de esto encontraremos el meterpreter que es un intérprete que nos permitirá la conexión y así podremos ejecutar los comandos que necesitemos en los sistemas operativos Windows para confirmar que realmente estamos dentro del servidor remoto (victima).

Figura 36. Ejecución de comando Windows por medio de Meterpreter



Fuente: Autor

12.4 CREANDO USUARIO APROVECHANDO LA VULNERABILIDAD

Luego de estar adentro del servidor victima explotando la vulnerabilidad con metasploit ingresaremos a la Shell del sistema operativo Windows para saber los procesos que están corriendo en este momento en la máquina.

Figura 37. Ejecución Shell desde meterpreter

Fuente: Autor

- Ejecución de comando por medio de meterpreter

Net localgroup (listar grupos del Equipo Vulnerado)
Net User DanielViera /add (Crear un usuario local en el equipo vulnerado)

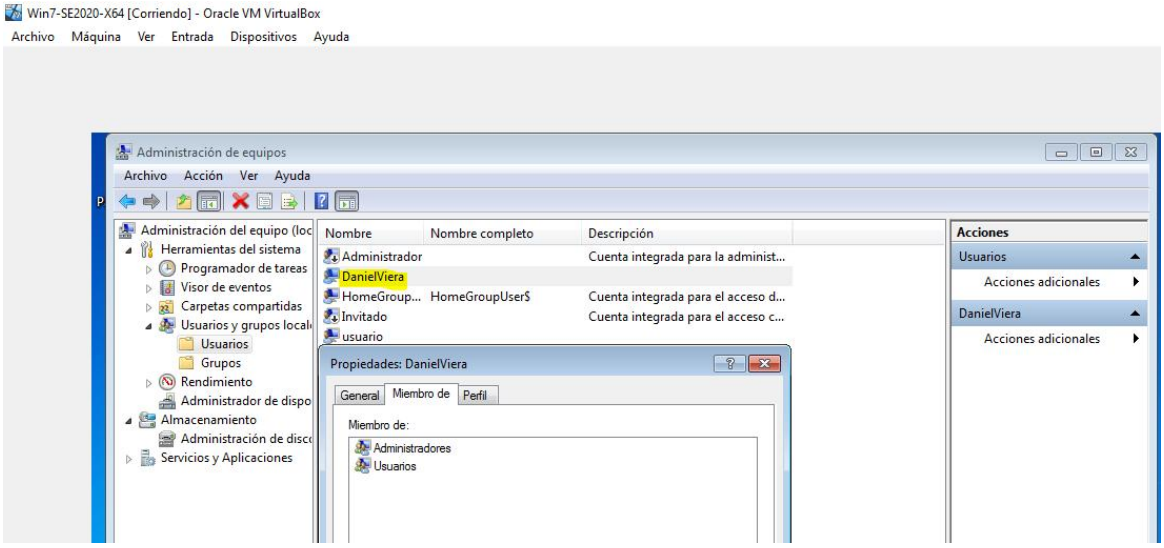
Figura 38. comando creación de Usuarios meterpreter.

Fuente: Autor

- Net localgroup Administradores DanielViera /add (Agregar el usuario creado al grupo administradores del Equipo vulnerado)

Para validar y evidenciar que realmente logramos acceso a la maquina víctima validamos el usuario que fue creado en este caso DanielViera

Figura 39. Evidencias Windows 7.



Fuente: Autor

Estos ataques por lo general son utilizados por APT para ejecutar RATs o hacer labores de ciber espionaje lo cual le permite tener control de la maquina remotamente con el fin de hacer uso de la información que se encuentre alojada en el servidor, de esta forma se puede evidenciar que el atacante tiene el control total de la maquina sin que la víctima lo sepa.

Esta amenaza consiste es explotar una vulnerabilidad por el puerto 445 que le permita a un atacante tener hacer cargue de Payload, Downloader de información o de malware para infectar la red y poder escalar privilegios sin problema dentro de la red para hacer movimientos laterales y ganar acceso sin ser detectado. Se evidencia como el administrador del sistema se ve la creación del usuario con permisos de administrador en el servidor.

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

Para esta fase de la explotación a la máquina virtual con sistema operativo Windows que por lo general son los más vulnerables, herramientas de código abierto para el análisis de vulnerabilidades en sistemas operativos y aplicaciones de diferentes fabricantes son de gran apoyo para los equipos de Red Team y Blue Team pero también para los administradores debido que facilitan detectar las falencias que tienen los sistemas para poder mitigar estos riesgos que se detecten de forma oportuna para reducir la superficie de ataque para impedir que los sistemas sean vulnerados por los hackers y afecten los activos críticos y la información que se encuentra almacenada en ellos se vea expuesta. Se puede evidenciar que los puertos abiertos en los sistemas deben de tener una razón de ser y los servicios o puertos sensibles innecesarios deben ser cerrados para reducir el riesgo también proteger la dirección IP, MAC DNS que pueden vulnerados con muchas técnicas avanzadas que hoy en día periten suplantar la identidad de un host en la red haciéndose pasar por otro. Cuando se detecta una vulnerabilidad en algún servicio puede ser explotado con algún exploit público y poder cargar un playload utilizando una Shell y con el meterpreter poder escalar privilegios a nivel de usuario en el sistema operativo de la víctima lo cual permitirá crear, modificar y eliminar directorios, archivos o modifica registros o llaves del REGEDIT lo cual puede ser grave para salvaguardar la seguridad de los datos que se encuentren en la compañía debido que también los atacantes pueden hacer movimientos laterales en el sistema operativo y en la red lo cual puede ser un gran riesgo por el nivel de compromiso al que se ve expuesta la empresa debido que podría llegar a tener acceso a otros equipos de cómputo del área financiera, contable entre otras.

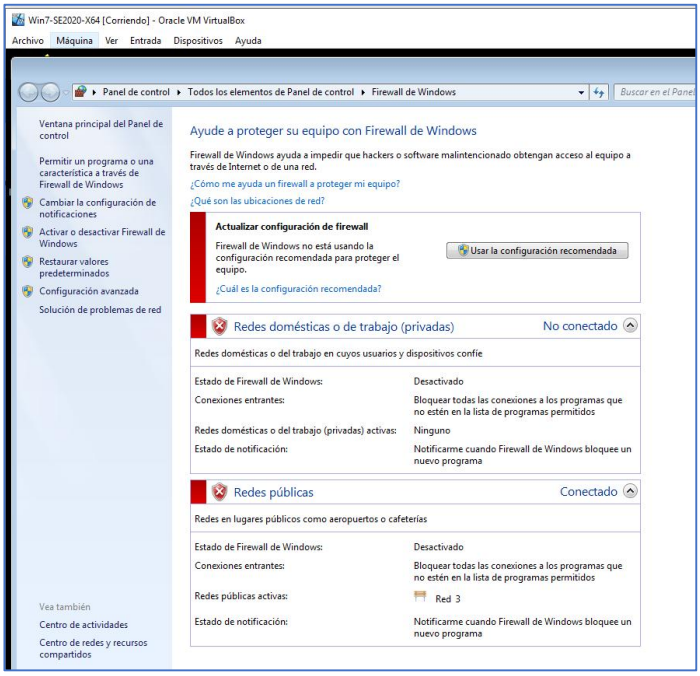
12.6 ACCIONES PARA TOMAR FRENTE A UN CASO DE ATAQUE INFORMÁTICO EN TIEMPO REAL

Cuando se habla de la seguridad en sistemas informáticos no se puede decir que existe un sistema completamente seguro y una solución que sea efectiva 100% frente amenazas como lo son las APT's por lo que se recomienda tener un proceso detallado para la respuesta a incidentes el cual indique el proceder y de cómo contener un ataque de la forma más efectiva y rápida posible, como lo puede ser teniendo un GRIS en el cual se notique a los interesados tomar las mejores decisiones para afrontar un ataque a gran escala, como aislar zonas de la red o computadoras y luego analizar los equipos que no fueron afectados por el ransomware o malware para descartar algún tipo de compromiso y así realizar una limpieza un análisis de los equipos infectados.

A continuación, se describen los pasos que se realizaran sobre el objetivo atacado con sistema operativo Windows 7 X64:

- Validación del estado del Endpoint del equipo victima el cual se encuentra desactivado:

Figura 39. Configuración de firewall desactivada.

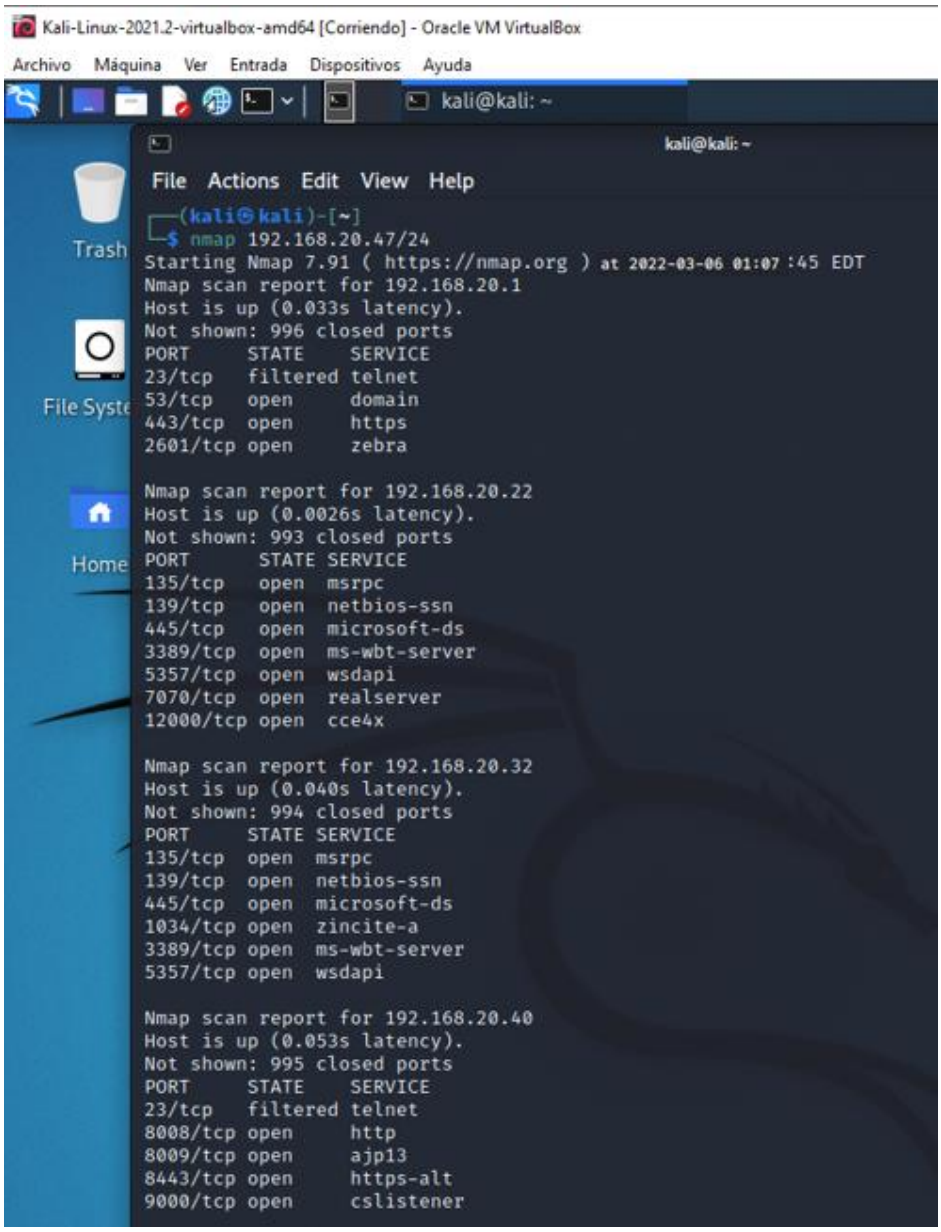


Fuente: Autor

- Se valida el estado del equipo para confirmar que no tenga todos los parches de seguridad y evitar la explotación de alguna vulnerabilidad por estar actualizado por lo que se recomienda que este desactivado las actualizaciones automáticas como configuración recomendada:

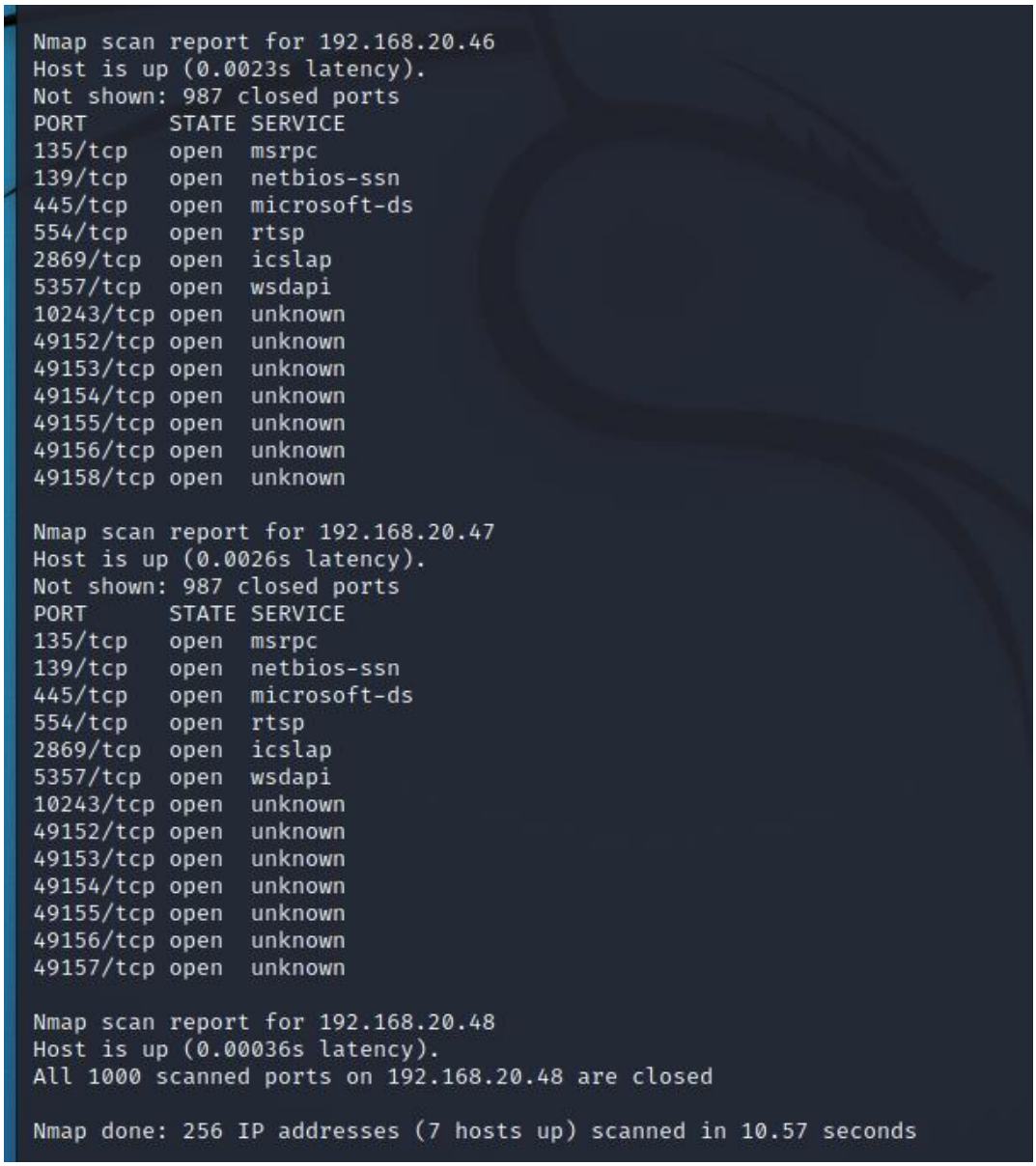
- Se realiza escaneo de los equipos que están en el segmento de red con la herramienta Nmap la cual está en la máquina virtual de Kali Linux con dirección IP: 192.168.20.48 que realizara los escaneos hacia las direcciones IP's 192.168.20.46 y 192.168.20.47 que tienen sistema operativo 7, se ejecutara el comando nmap 192.168.20.0/24 el cual corresponde al segmento de red, pero nos enfocaremos en las direcciones IP del ambiente del laboratorio que hemos implementado para esta etapa 4.

Figura 40. Analisis con Nmap



Fuente: Autor

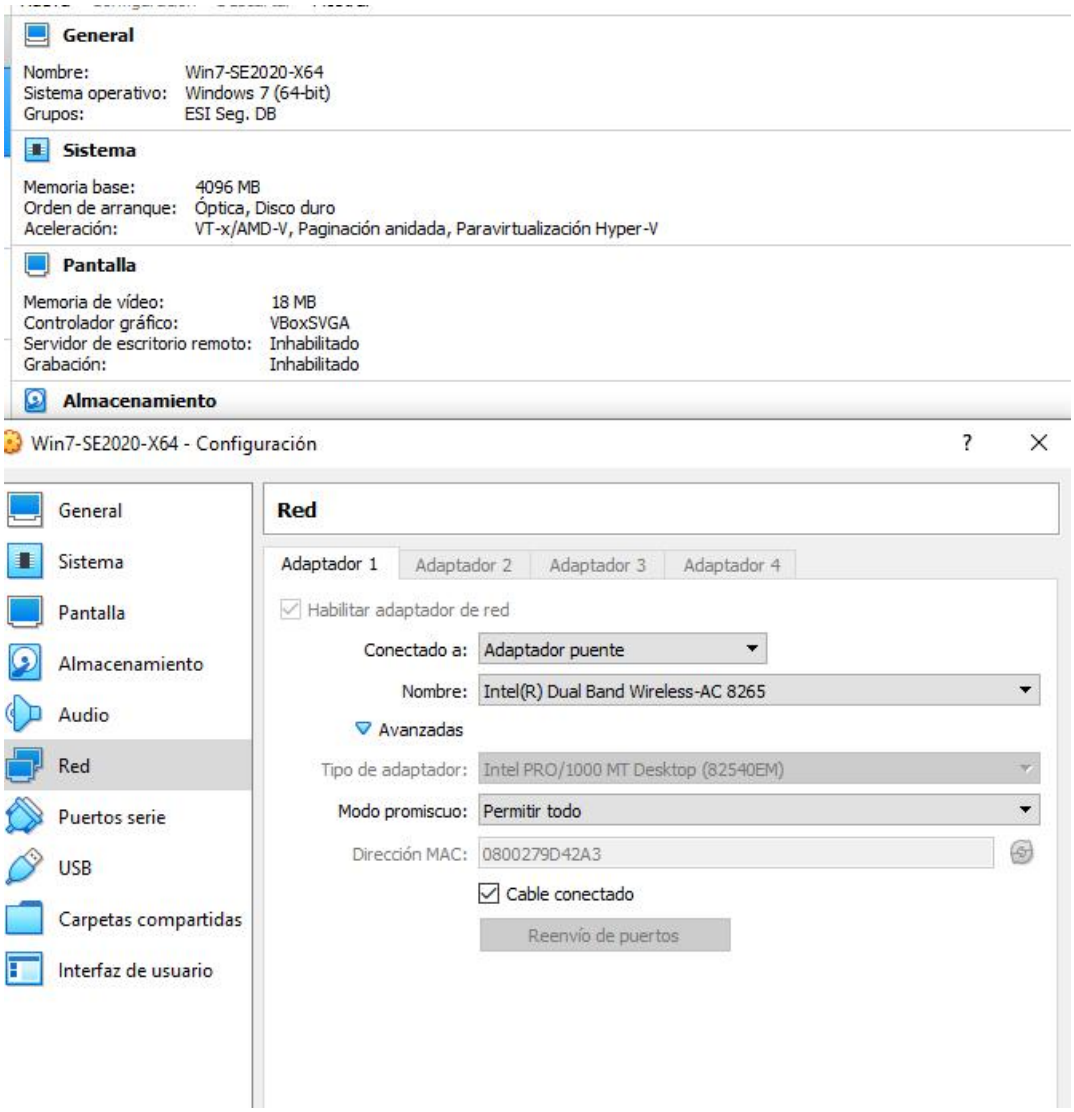
Figura 41. Análisis nmap



Fuente: Autor

- Se valida la configuración de la tarjeta de red la cual debe estar configurado en modo promiscuo lo cual quiere decir que escuchará todo y permitirá todo el tráfico que pasa atabes de las interfaces de la máquina virtual como podemos observar en las siguientes imágenes:

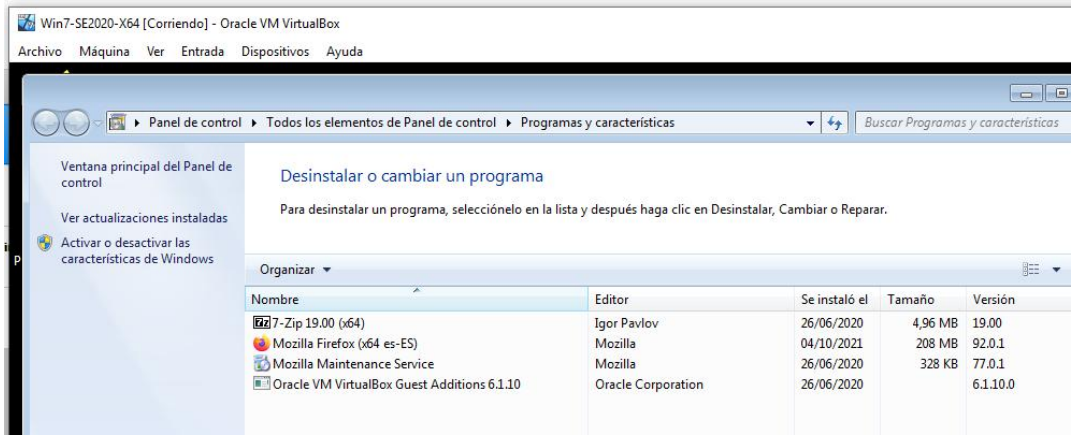
Figura 42. Validación tarjeta de red



Fuente: Autor

- Se valida que no exista instalado un programa antimalware, antivirus o EDR en la máquina virtual con sistema operativo Windows 7 x64 luego de revisar esto se confirma que no existe nada que pueda afectar las pruebas como podemos observar en la siguiente imagen:

Figura 43. Verificación de antivirus



Fuente: Autor

Se deben tener presente las siguientes recomendaciones para la detección de ataques informáticos:

- **Prevención de ataques:** esto nos permite tomar una posición de postura de seguridad y acciones de las metodologías para prevenir ataques en una etapa temprana o en una primera fase de reconocimiento de los ataques que son la de Fingerprinting y Footprinting donde se puede visualizar tráfico anual en la red.

- **Recomendaciones**: hacer respaldo de la información diarios de la información que se considere critica de la organización, tener soluciones antimalware como EDR, Endpoint, filtrado de contenido web, deshabilitar puertos sensibles expuestos hacia internet.

- **Detección:** Se debe tener soluciones como IDS, IPS y analizadores de red que tengan filtros para poder identificar diferentes tipos de ataques en la red, se debe monitorear la red constantemente como soluciones como PTR o SolarWinds que permitan apoyar el proceso de monitoreo

y adicional tener un SOC (Security Center Operation) el cual apoya a la visibilidad de la red y también ayuda a la detección de amenazas avanzadas como las APTs, malware y ransomware.

- **Ataques comunes:** Ransomware, DDoS, DoS, Virus, Gusanos, Adware, Phishing, Troyanos, Spaer Phishing, Ingeniera Social.

- **Ciberresilencia:** Las empresas deben definir un plan de Ciberresilencia y un plan de continuidad donde se tenga un plan claro donde se pueda definir las aplicaciones y sistemas críticos de la organización el cual permita tener recuperación de los sistemas y hacer pruebas constantes de la posible indisponibilidad de los sistemas, aplicaciones y cuánto tiempo se demoran en recuperarse frente a un ciberataque o un desastre natural.

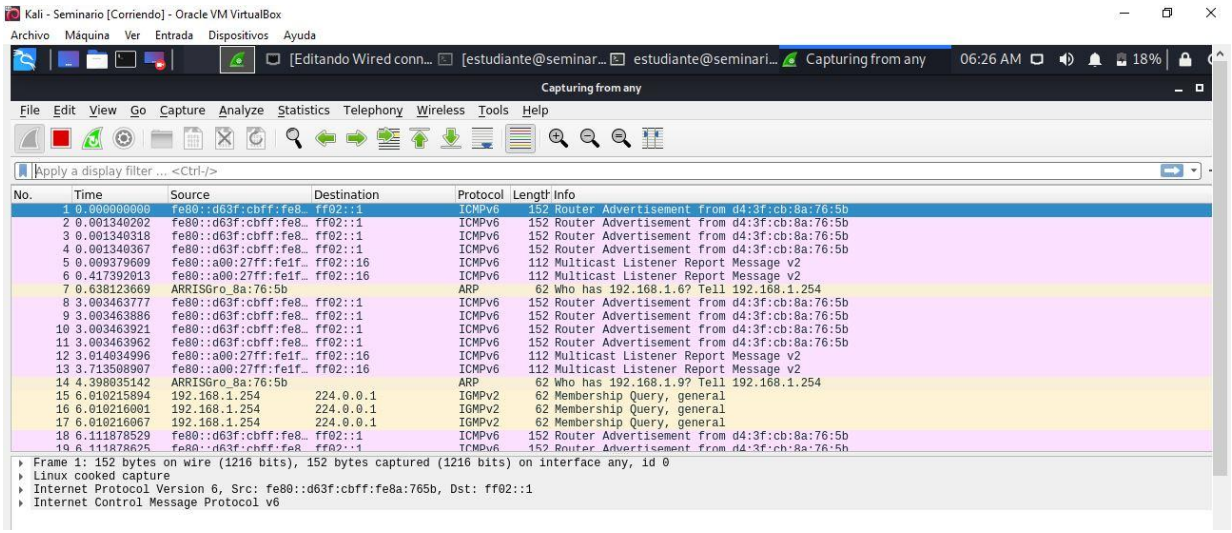
- **Primero:** Se debe tener un roadmap y definir las aplicaciones críticas y sistemas que estarán en el plan de continuidad y Ciberresilencia.
- **Segundo:** Detallar el proceso de respuesta a incidentes y de cómo se debe contener un ataque en las fases iniciales que permitan
- **Tercero:** Tener detallado el proceso del PRD donde se realicen dos pruebas integrales al año y 3 pruebas individuales por cada aplicación para saber los tiempos de recuperación y retorno a la normalidad.
- **Cuarto:** este proceso se debe dar a conocer a todos los empleados debido que deben formar parte de la logista a la hora de una incidencia ya sea por un ciberataque o por una falla natural, esto con el propósito de conocer las pérdidas a nivel informático, financiero y de capital humano que afectaría los procesos de la empresa y en el cual se pueda generar sinergia entre todas las áreas para tener un proceso claro y efectivo al momento de ejecutarlo.

13 HARDENIZACIÓN PARA MINIMIZAR O MITIGAR ATAQUES DE SEGURIDAD INFORMÁTICA

Para aplicar planes de remediación a los sistemas e infraestructura que tiene la organización se debe tener un PTR (Plan de Tratamiento de Riesgos) donde se le realice seguimiento a cada hallazgo y se le permita dar cierre a cada uno donde se describan vulnerabilidades, actualizaciones de seguridad, donde se identifiquen puertos sensibles en la red o ataques, malware, escaneos de red.

Se procede a realizar monitoreo de la red con la herramienta gratuita WireShark permitiendo detallar todo el tráfico que pasa por la red de la empresa, para saber si se detalla algún tipo de ataque.

Figura 44. Analisis de tráfico



Fuente: Autor

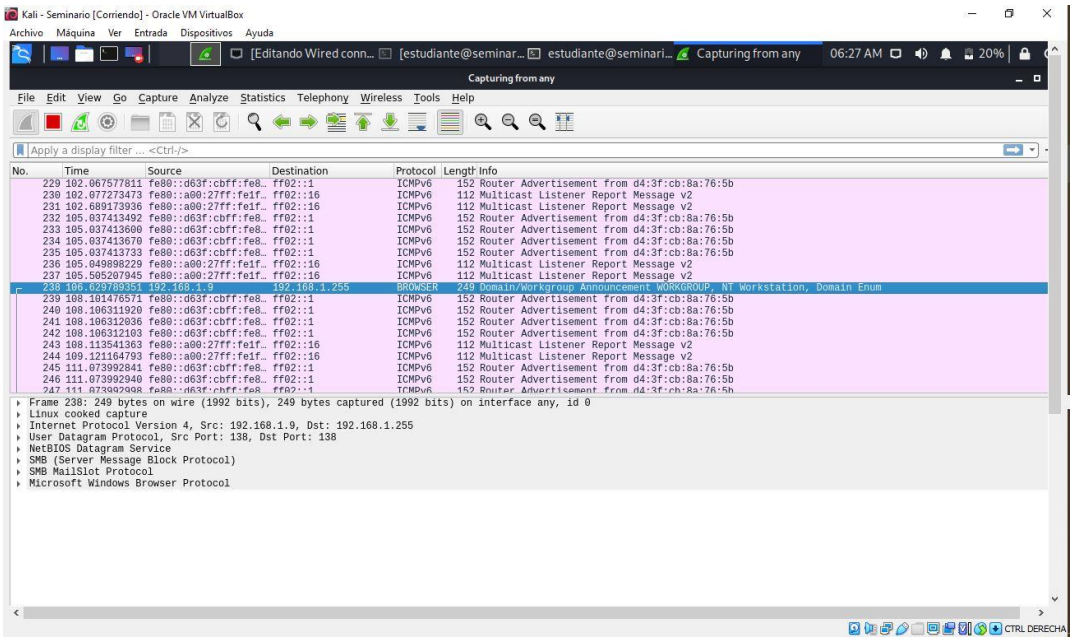
Explicación de los diferentes colores que aparecen en la herramienta WireShark cuando se realiza el análisis:

- Rojo: problema critico en el paquete de red tendrá un mensaje de "error"
- Amarillo: Indica atención. En los paquetes analizados podrá aparecer "Warn"

- Celeste: situaciones relevantes fuera del funcionamiento normal de la red.

- Gris: información detallada del flujo de paquetes de red que pasan por la interfaz que tiene configurada el WireShark y aparece la palabra "Note".
- Se muestra evidencia del análisis:

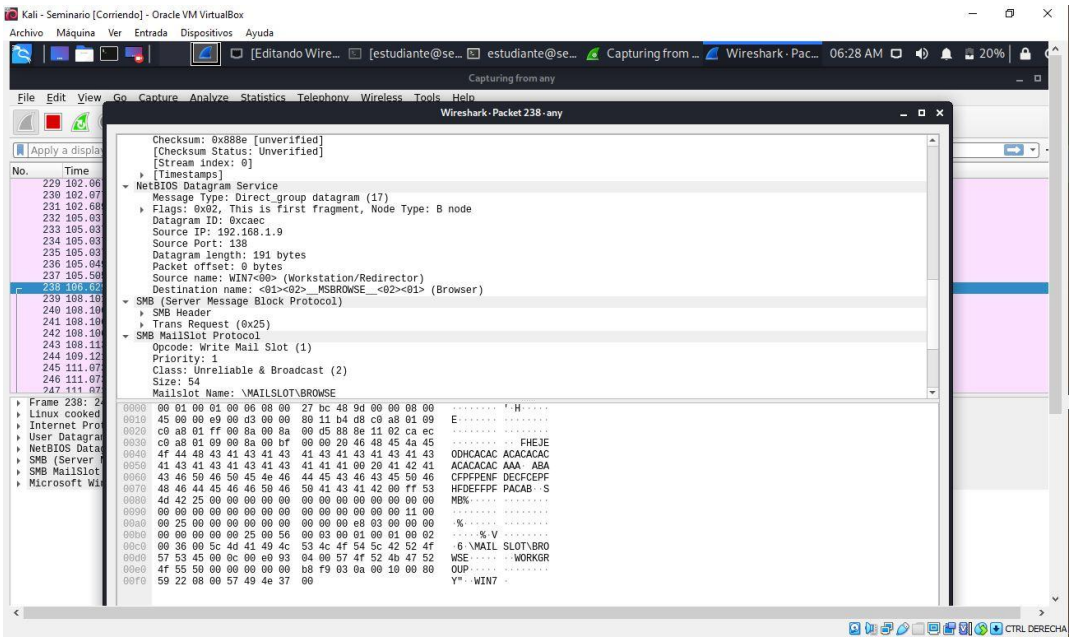
Figura 45. Analisis de trafico



Fuente: Autor

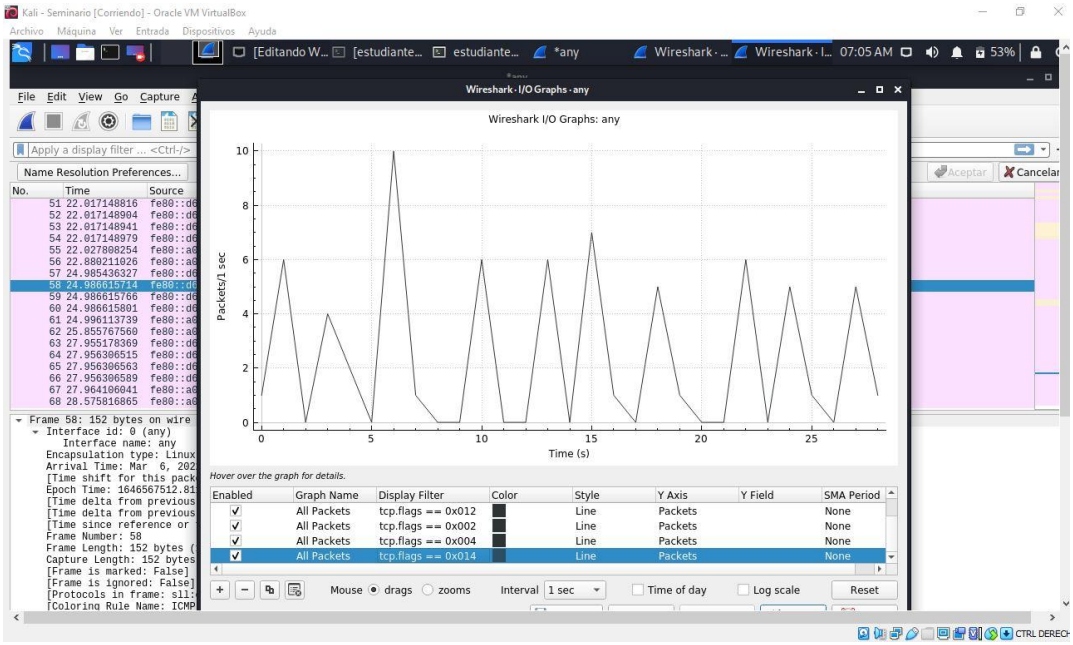
La siguiente imagen muestra el análisis del tráfico de red abriendo un paquete de red detectado por la herramienta y explica a detalle la comunicación.

Figura 46. Analisis de paquete



Fuente: Autor

Figura 47. Grafica de umbrales de tráfico e información de red

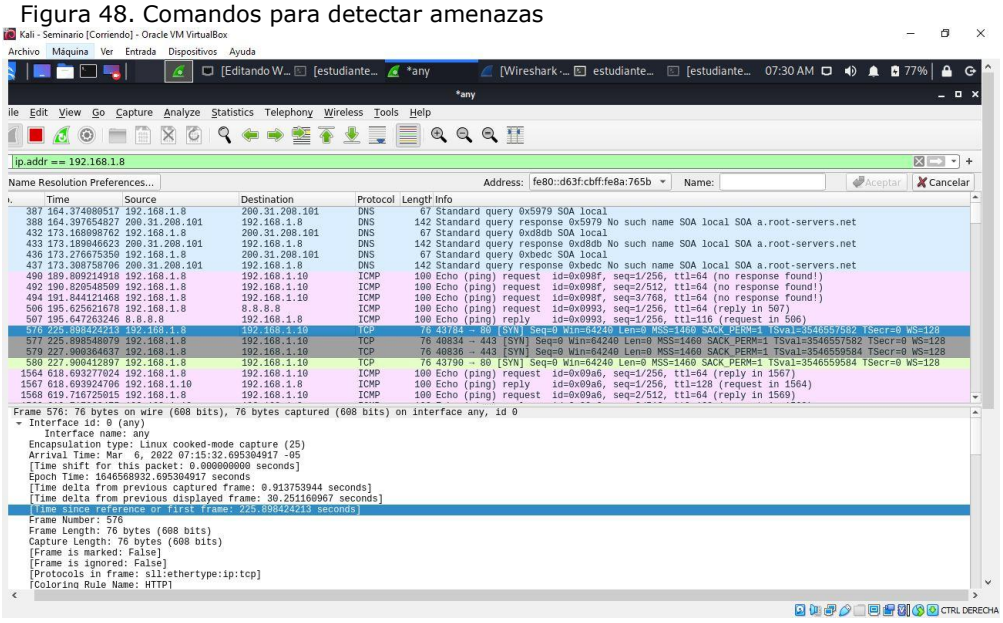


Fuente: Autor

Podemos detallar con esta grafica el pico que se realizó al momento del escaneo con la herramienta Nmap la host víctima y la transmisión de paquetes en la red.

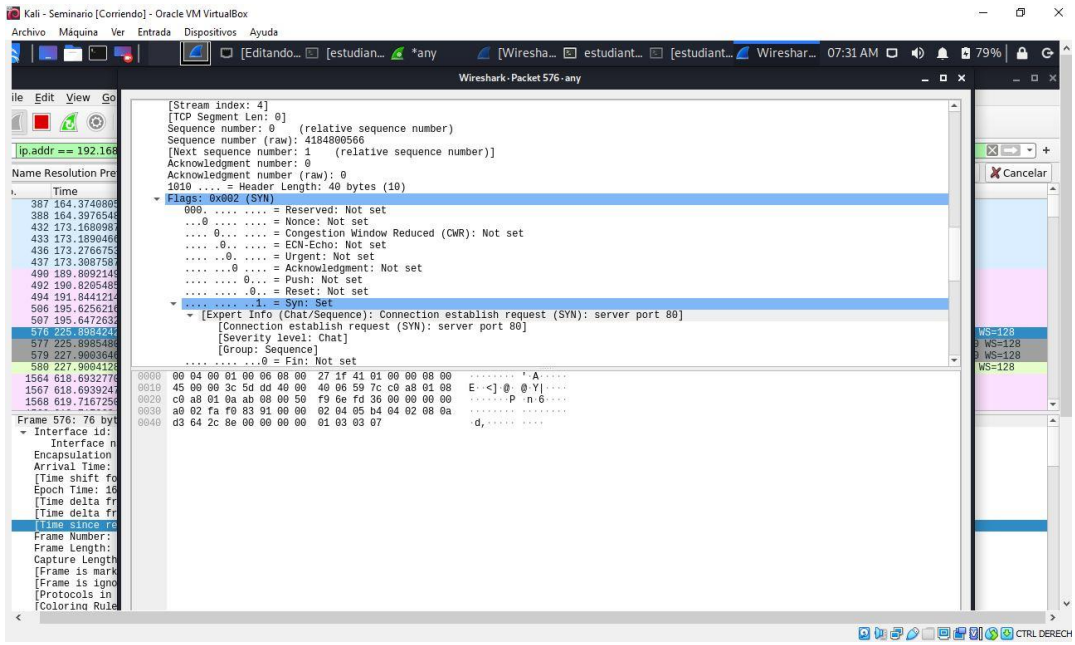
Luego de analizar el tráfico de la red se toman las siguientes medidas en la herramienta WireShark para identificar ataques informáticos en la red.
Se agregan los siguientes filtros para identificar un escaneo, ataques de DDos, DoS, suplantación ARP, ataques de inundación de SYN en la red:
Para obtener paquetes SYN, SYN + ACK, RST y RST + ACK, utilice el *filtro "tcp.flags == 0x012 o tcp.flags == 0x002 o tcp.flags == 0x004 o tcp.flags == 0x014*
Para obtener paquetes ICMP tipo 3 con código 1, 2, 3, 9, 10 o 13, use *"icmp.type == 3 y (icmp.code == 1 o icmp.code == 2 o icmp.code = = 3 o icmp.code == 9 o icmp.code == 10 o icmp.code == 13) "* filtro.
tcp.flags == 0x000 tcp.flags == 0X029 icmp.type == 3 y icmp.code == 3 icmp.type == 3 y icmp.code == 2 tcp.flags.syn == 1 tcp.flags.ack == 0

Figura 48. Comandos para detectar amenazas



Fuente: Autor

Figura 49. Comandos para detectar amenazas



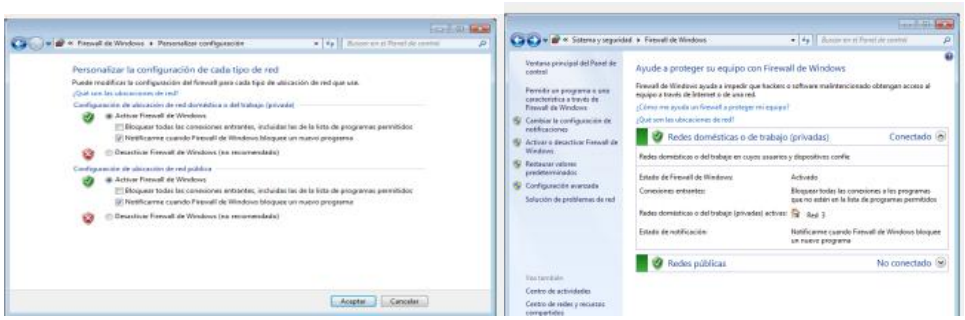
Fuente: Autor

Aquí podemos detallar el escaneo que se realizó con la herramienta Nmap desde la dirección IP: 192.168.1.8 hacia la IP de la víctima: 192.168.1.10

Luego de hacer el análisis de riesgo de la red, se realiza hardening a los equipos activando el firewall y se realiza la instalación del antivirus gratuito para ayudar a identificar cambios en los sistemas protegidos frente ataques informáticos:

- Se procede activar la solución de seguridad en la maquina Windows 7

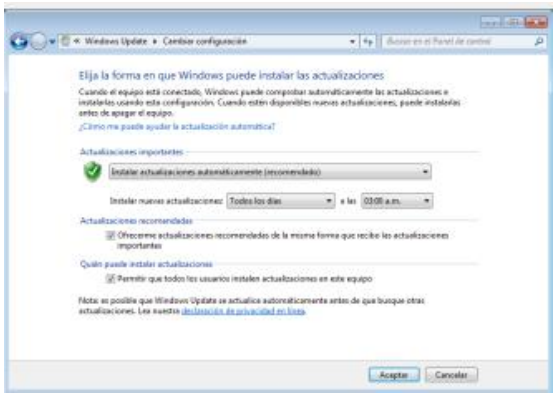
Figura 49. Activar protección



Fuente: Autor

- Se procede habilitar las actualizaciones de Windows:

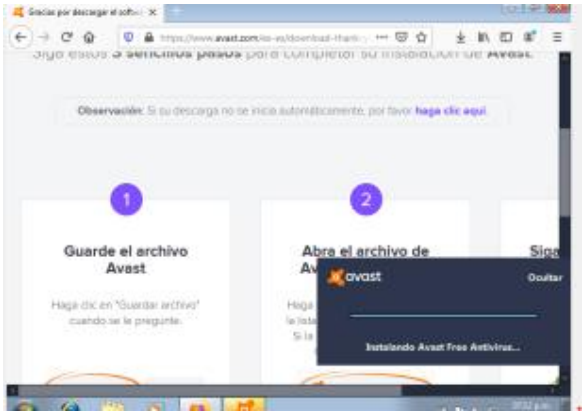
Figura 50. Activación actualizaciones



Fuente: Autor

- Se procede a instalar antimalware AvastFree en el Windows 7:

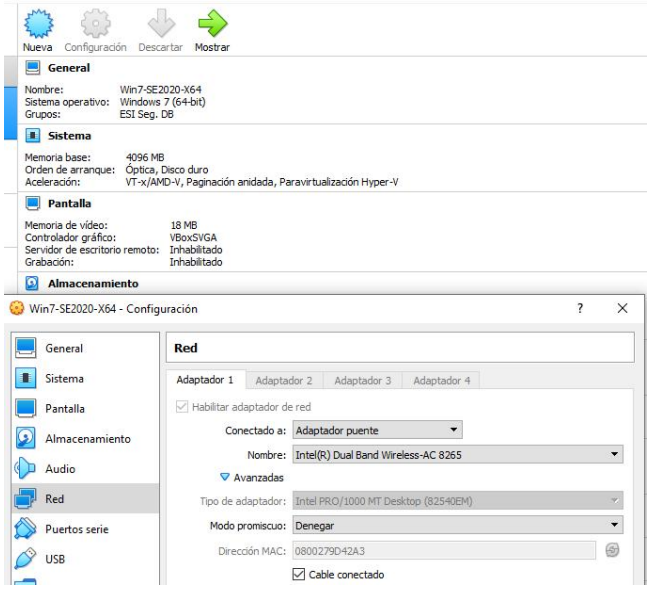
Figura 51. Activar protección



Fuente: Autor

- Se procede a modificar la configuración de la tarjeta de red en la máquina virtual a modo promiscuo para tener acceso a todo el tráfico:

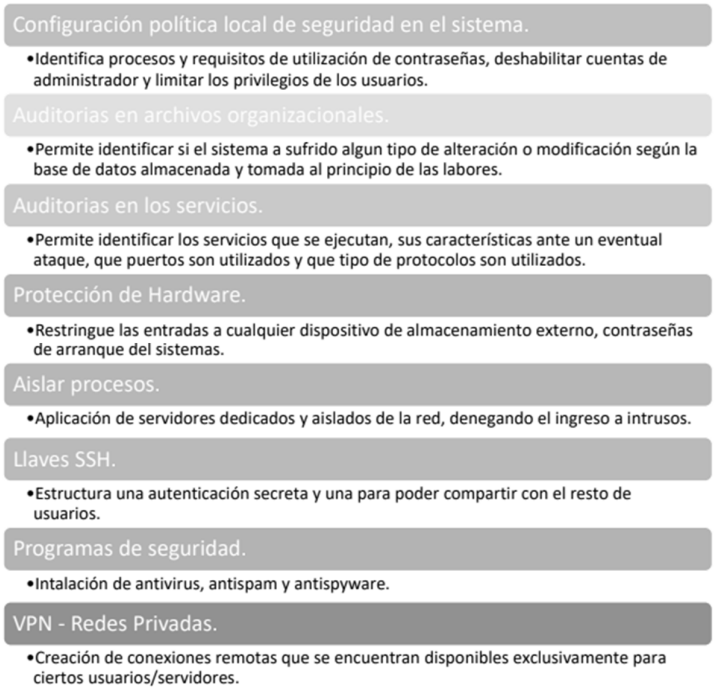
Figura 52. Configuración tarjeta de red



Fuente: Autor

Cabe resaltar que es de suma importancia conocer las mejores prácticas que ayudan a tener oportunidad en la repuesta frente ataques informáticos:

Figura 53. Mejores prácticas



Fuente: https://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/

14 DIFERENCIA ENTRE UN BLUE TEAM Y EQUIPO DE RESPUESTA A INCIDENTES

En el siguiente cuadro comparativo observaremos las diferencias y características más relevantes de ambos equipos:

Tabla 1. Comparación blueteam y respuesta a incidentes

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.

Fuente: https://www.sciencedirect.com/science/article/pii/S071686402030095X

15 ANÁLISIS DE TRABAJAR CON CIS "CENTER FOR INTERNET SECURITY" PARA ROPUESTA 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 ciberdefensa. 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 instalació 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.
- 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.

•Interceptar comunicaciones y conexiones inalámbricas en la red de la empresa.

• 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.

16 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 ventos. 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.

17 . HERRAMIENTAS PARA LA CONTECIÓN DE ATAQUES INFORMÁTICOS

A continuación, se realizará el testeo de las herramientas de código abierto y se detallara como podrían apoyar la gestión de los equipos de red team y blue para las pequeñas empresas, lo criterios son con base a la calificación que muchos expertos califican como las mejores.

Para el equipo de red team se recomiendan las siguientes en herramientas:

Suricata: Es una herramienta de código abierto que cumple las funciones de IDS e IPS en la red lo cual permite detectar intrusiones en tiempo real y tomar acciones inmediatas para detener un ataque en tiempo real y sirve como apoyo para los equipos de Blue Team para monitorear en línea todos los eventos en la red, también permite definir reglas para reducir los falsos positivos.

Evebox: Una solución de código abierto que se apoya en el motor de detección suricata para detectar amenazas en la red

The Hive: Es una herramienta de código abierto que ayuda a la respuesta a incidentes y se integra muy bien con MISP plataforma de intercambio de información de malware a nivel mundial.

Firewall OPNsense next Generation Firewall: Este tipo de solución de código abierto ayuda detectar y bloquear tráfico malicioso previamente definido para no bloquear servicios legítimos y permite aplicar controles en la red como:

- Aplication control
- Url Filtering
- VPN- Site to Site
- Encryted attacks protección
- Acceleration SSL

Docker: Esta solución nos permite llevar a cabo la monitorización de todo el análisis del correlacionador de eventos con pocos recursos en un servidor virtualizado que permita tener toda la fase de correlación de eventos.

[2]**Snort:** Es un IDS de código abierto que tiene la capacidad para realizar análisis de tráfico en tiempo real y registro de paquetes en redes.

Security Onion: Es una herramienta de código abierto que permite tener visibilidad del tráfico de la red generando alertas sobre las actividades sospechosas.

OpenWIPS-NG: Herramienta de código abierto ayuda a la detección de amenazas y prevención de ataques en redes inalámbricas.

OSSEC: Es un IDS que permite el análisis de los paquetes en la red comprobando la integridad y supervisión de registros en los sistemas operativos generando alertas en tiempo real para una respuesta oportuna a un incidente de seguridad.

Open Source Tripwire: Esta herramienta de código abierto es detectar cambios en los objetos del sistema de archivos. Como inicios de sesión y explora el sistema de archivos según las instrucciones configuradas en el sistema y almacena la información de cada archivo, cuando se cambian los archivos en exploraciones futuras, los resultados se comparan con los valores almacenados anteriormente para saber si ha sufrido cambios.

HIDS: Es una herramienta de detección de intrusiones que proporciona salvaguardas y seguridad en la red frente a las intrusiones informáticas.

IDS basados en firmas: Es una herramienta de código abierto que permite inspeccionar los paquetes de la red y comprarlos con las firmas integradas

[2] **2016.** *Hackers Don't Have to Be Human Anymore. This Bot Battle Proves It.* [En línea] 8 de 5 de 2016. https://www.wired.com/2016/08/security-bots-show-hacking-isnt-just-humans/.

para detectar patrones maliciosos de ataque preconfigurados y predeterminados.

IDS basados en anomalías: es una herramienta que permite el monitoreo de la red en tiempo real y permite el análisis de puertos y está basado en comportamiento si un umbral supera la línea establecida alertara de una posible intrusión

IDS Pasivo: Solo ayuda a la detección y alerta de eventos sospechosos en la red.

Para el equipo de blue team se recomiendan las siguientes en herramientas:

MISP: Es una herramienta de código abierto de intercambio de información de malware, ransomware, virus que sirve para recopilar, almacenar, distribuir y compartir indicadores de compromiso de seguridad cibernética y análisis de malware.

AlienVault Open Threat Exchange: Es una herramienta de acceso público para la gran comunidad de internet y ayuda a los equipos de blue team poder saber las tendencias diarias sobre amenazas de día cero y proporciona indicadores de compromiso de amenazas generados por la comunidad, permite la investigación colaborativa y automatiza el proceso de actualización de la infraestructura de seguridad con datos de amenazas desde cualquier fuente.

VirusTotal: Es una plataforma para el análisis de amenazas e indicadores de compromiso gratuita que permite a los equipos de blue team y red team tener mayor certeza de los archivos, urls, direcciones IP, dominios que pueden ser maliciosos para prevenir ataques antes de que sucedan.

Implementar nodo de un MISP en una organización ayuda a mejora las capacidades de ciberseguridad y de análisis de datos, especialmente en términos de correlación, almacenamiento, procesamiento de datos y visualización de la información. Los MISP permiten obtener indicadores de compromisos en forma oportuna lo cual permite dar oportunidad a la respuesta frente a un incidente que podrían evitar un incidente. un MISP El objetivo de fondo es tomar medidas pro-ciberseguridad sin esperar que existe

un marco normativo ideal, y beneficiar a diferentes comunidades a nivel mundial mediante una fórmula de colaboración probada y exitosa, que permita formar una cultura organizacional de ciberseguridad en nuestro ecosistema y poder generar sinergias y tener una seguridad proactiva.

Alien Voult OTX

Es una de las herramientas de código abierto más potentes de la industria de ciberseguridad que ayudan a proteger la información de las empresas su producto estrella es Open Threat Exchange (OTX), es una herramienta de código abierto comunitaria que brinda respuesta a amenazas de seguridad. La herramienta permite a los expertos en ciberseguridad investigar de una forma granular y hacer parte de una gran comunidad colaborativa y enfrentar estas nuevas amenazas, aplicando una nueva capacidad que hoy en día se debe tener en cuenta y es la inteligencia artificial para analizar gran cantidad de datos de diversas fuentes de datos para luego integrar los datos analizados y obtener información recopilada e integrarla a los sistemas de seguridad.

OTX y otras propuestas de uso código abierto, en AlienVault ofrecen un producto de pago es una solución de seguridad llamada Unified Security Management que integra lo mejor de ambas plataformas para la detección de amenazas, la respuesta a incidentes y la gestión de la seguridad unificada.

SandBox Cuckoo

Esta herramienta nos permite realizar el análisis de malware estático y dinámico para poder extraer el comportamiento del malware dentro de una máquina y comprender su funcionamiento y poder extraer los indicadores de compromiso para luego ser aplicados en las herramientas de seguridad como Endpoint, firewall’s, WAF, EDR’s.

Firewall de aplicaciones web: (WAF) es un elemento que busca resguardar los sistemas web mediante el monitoreo y filtrado del tráfico

tipo HTTP entre el servidor de la aplicación web e Internet. Generalmente, resguardar las aplicaciones web de ataques como la inyección de SQL, inclusión de archivos, la falsificación de cross-site, cross-site-scripting (XSS), entre otros.

Un WAF, que no está creado para todos los ataques, pero en su lógica se desarrolla una defensa holística en contra de varios vectores de ataque. Proteger una aplicación web con un WAF, es colocar una protección entre el sistema web e Internet. A diferencia de un servidor proxy que buscar proteger la identidad de una máquina cliente mediante un intermediario, con un WAF se busca proteger al servidor de la exposición haciendo que los usuarios cliente pasen por el firewall antes de llegar al servidor.

Los WAF trabaja mediante reglas o políticas que protegen contra vulnerabilidades en la aplicación ya que filtran el tráfico malicioso. La ventaja de esta tecnología radica en la facilidad y velocidad con la que se puede modificar una política, generando respuesta rápida a los posibles vectores de ataque.

Funcionamiento

La mayoría de WAF's procesan en tráfico entrante de manera similar a través de cinco etapas:

- Analizar el paquete HTTP que envía el usuario cliente.
- Seleccionar la regla o política dependiendo del tipo de parámetro de entrada.
- Normalizar los datos para ser analizados.
- Aplicar una regla de detección.
- Decidir si el paquete es o no dañino.

Aquí, el WAF define si termina la conexión o pasa el tráfico al nivel de aplicación. En el cuarto punto, Aplicar una regla de detección funciona diferente dependiendo del WAF los cuales se basan en los diferentes parámetros para ser clasificados así:

- Expresiones regulares.
- Reputación de paquetes.
- Detección de anomalías.
- Generador de puntuación
- Tokenizadores.
- Analizadores léxicos.

Ventajas

Los WAF proporciona respuestas inteligentes, de acuerdo con la configuración de seguridad web y las amenazas que podría afectar una red. Los WAF se diseñaron para robustecer la seguridad de la red de posibles amenazas no conocidas como por ejemplo ataques de día cero, inyección de SQL, vulnerabilidades de seguridad, ataques de secuencias de comandos entre sitios, entre otro que utilizan el navegador como vector de ataque.3 Los WAF implementados de manera correcta ayudan a mitigar los ataques de tráfico excesivo o botnets, DDos manteniendo el tráfico de aplicaciones sin afectaciones mientras defiende en paralelo los flujos de datos maliciosos.

A continuación, se realizarán tres ataques a la maquina 1 utilizando las herramientas disponibles en la maquina 2 con Kali Linux.

18 RECOMENDACIONES

En el presente documento se recomiendan las herramientas de código abierto que pueden utilizar los equipos de red team y blue team para realizar las consultorías a las empresas deben tomar consciencia y tomar la iniciativa de implementar modelos de seguridad bajo normas internacionales y estandartes de seguridad o framework con el apoyo de controles por medio de herramientas de código abierto que permitan implementar una postura de seguridad que ayude a reducir la superficie de riesgo de un ataque, esta investigación pretende recomendar herramientas de código abierto que generen sinergias entre los equipos de red team y blue team que permitirán a las empresas a generar ciber resiliencia frente a las amenazas del hoy implementando SOC internos o por outsourcing que les permitirá medir el nivel de madurez en el que se encuentran las empresas y proponer PTR (Plan de Tratamiento de Riesgos) para corregir los hallazgos que se encuentren con el análisis de vulnerabilidades y de riesgos de la infraestructura expuesta a un ataque informático.

Enlace del Video de la Sustentación del Trabajo:

https://youtu.be/VfyiMPc4FSo

CONCLUSIONES

En las empresas es necesario que se cree un área de ciberseguridad compuesta por personas con habilidades técnicas avanzadas que permitan ejecutar todas las tareas que impliquen la posible afectación de un sistema informático.

De acuerdo con el ejercicio realizado muestra la importante de tener todos los sistemas informáticos al día con sus parches de seguridad para evitar la explotación de vulnerabilidades críticas que pongan en riesgo la integridad de toda una empresa. El equipo conformado por las personas de ciberseguridad, deberán tener capacidades especiales y tener dominio de toda la administración y gestión de las políticas de seguridad informática para tener claro las fases de un Blue Team y un Red Team.

El personal del área de ciberseguridad ejecutar proyectos y estrategias, que permitan mitigar los ataques informáticos y permitan responder frente a un incidente de ciberseguridad y se debe contar con un equipo de respuesta a incidentes que por lo general hace parte del equipo de Blue Team que es un aliado estratégico para los administradores de los sistemas, que cuentas con las habilidades para contener, recuperar y responder a un incidente con todas las capacidades necesarias para afrontar un ciberataque.

Lo ideal sería que las personas que estarían a cargo de la seguridad de los sistemas tengan conocimientos en normas de seguridad informática y de leyes colombianas que le permitan tipificar los delitos informáticos con el propósito de que el personal no incurra en conductas antiprofesionales y garantizando los tres pilares de la seguridad confiabilidad, integridad y autenticación.

BIBLIOGRAFÍA

Angry Org. 2014. *Angry IP Scanner.* [En línea] 2014. [Citado el: 5 de Julio de 2020.] https://angryip.org/.

blog.segu-info. 2020. https://blog.segu-info.com.ar/2020/01/misp-y-thehive-herramientas-para.html?m=0. *blog.segu-info.com.ar.* [En línea] 20 de enero de 2020. https://blog.segu-info.com.ar/2020/01/misp-y-thehive-herramientas-para.html?m=0.

cdn-cybersecurity. 2021. La automatización de la seguridad. *https://cdn-cybersecurity.att.com/docs/product-briefs/DS_Server-ES.pdf.* [En línea] 3 de 6 de 2021. https://cdn-cybersecurity.att.com/docs/product-briefs/DS_Server-ES.pdf.

cisecurity. 2010. https://www.cisecurity.org/blog/cyber-attack-defense-cis-benchmarks-cdm-mitre-attck/. *Cyber-Attack Defense: CIS Benchmarks + CDM + MITRE ATT&CK.* [En línea] 5 de octubre de 2010. https://www.cisecurity.org/blog/cyber-attack-defense-cis-benchmarks-cdm-mitre-attck/.

CROSSWALLER. 2019. ¿Qué es una auditoría de caja negra, caja blanca y caja gris? [En línea] 1 de Mayo de 2019. http://crosswaller.com/2019/05/01/tipos-de-auditorias-de-seguridad/.

cuckoo. 2021. cuckoosandbox. *https://cuckoosandbox.org/.* [En línea] 2 de 8 de 2021. https://cuckoosandbox.org/.

CVE DETAILS. 2005. CVE DETAILS. [En línea] 20 de Octubre de 2005. https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-1999-0651.

ESIC. 2018. Red team: qué es, estrategias y ejemplo de un caso real. [En línea] Febrero de 2018. https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque.

incibe. 2015. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemasPandaSecurity. *https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemasPandaSecurity.* [En línea] 5 de febrero de 2015. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemasPandaSecurity..

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

IT DIGITAL SECURITY. 2018. ¿Qué es un Blue Team y cómo trabaja? [En línea] Mayo de 2018. https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja.

KASPERSKY. 2013. ¿Qué es una APT? [En línea] 11 de Junio de 2013. https://latam.kaspersky.com/blog/que-es-apt/761/#:~:text=11%20Jun%202013-,APT%20significa%20%E2%80%9CAdvance%20Persistent%20Threat%E2%80%9D%2.

LARA, JUAN RODRIGUEZ. 1.4.1.1 Amenazas internas y externas. [En línea] https://sites.google.com/site/maestrojuanrodriguezlara/topicos-selectos/1-4-1-la-propagacion-del-lado-obscuro/1-4-1-1-amenazas-internas-y-externas.

MALWAREBYTES. Suplantación de identidad (phishing). [En línea] https://es.malwarebytes.com/phishing/.

MARTINEZ, ERNESTO. 2018. Las diferentes amenazas de seguridad informática. [En línea] 2018. https://sites.google.com/site/lasamenazaslainformatica/.

misp-project. 2021. https://www.misp-project.org/galaxy.html. *misp.* [En línea] 5 de 11 de 2021. https://www.misp-project.org/galaxy.html.

NAMP. Nmap. [En línea] https://nmap.org/.

Nmap ORG. 1997. [En línea] 1997. [Citado el: 5 de Julio de 2020.] https://nmap.org/.

OpenVas. 2006. *OpenVAS - Open Vulnerability Assessment Scanner.* [En línea] 2006. [Citado el: 5 de Julio de 2020.] https://www.openvas.org/.
OPENVAS. OpenVAS - Open Vulnerability Assessment Scanner. [En línea] https://www.openvas.org/.

OPTICAL NETWORKS. 2020. ¿Qué es un WAF? – Web Application Firewall. [En línea] 7 de Febrero de 2020. https://www.optical.pe/blog/que-es-un-waf/.

OSI. 2018. ¿Qué son los ataques DoS y DDoS? [En línea] 21 de Agosto de 2018. https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos.

OWASP, Incibe. 2014. OWASP Testing . *https://www.incibe-cert.es/blog/owasp-4.* [En línea] 15 de 10 de 2014. https://www.incibe-cert.es/blog/owasp-4.

Pablo Arellano, Pablo Hasbún, M. Idalia Sepúlveda, Andrés Ferre, Antonia Léniz, Diego Domínguez, Osvaldo Llanos, Nicolette Van Sint Jan, Leonardo Soto, Ximena Miranda, Nicolás Montecinos, Sergio Betancourt, Andrea Peña, Bárbara de la Cortina, Natalia Seguel, Inés Barbagelata, Tomas Regueira,IMPLEMENTACIÓN DE SISTEMA DE COMANDO DE INCIDENTES PARA ENFRENTAR PANDEMIA SARS-COV-2 EN CLÍNICA LAS CONDES, CHILE,https://www.sciencedirect.com/science/article/pii/S071686402030095X

pandasecurity. 2018. https://www.pandasecurity.com/es/mediacenter/seguridad/pentesting-herramienta-empresa/. *Pentesting: una herramienta muy valiosa para tu empresa.* [En línea] 26 de february de 2018. https://www.pandasecurity.com/es/mediacenter/seguridad/pentesting-herramienta-empresa/.

RAUL, HENRY. 2017. Metodología de Pruebas de Intrusión en la NIST SP 800-115. [En línea] 10 de Mayo de 2017. https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/.

REDZONE. 2014. Burp Suite se actualiza a la versión 1.6 con múltiples mejoras. [En línea] 16 de Abril de 2014. https://www.redeszone.net/2014/04/16/burp-suite-se-actualiza-la-version-1-6-con-multiples-mejoras/.

research, internetof things. 2009. http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf. *internet-of-things-research.eu.* [En línea] 15 de september de 2009. http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf.

REYDES. 2018. Escanear un Servidor Web utilizando Nikto. [En línea] 30 de Agosto de 2018. http://www.reydes.com/d/?q=Escanear_un_Servidor_Web_utilizando_Nikto.

TAMAYO, SEBASTIAN. 2020. Riesgo, Amenazas y Vulnerabilidad conceptos claves de un ataque informático. [En línea] 2020. https://globalimf.com.ec/openuide/blog/gestion-de-riesgos-informaticos/.

Tenable. *Tenable.* [En línea] [Citado el: 5 de Julio de 2020.] https://es-la.tenable.com/products/nessus.

TO, SIX TECHNOLOGIES WITH POTENTIAL IMPACTS ON US INTERESTS OUT. 2008. globaltrends.thedialogue.org. [En línea] 2008. http://globaltrends.thedialogue.org/publication/disruptive-civil-technologies-six-technologies-with-potential-impacts-on-us-interests-out-to-2025/.

welivesecurit. 2018. https://www.welivesecurity.com/la-es/infographics/estado-seguridad-pymes-latinoamerica/. *www.welivesecurity.com.* [En línea] 15 de 8 de 2018. https://www.welivesecurity.com/la-es/infographics/estado-seguridad-pymes-latinoamerica/.

welivesecurity. 2017. https://www.welivesecurity.com/la-es/2017/10/06/trucos-mitos-virustotal/. *5 Trucos y 7 mitos sobre el uso de VirusTotal que quizá no conocías.* [En línea] 6 de octubre de 2017. https://www.welivesecurity.com/la-es/2017/10/06/trucos-mitos-virustotal/.

welivesecurity. (24-/05/2010). Defensa en profundidad: qué es. https://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/

wired. 2016. https://www.wired.com/2016/08/security-bots-show-hacking-isnt-just-humans/. *Hackers Don't Have to Be Human Anymore. This Bot Battle Proves It.* [En línea] 8 de 5 de 2016. https://www.wired.com/2016/08/security-bots-show-hacking-isnt-just-humans/.

WireShark Org. 2020. *WireShark.* [En línea] 5 de Julio de 2020. https://www.wireshark.org/.