CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS DE BLUE TEAM Y RED TEAM

EDGAR GALVÁN RAMOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2022

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS DE BLUE TEAM Y RED TEAM

EDGAR GALVÁN RAMOS

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
Luis Fernando Zambrano Hernandez
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2022

CONTENIDO

LISTA DE ILUSTRACIONES

GLOSARIO

BLUE TEAM: El equipo azul, responsable de hacer balance regular de los sistemas de TI utilizados en una empresa. Además, se deben identificar las debilidades y verificar la eficacia de las herramientas de seguridad utilizadas para proteger el entorno de TI. Por lo general, proviene del personal interno.[1]

CSIRT: es un equipo de reacción los ataques presentados de Seguridad Informática[2]

CVE: base publica con el historial de los ataques presentados y su forma de atención, de los ataques más conocidos a los que están expuestos los sistemas

EXPLOIT: Un programa de computadora o software utilizado para explotar fallas de seguridad en un sistema o aplicación.

HARDENIZACIÓN: es el conjunto de proteger un sistema reduciendo su vulnerabilidad, esto se logra entre otras cosas, eliminando software, usuarios, servicios, etc.

MARCO DE CIBERSEGURIDAD: son un grupo de pautas y mejores practicas que las diferentes organizaciones hacen uso para asegurar su infraestructura para evitar los diferentes ataques a los cuales, se está expuesto. Estos estándares facilitan la comunicación interna y externa de intercambio de información.[3]

METASPLOIT: es una herramienta que permite recopilar información en las pruebas de penetración y su explotación.[4]

METERPRETER: es un payload que permite conectarse a otra maquina y ejecutar tareas a un nivel muy bajo que es compleja su detección.[5]

---

[1] ComputerWeekly.de (2020), Red Team, Blue Team, purple Team: Wer Kummert Sic hum was? [En Línea] Disponible en: https://www.computerweekly.com/de/tipp/Red-Team-Blue-Team-Purple-Team-Wer-kuemmert-sich-um-was

[2] NIST, Glosario [En Línea] Disponible en: https://csrc.nist.gov/glossary/term/csirt

[3] Ciberseguridad.com(2022) que es el marco de ciberseguridad NIST? [En Línea] Disponible en: https://ciberseguridad.com/herramientas/marco-ciberseguridad-nist/

[4] Treehackme (2022), metasploit [En Línea] Disponible en : https://tryhackme.com/room/metasploitintro

[5] Keepcoding (2020), Que es una vulnerabilidad? [En Línea] Disponible en: https://keepcoding.io/blog/que-es-meterpreter/#Que_es_Meterpreter

PARCHE DE SEGURIDAD: Los parches son un grupo de cambios aplicados al software para mejorar fallas de seguridad en sistemas operativos o programas.[6]

PAYLOAD: Carga útil, Consiste en la información transmitida desde la capa anterior.[7]

READ TEAM: son un grupo de especialistas autorizadas para simular la infraestructura a la que está sujeta una organización ante un eventual ataque.[8]

SIEM: Es una solución de seguridad que ayuda a las organizaciones a reconocer posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de afectar las actividades operativas de la organización.[9]

VULNERABILIDAD EN CIBERSEGURIDAD: es una falencia informática que pone en riesgo al sistema. Puede ser un software malicioso. Para acceder al control de un equipo o hacerle daño.[10]

---

[6] INCIBE(2017), Glosario de términos de ciberseguridad [En Línea] Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

[7] NIST, Glosario [En Línea] Disponible en: https://csrc.nist.gov/glossary/term/payload

[8] NIST, Glosario [En Línea] Disponible en: https://csrc.nist.gov/glossary/term/red_team

[9] IBM (2022), What is SIEM? [En Línea] Disponible en: https://www.ibm.com/topics/siem

[10] Keepcoding (2020), Que es una vulnerabilidad? [En Línea] Disponible en: https://keepcoding.io/blog/que-es-una-vulnerabilidad-en-ciberseguridad/

RESUMEN

El presente documento técnico relaciona los procesos, métodos, herramientas y marcos legales que rigen a los equipos rojos y azules en cualquier organización con una infraestructura de TI. A través de la conceptualización y la práctica virtual, en este documento se aplica la estrategia de PBL (Problem-Based Learning) en tres fases, en las cuales se presenta en la primera fase los temas jurídicos y cuestiones éticas. Estos son los marcos que todos los miembros de un equipo rojo o azul deben implementar para realizar sus tareas diarias de ciberseguridad, para evaluar el alcance que cualquier integrante de estos equipos debe tener en cuenta. La fase dos está estructuradas con un conjunto de estrategias y herramientas en pro de apoyar la implementación y cumplimiento de los procesos de detección de fallos de seguridad TI y plataformas TI, identificando las metodologías de pruebas de penetración a tener en cuenta para la solución de un problema presentado. Por último, en la fase tres consiste en un conjunto de procesos y herramientas encaminadas a la contención de un ataque informático y su posterior corrección, a partir del establecimiento de buenas prácticas de ciberseguridad en la organización y de esta forma proteger la información de las organizaciones.

PALABRAS CLAVES: Hardenización, Proteger**,** Red Team y Blue Team, Riesgo, Vulnerabilidad.

INTRODUCCIÓN

El presente documento se encuentra conformada por los marcos legales y éticos para ser ejecutados por cualquier integrante Red Team o Blue Team en la acción de sus tareas cotidianas de eventos de Ciberseguridad.

Reconocer de un problema su normatividad y el despliegue de su infraestructura, en marcado en las normas éticas y legales, relacionados con La ejecución de las actividades.

Permitir mediante un escenario real, dar respuestas orientadoras a unas problemáticas que describen en la guía de la empresa Hackers Security en temas técnicos que se ejecutan.

Por último, el presente documento, se encuentra conformada por una guía de herramientas y procesos las cuales se orientan a la contención de un ataque informático y a su posterior remediación a partir de la generación de buenas prácticas de Ciberseguridad.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Construir un documento técnico, con el conocimiento de los procesos, metodologías, herramientas y marco legal que rige dentro de los equipos Red Team & Blue Team. Para conocer su funcionalidad dentro de una organización.

1.2 OBJETIVOS ESPECÍFICOS

- Conocer el contexto, legal y ético para ser aplicados por los equipos Red & Blue Team.

- Determinar estrategias y herramientas que sirvan de apoyo para la ejecución y cumplimiento, relacionados con procesos de identificación de fallos de seguridad en plataformas de TI

- Analizar y contener a partir de unos estándares, los cuales se orientan a la contención de un ataque informático y a su posterior remediación por parte de un equipo Blue Team.

2 DESARROLLO DEL INFORME

A continuación, se desarrollan las diferentes fases:

2.1 CONTEXTO ÉTICO, LEGAL RED TEAM & BLUE TEAM

LEY 1273 DEL 2009 DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS

Se adiciona al código penal

Capítulo 1 De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

- El artículo 269A (acceso abusivo a un sistema informático) quien acceda de manera abusiva y sin consentimiento a la información ajena.
- Articulo 269B (obstaculización ilegitima de sistemas informáticos, red de telecomunicaciones) quien impida o afecte un sistema informático o una red
- Articulo 269D (Daño Informático) quien sin estar autorizado deteriore o elimine información de un sistema informático.
- Articulo 269E (Uso de software malicioso) quien sin estar autorizado distribuya software malicioso dañino.
- Articulo 269F (Violación de datos personales) quien sin estar autorizado extraiga y use o comercialice información de datos personales de una base de datos, ficheros.
- Articulo 269G (Suplantación de sitios web para capturar datos personales) quien sin estar facultado legalmente altere un dominio de una página web o suplante un sitio web con el fin de extraer información y comercializarla.

Quien incurra en alguna de los anteriores artículos incurre en una pena de hasta 96 meses de prisión y una multa de hasta 1.000 SMLV.

- Articulo 269C (Interceptación de datos informáticos) quien sin estar autorizado legalmente intercepte datos, incurre en una pena de 36 a 72 meses.
- Articulo 269H (Circunstancias de agravación punitiva) las penas de prisión anteriores se aumentarán de la mitad a las tres cuartas partes si se causara sobre redes o sistemas informáticos estatales u oficiales, sector financiero nacional o internacional. O por un empleado público, aprovechando la confianza depositada, deja ver la información afectando a la persona, comercializando la información o con fines terroristas.

Capítulo 2 De los atentados informáticos y otras infracciones

- Articulo 269I (Hurto por medios informáticos y semejantes) quien viole medidas de seguridad y manipule un sistema informático o una red de sistema electrónico o un usuario autenticado incurre en una pena de 32 a 108 meses o hasta 48 meses si la cuantía es menos de 4SMLV y cuando sea mayor a esta cuantía será de 48 a 108 meses de prisión.
- Articulo 269J (Transferencia no consentida de activos) quien incurra a través de una manipulación informática consiga la transferencia sin permiso de un activo de un tercero con fin lucrativo incurre en una pena de 48 a 120 meses de prisión y una multa de 200 a 1.500 SMLV.

LEY ESTATUTARIA DE 1581 DE 2012

Titulo 1 objeto, ámbito de aplicación y definiciones

Articulo 1 OBJETO. Toda persona tiene derecho a conocer, rectificar y actualizar la información que se haya almacenado sobre ellos en las bases de datos o archivos. De igual forma tiene derecho al habeas data, con la potestad de rectificar, incluir o excluir de una base de datos o archivos

Articulo 2 Ámbito de aplicación. Esta ley aplica al tratamiento de datos personales a nivel nacional e internacional por entidades de naturaleza privada o pública, según la normas y tratados de la legislación colombiana.

- Articulo 3 Definiciones. Para efectos de esta ley se entiende por:
- Autorización: consentimiento para el tratamiento de datos personales para el tratamiento de datos personales.
- Base de datos: almacenamiento de datos de forma organizada
- Dato personal: cualquier información de una o varias personas.
- Encargado de tratamiento: cualquier persona que realice el tratamiento de los datos personales.
- Responsable del Tratamiento: persona natural o jurídica que decida sobre el tratamiento de datos.
- Titular: persona natural objeto del tratamiento de datos.
- Tratamiento: cualquier operación que se realice sobre el tratamiento de datos como almacenar, uso circulación o supresión.

ETAPAS DEL PENTESTING

son pruebas de intrusión que se ejecutan sobre un sistema, red o en una infraestructura de red para conocer sus vulnerabilidades. Dentro de los tipos de pentesting están divididas en:

Caja negra: no se tiene conocimiento sobre el sistema que se va a analizar.

Caja gris: se tiene un conocimiento limitado del sistema a analizar

Caja blanca: se tiene conocimiento sobre las diferentes conexiones y sistemas del objetivo

Etapas del pentesting y la herramienta que interviene en cada una de ellas:

RECOPILACIÓN DE INFORMACIÓN / ENUMERACIÓN

Corresponde a la fase principal del pentest y se trata de recolectar toda la información posible como Escaneo de dominios, IPs, puertos, versiones, servicios, firewalls y otras conexiones.

ANÁLISIS DE VULNERABILIDADES

se realizan todas las acciones que permitan encontrar las diferentes falencias o debilidades que tiene nuestro objetivo, los usuarios y su información.

Encontrar configuraciones deficientes, poca protección en los datos sensibles o una mala administración de cuentas y contraseñas. De igual forma el análisis de los diferentes activos e infraestructura y estaciones de trabajo, dispositivos móviles, páginas web que pueden ser vulnerables a un ataque.

Dentro de las herramientas mas usadas se encuentra NESSUS.

EXPLOTACIÓN DE VULNERABILIDADES

se trata de aprovechar la información obtenida en la validación de vulnerabilidades y con base en esto ejecutar diferentes exploits y hacer uso de las credenciales y puertas abiertas encontradas para ingresar a los diferentes equipos que se tiene como objetivo.

Una de las herramientas más usada se encuentra OpenVas

POST EXPLOTACIÓN

Esta fase no es tan usada y consiste en una vez ingresado al sistema intenta obtener más privilegios que permitan obtener información confidencial y realizar acciones sin o con el consentimiento del sistema objetivo.

La herramienta más usada Empire.

REPORTE

Finalmente, se entrega el reporte de las vulnerabilidades encontradas junto con la contraparte para poder solucionarlas.

Una de la herramienta más usada es Dradis.

Definir y explicar las herramientas Metasploit, Nmap, OpenVast, ExploitDB y CVE.

• **Metasploit:**

Marco de código (abierto), utilizado por profesionales en seguridad y ciberdelincuentes para hallar, aprovechar y validar vulnerabilidades.

Metasploit Framework es un marco que tiene varias herramientas de explotación y varias herramientas de prueba de penetración.

• **Nmap:**

se utiliza especialmente para saber que dispositivos se están ejecutando, cuales hosts (servidores, conmutadores y enrutadores), están disponibles y que servicios tienen, así como detectar riesgos de seguridad y encontrar puertos abiertos. La información obtenida es con base en los comandos que se hayan ejecutados.

• **OpenVas:**

Es un framework de uso libre que sirve para escanear vulnerabilidades con todos sus servicios y herramienta, de forma individual o grupal con otras herramientas de seguridad.

Servicios en línea:

• **ExploitDB:**

ExploitDB pertenece a los sitios web públicos relevantes, que aporta una gigantesca proporción de vulnerabilidades a la base de datos oficial de CVE. Para contribuir a documentar la Base publica de CVE. Un gran porcentaje de estas vulnerabilidades tiene riesgo de seguridad altos o críticos. para las publicaciones de ExploitDB, se proponen sustraer 9 puntos clave de vulnerabilidad (producto/versión/componente vulnerable, tipo de vulnerabilidad, abastecedor, tipo de agresor, causa raíz, vector de ataque e impacto) de la referencia descriptiva.

• **CVE:**

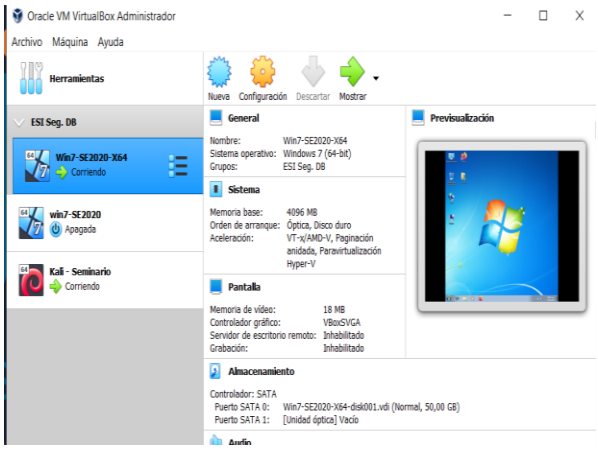
(vulnerabilidades y exposiciones comunes) es un estándar que identifica las falencias y peligros de seguridad en los sistemas informáticos, enumerándolos en un directorio de acceso general. La finalidad es simplificar el trueque de datos acerca de vulnerabilidades, ejemplificando, entre diferentes elaboradores, y permitir una identificación clara. Los sistemas IPS o IDS tienen la posibilidad de usar el directorio CVE en su administración de vulnerabilidades.

Analizar y configurar el “banco de trabajo”.

A continuación, se despliegan las siguientes maquinas en la MV VirtualBox:

- windows 7 X64
- windows 7 X86
- Kali Linux

Ilustración 1 instalación máquinas Virtuales

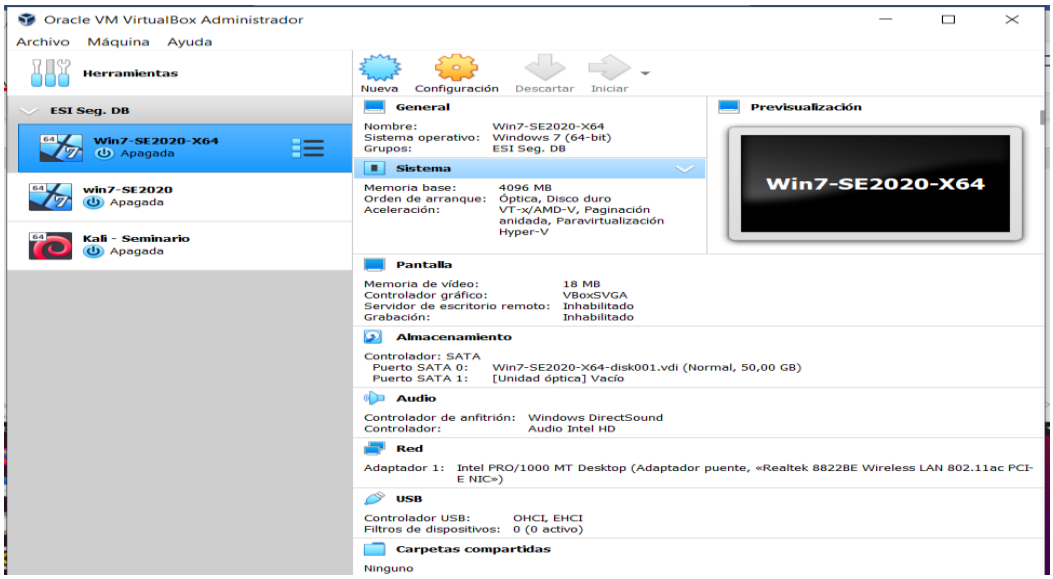


Fuente: propia

A continuación, se despliegan las características técnicas de cada maquina

WINDOWS 7 X 64

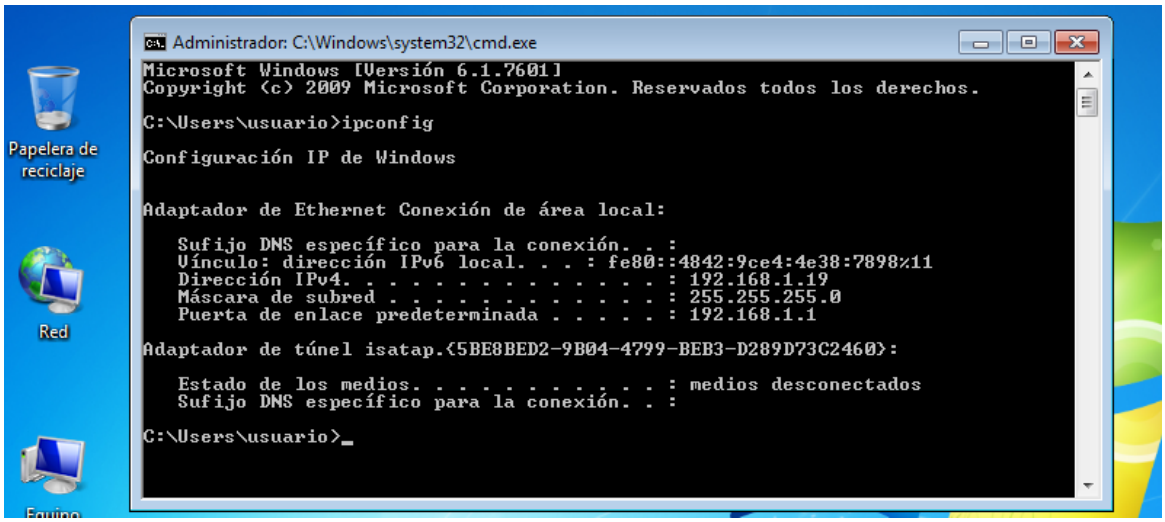
Ilustración 2 Windows7 x64



Fuente: propia

IP: 192.168.1.19

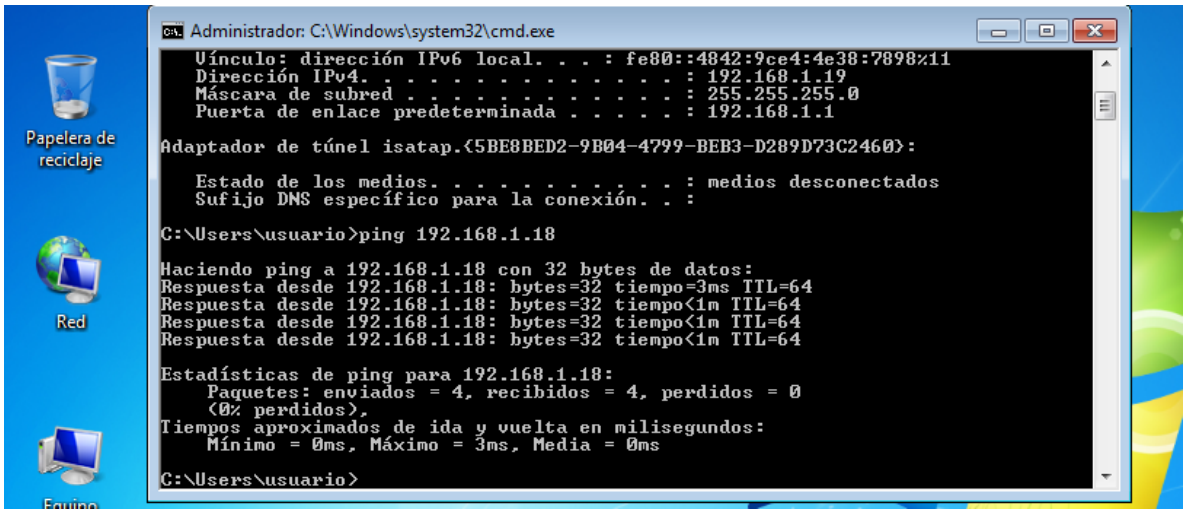
Ilustración 3 IP Windows 7 x64



Fuente: propia

A continuación, se realiza ping desde Windows 7 x64 a la IP de la maquina Kali Linux 192.168.1.18

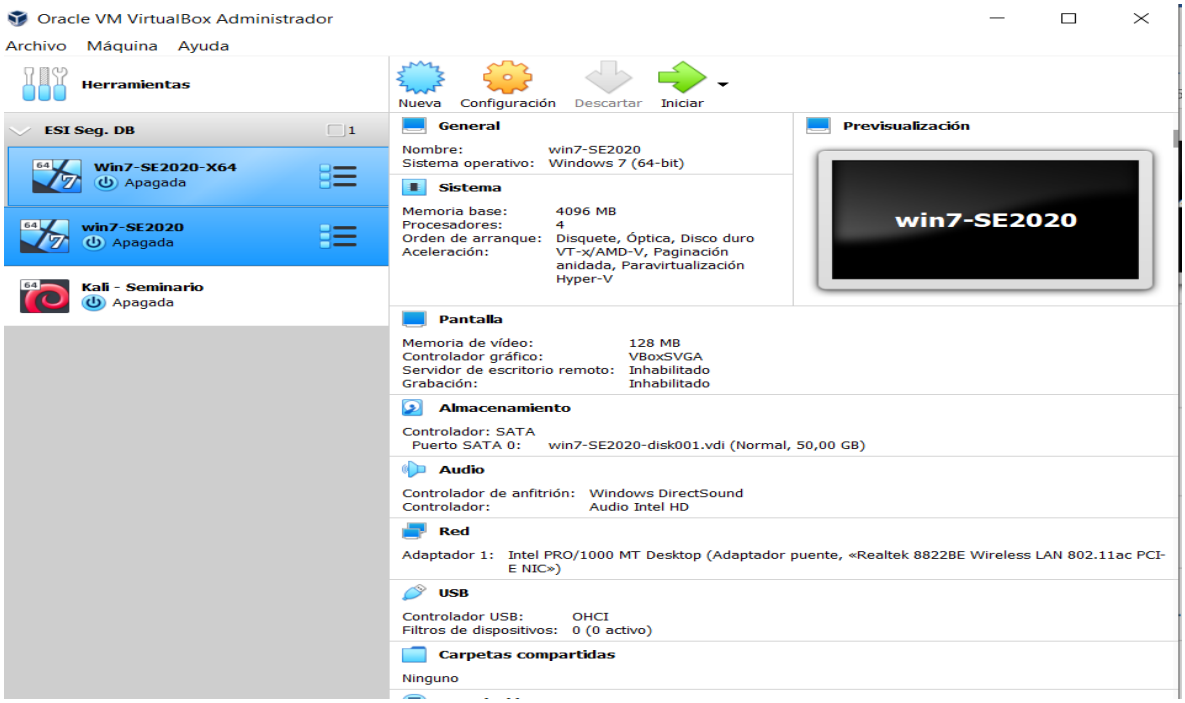
Ilustración 4 Ping desde windows 7 x64



Fuente: propia

WINDOWS 7 X 86

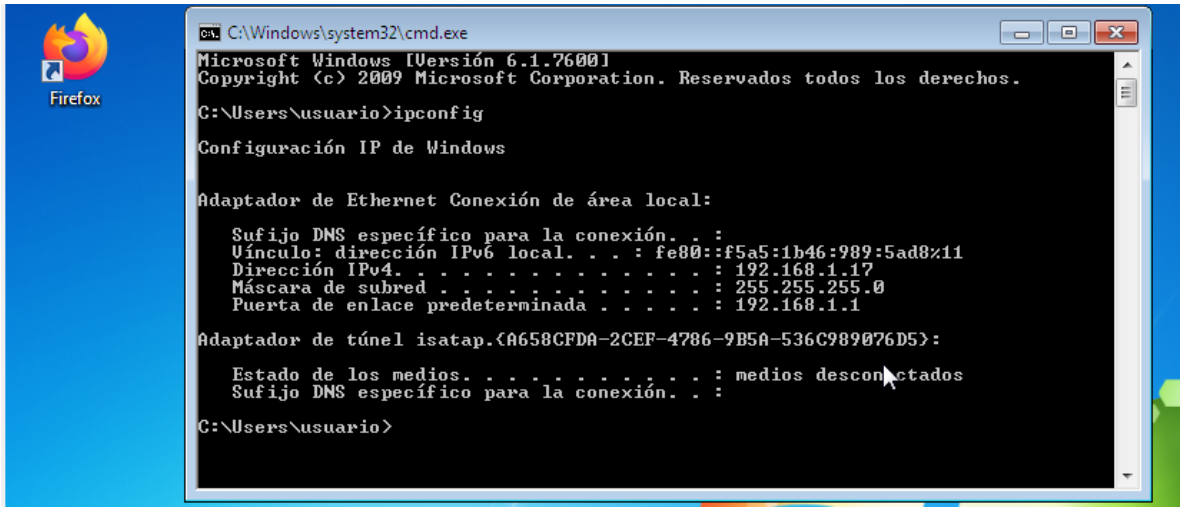
Ilustración 5 Windows 7 x86



Fuente: propia

IP: 192.168.1.19

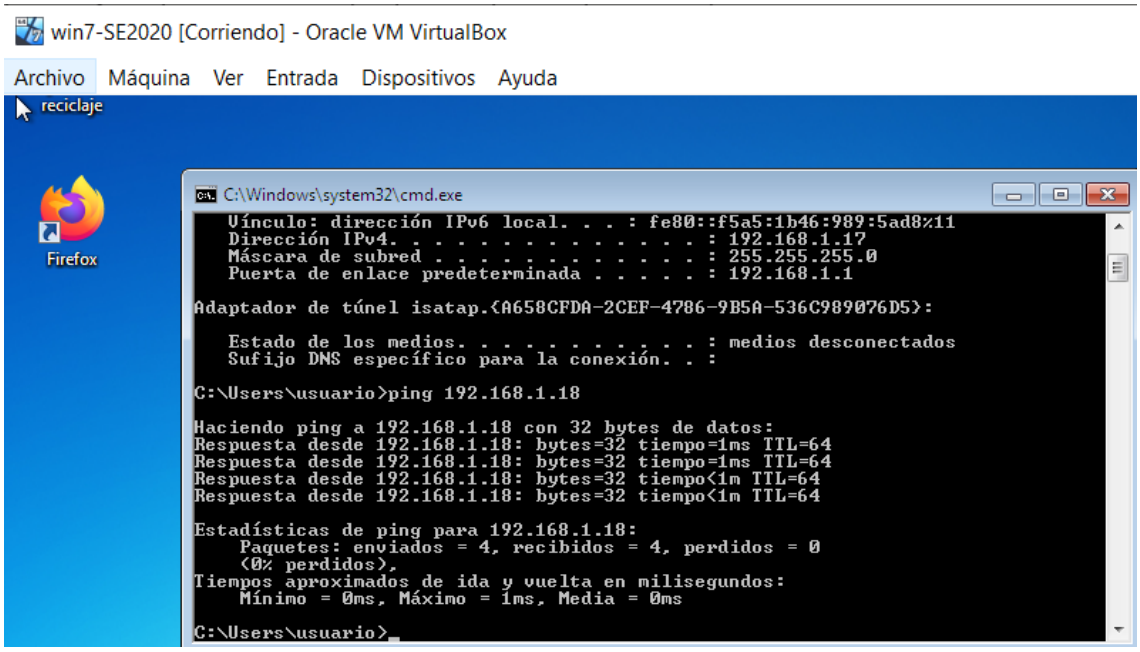
Ilustración 6 IP Windows 7 SE2020



Fuente: propia

A continuación, se realiza ping desde Windows 7 SE2020 a la IP de la maquina Kali 192.168.1.18

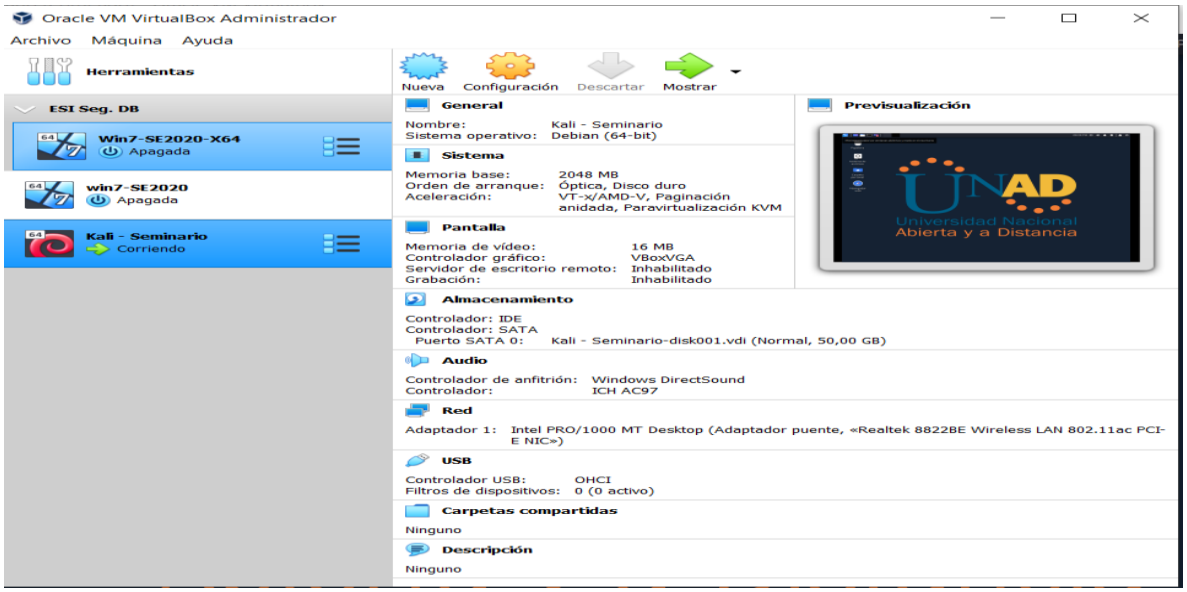
Ilustración 7 Ping desde Windows 7 SE2020 a Kali



Fuente: propia

KALI LINUX

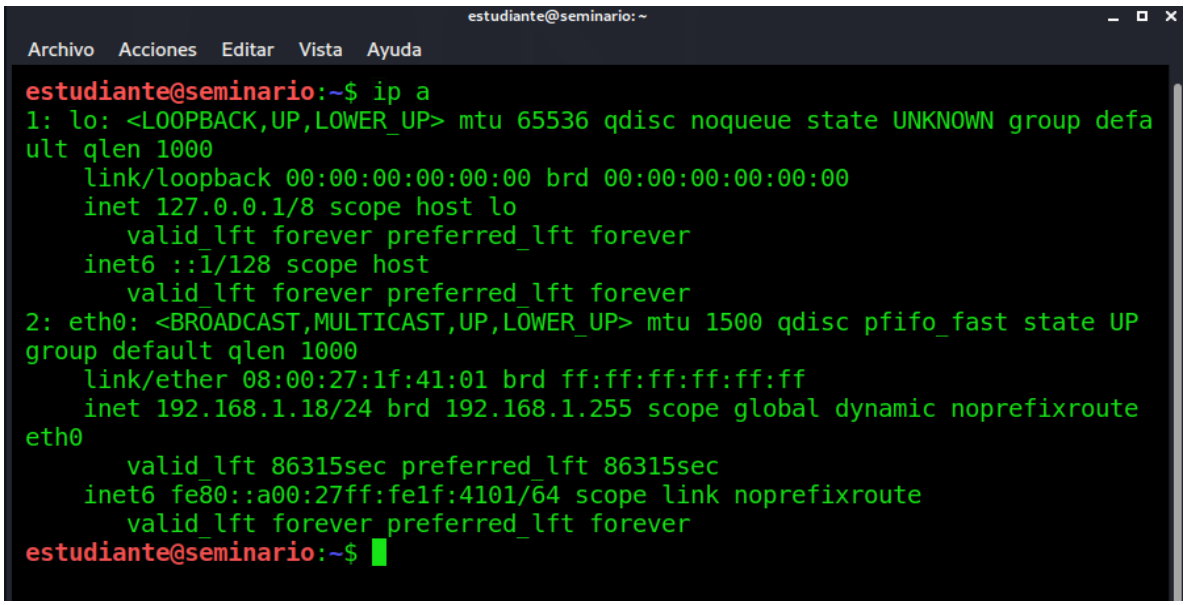
Ilustración 8 Kali Linux



Fuente: propia

IP Kali Linux: 192.168.1.18

Ilustración 9 IP Kali Linux



Fuente: propia

A continuación, se desarrollan las diferentes actividades de análisis y evaluación enmarcados en la normatividad relacionada con el ejercicio de los Red Team & Blue Team.

2.2 PASOS Y PROCESOS RED TEAM

INFORME DE HERRAMIENTAS Y PROCEDIMIENTOS UTILIZADOS PARA DAR SOLUCIÓN AL ESCENARIO DE RED TEAM DE ACUERDO CON LOS PASOS DEL PENTESTING

A continuación, se describen las herramientas a utilizar en cada fase:

Ilustración 10 Fases del pentesting

FASES DEL PENTESTING	DESCRIPCIÓN	HERRAMIENTA
Recopilación de la información	Se trata de recolectar toda la información posible de la maquina objetivo, como Ips, puertos, versiones, servicios, etc.	La herramienta para usar en esta fase es NMAP
Análisis de Vulnerabilidades	Se realizan todas las acciones para encontrar las falencias o debilidades que tienen los equipos objetivo	La herramienta para utilizar en esta fase es NMAP.
Explotación de Vulnerabilidades	De acuerdo con la información obtenida en la fase anterior se ejecutan diferentes exploits para aprovechar las diferentes vulnerabilidades	La Herramienta para usar es Metaexploit
Post Explotación	En esta fase se ingresa al equipo objetivo y se obtienen privilegios que permitan obtener información confidencial	La Herramienta para usar es Metaexploit

Fuente: propia

INFORME CON ANÁLISIS DEL CASO DE RED TEAM, QUE PERMITIÓ DAR SOLUCIÓN AL FALLO IDENTIFICADO.

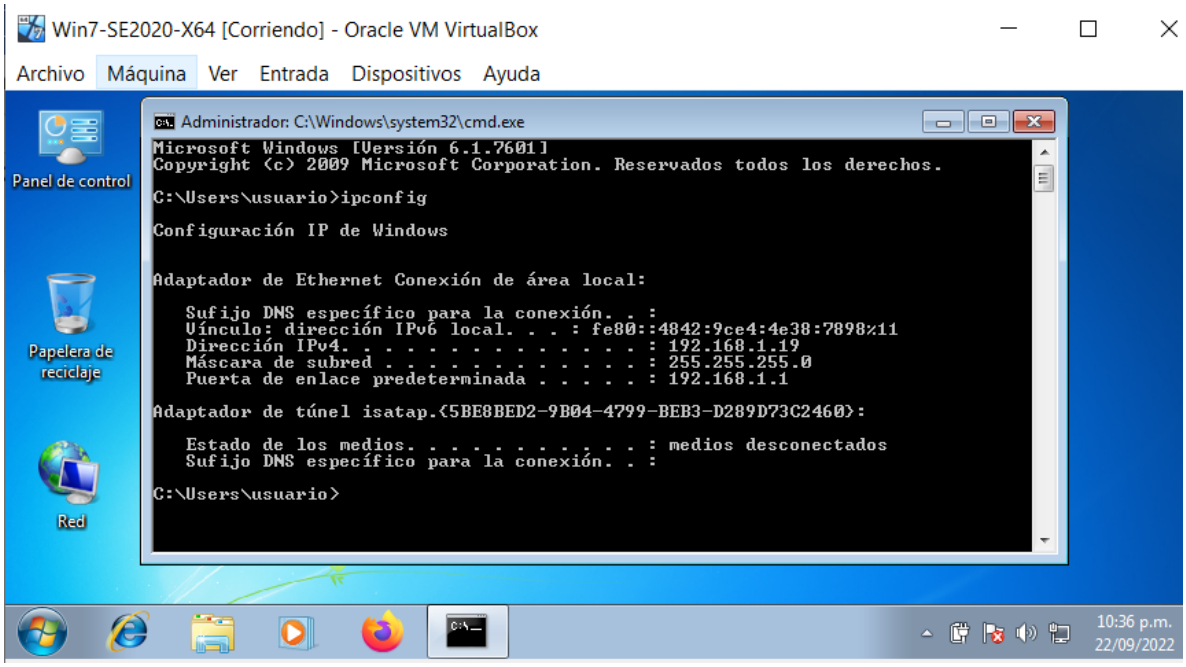
se analizará con Kali Linux las vulnerabilidades que se encuentran con cada una de las maquinas con la herramienta nmap:

NMAP

- **maquina Windows7 x64**

IP: 192.168.1.19

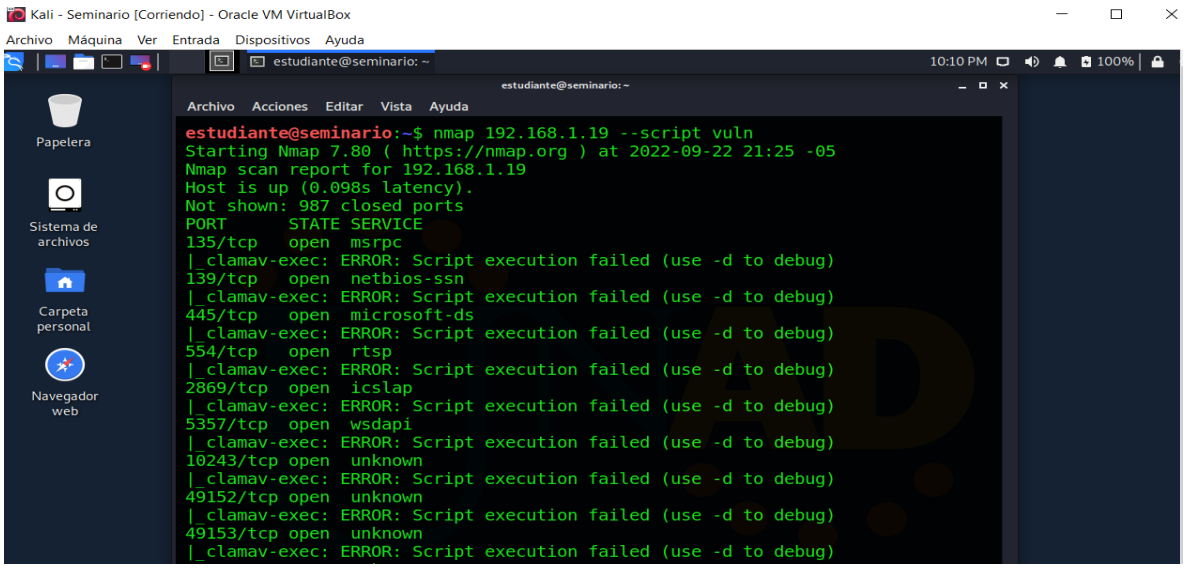
Ilustración 11 IP Windows 7 x64



Fuente: propia

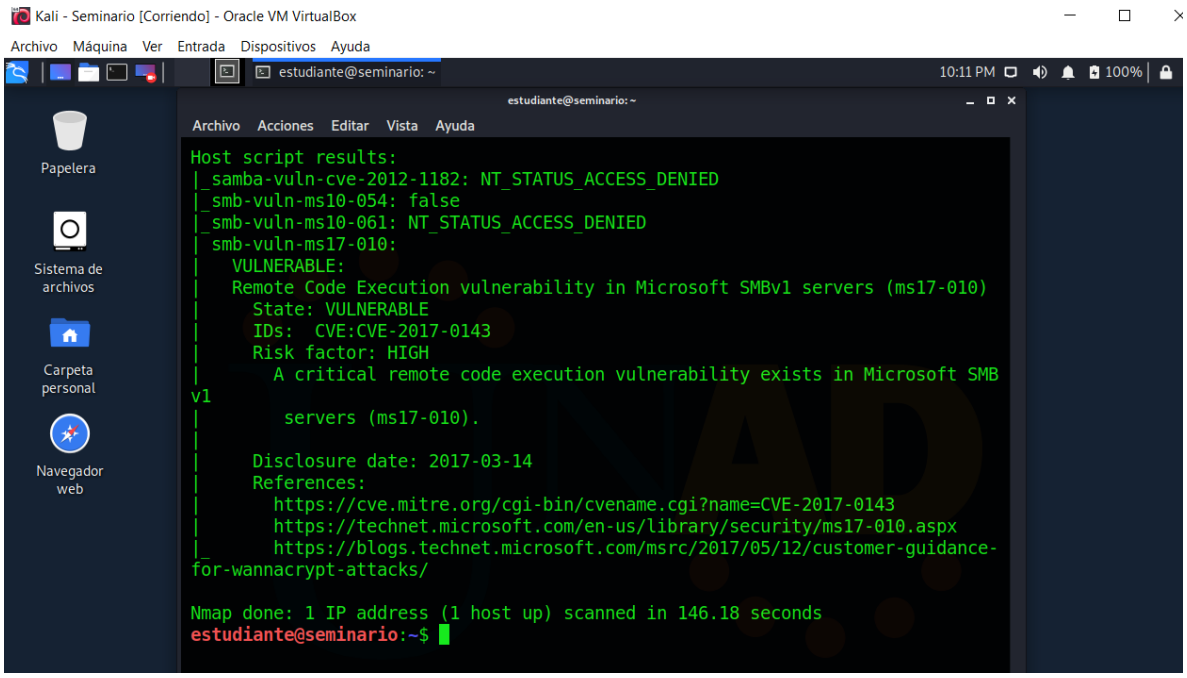
Se digita el comando nmap 192.168.1.19 –script vuln y se realiza análisis de vulnerabilidades desde Kali Linux

Ilustración 12 análisis vulnerabilidades Windows7 x64



Fuente: propia

Ilustración 13 escaneo vulnerabilidades Windows7 x64



Fuente: propia

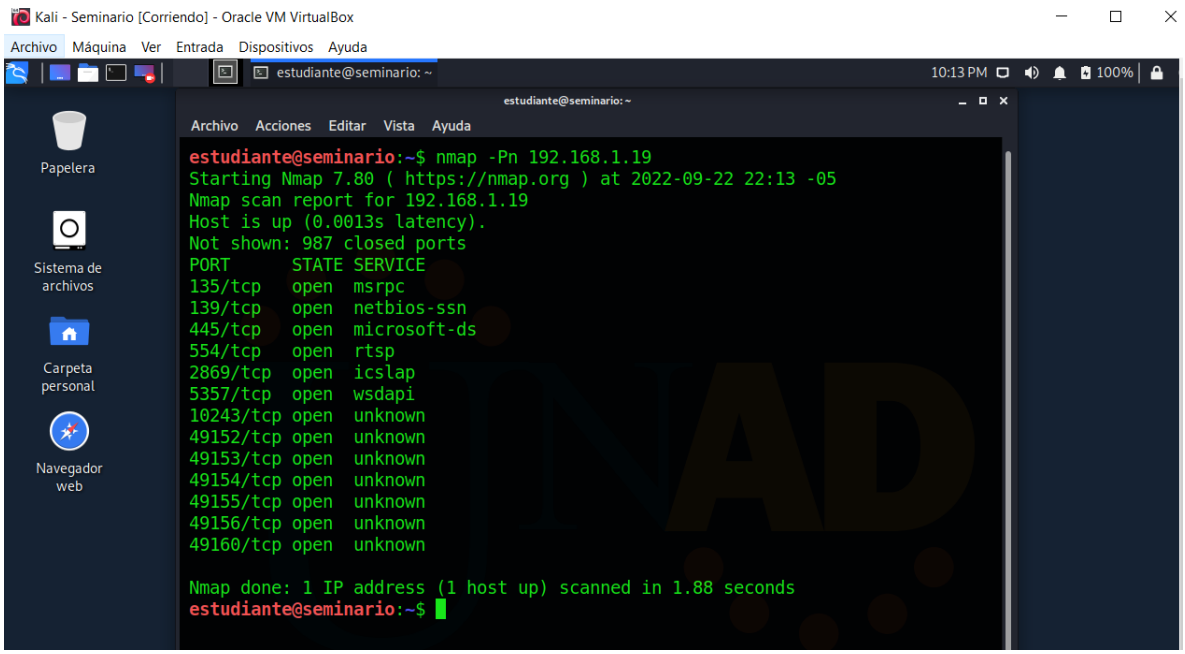
El Escaneo permite visualizar las siguientes vulnerabilidades:

CVE-2012-1182: El generador de código RPC en samba 3.x, anterior a las versiones 3.4,16, 3.5,14,3.6. No implementa una validación en una longitud de una matriz, lo que permite a los atacantes remotos ejecutar una llamada arbitraria.

CVE-2017-0143: El protocolo de red de capa de aplicación comúnmente utilizado en Microsoft Windows para proporcionar acceso compartido a archivos e impresoras. SMBv1, permite a los atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, también conocido como “vulnerabilidad de ejecución remota de código SMB de Windows”.[11]

Se digita el comando nmap 192.168.1.19, para conocer los puertos abiertos

Ilustración 14 Puertos abiertos Windows7 x64



Fuente: propia

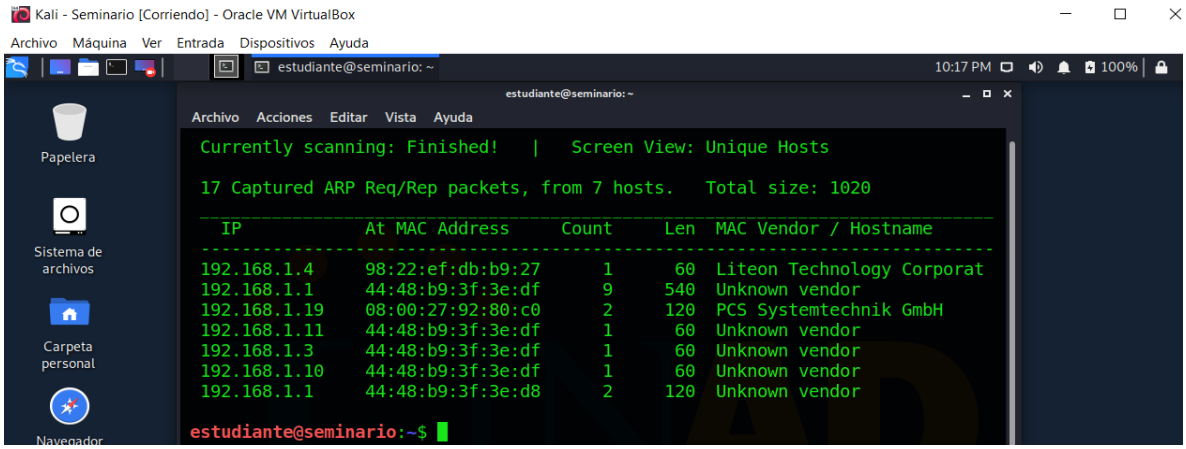
Al realizar el escaneo de puertos permite visualizar los puertos abiertos que tiene la máquina.

[11] CVE. (2022) CVE-2017-1182 [En Línea]Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Finalizando el análisis se digita el siguiente comando para visualizar las Ips activas

sudo netdiscover -r 192.168.1.0/24. Dentro de la cual se visualiza la IP 192.168.1.19 de windows7 x64

Ilustración 15 IPs Activas desde Kali Linux – Windows7 x64

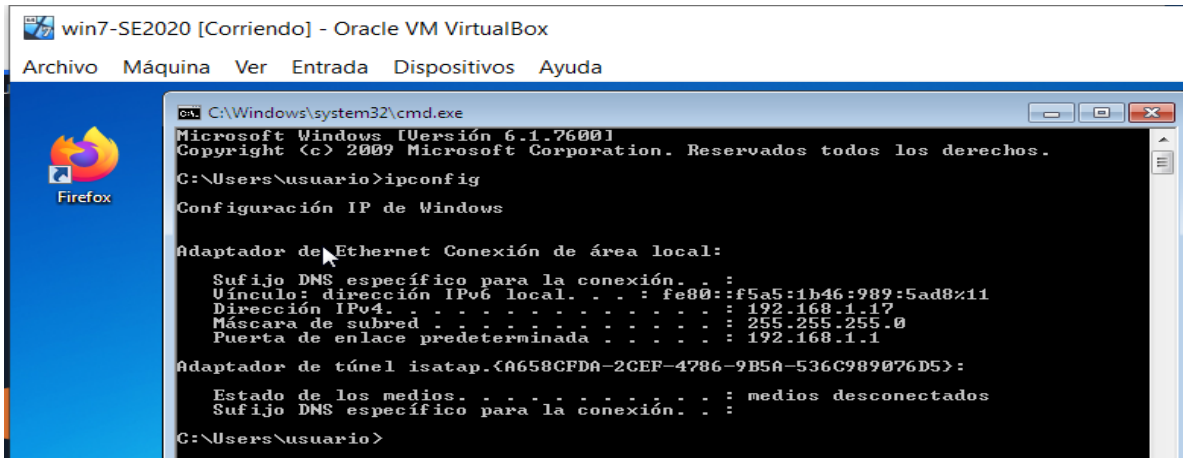


Fuente: propia

- **Windows 7 x86**

IP: 192.168.1.17

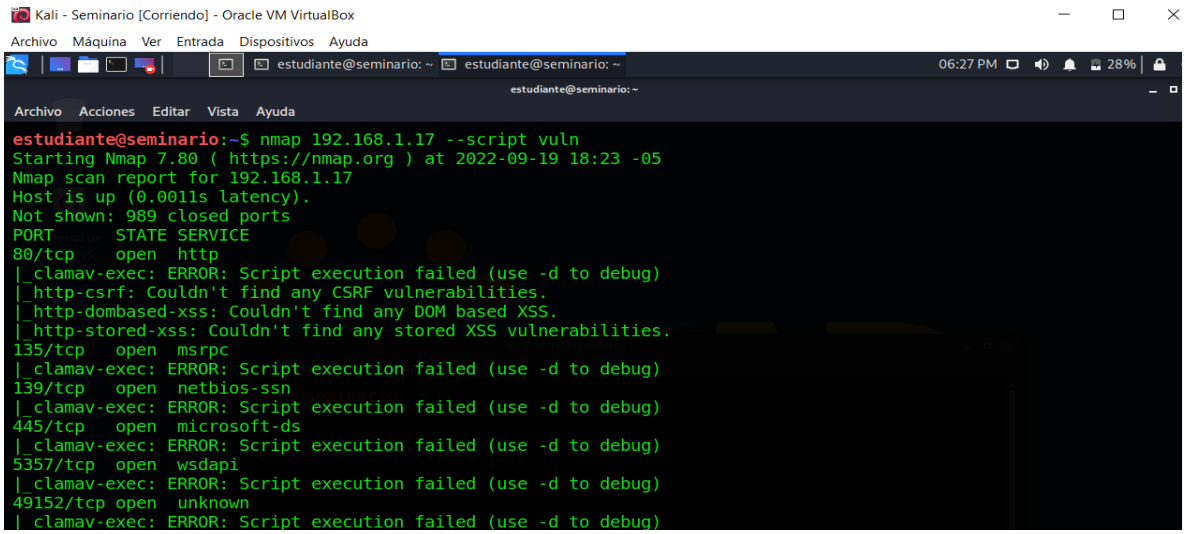
Ilustración 16 IP Windows7 x86



Fuente: propia

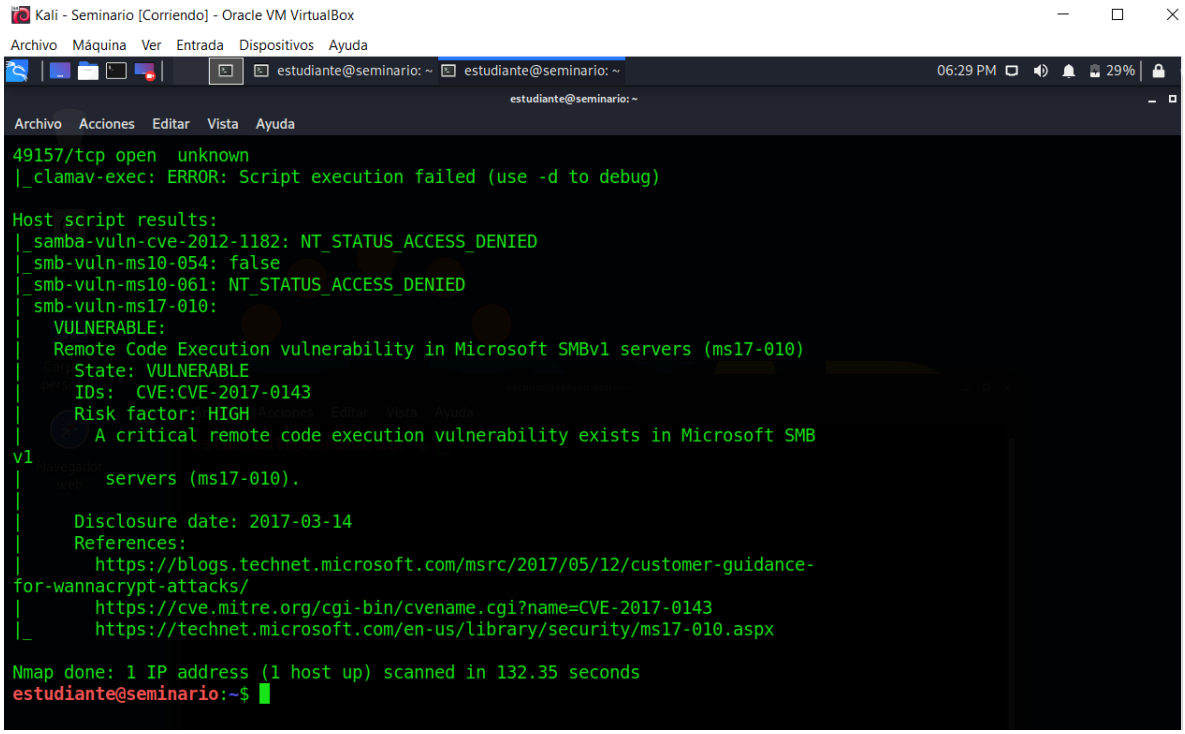
análisis desde Kali linux

Ilustración 17 Analisis Vulnerabilidades Windows7 x86



Fuente: propia

Ilustración 18 escaneo vulnerabilidades Windows7 x86



Fuente: propia

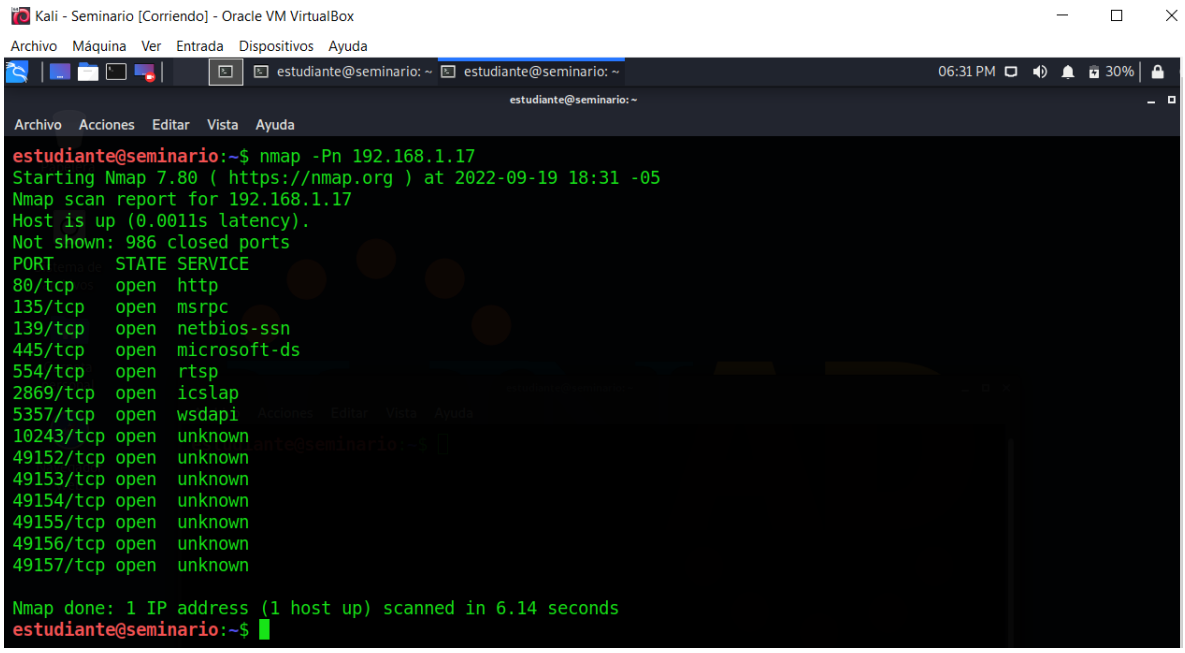
El Escaneo permite visualizar las siguientes vulnerabilidades:

CVE-2012-1182: El generador de código RPC en samba 3.x, anterior a las versiones 3.4,16, 3.5,14,3.6. No implementa una validación en una longitud de una matriz, lo que permite a los atacantes remotos ejecutar una llamada arbitraria.

CVE-2017-0143: El protocolo de red de capa de aplicación comúnmente utilizado en Microsoft Windows para proporcionar acceso compartido a archivos e impresoras. SMBv1, permitiendo la ejecución de código malicioso por medio de paquetes manipulados, conocido como “vulnerabilidad de ejecución remota de código SMB de windows”.[12]

De igual forma se realiza el análisis de los puertos abiertos los cuales se visualizan en la siguiente ilustración.

Ilustración 19 Puertos abiertos Windows7 x86



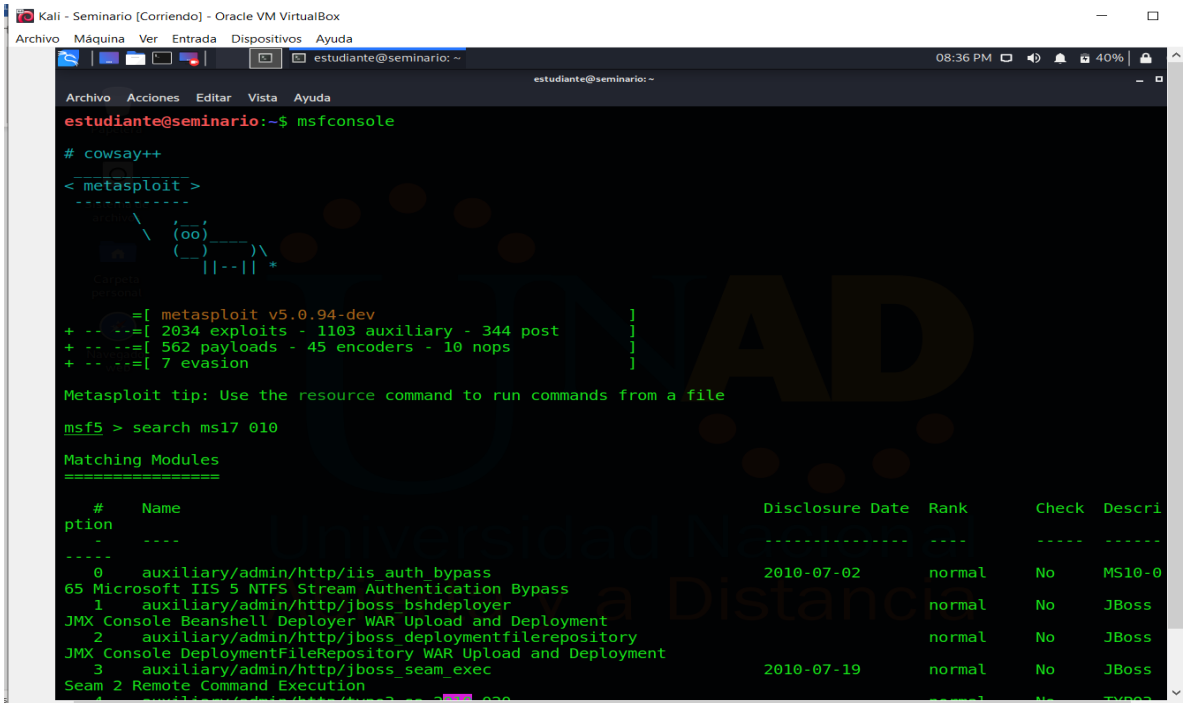
Fuente: propia

[12] CVE. (2022) CVE-2017-1182 [En Línea]Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

ANALISIS DE VULNERABILIDADES EN EL BANCO DE TRABAJO.

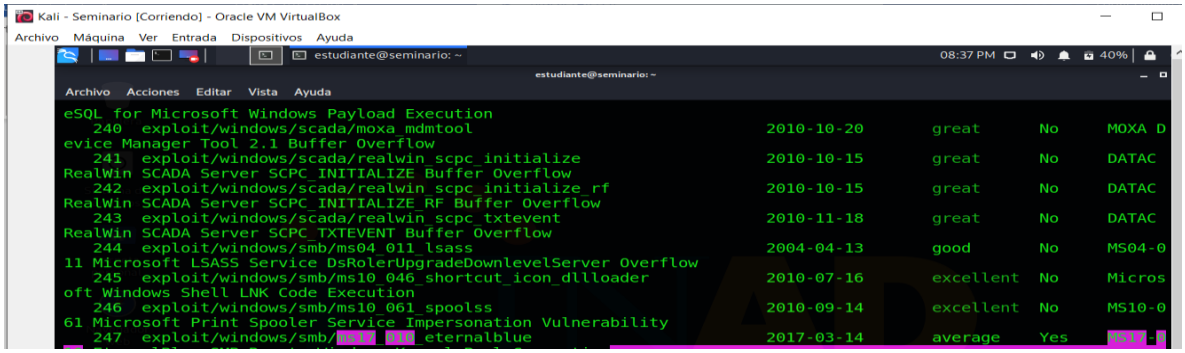
En esta fase se hará uso de la herramienta metaexploit para aprovechar y ejecutar las vulnerabilidades ms17-010 y poder ingresar a los equipos objetivos.
A continuación, se realiza la búsqueda del exploit ms17010

Ilustración 20 Búsqueda del exploit ms17-010



Fuente: propia

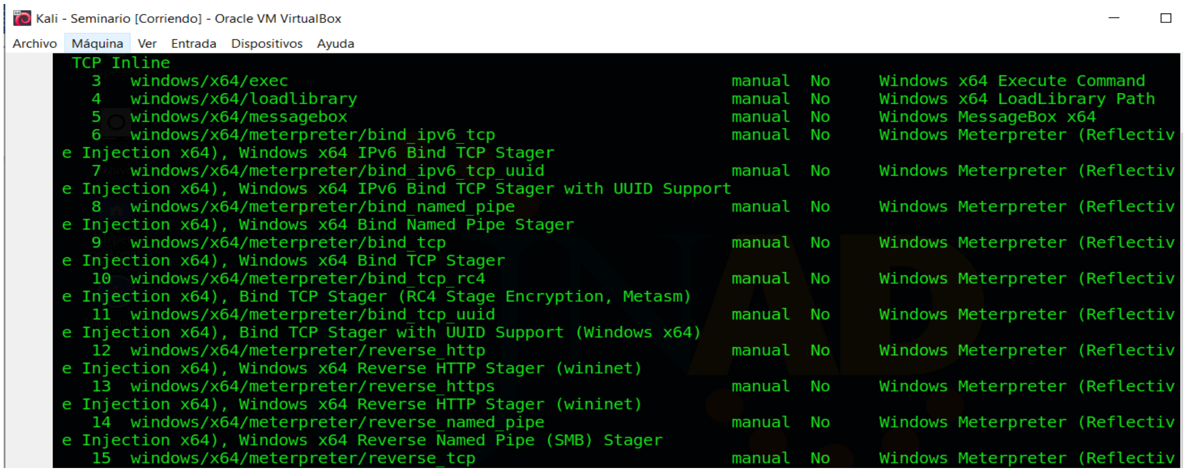
Ilustración 21 exploit eternalblue



Fuente: propia

En las vulnerabilidades encontradas se visualiza el exploit “Eternalblue” o “pantalla azul” y los payloads disponibles para este exploit el cual se ejecutará con “Windows/x64/meterpreter/reverse_tcp”

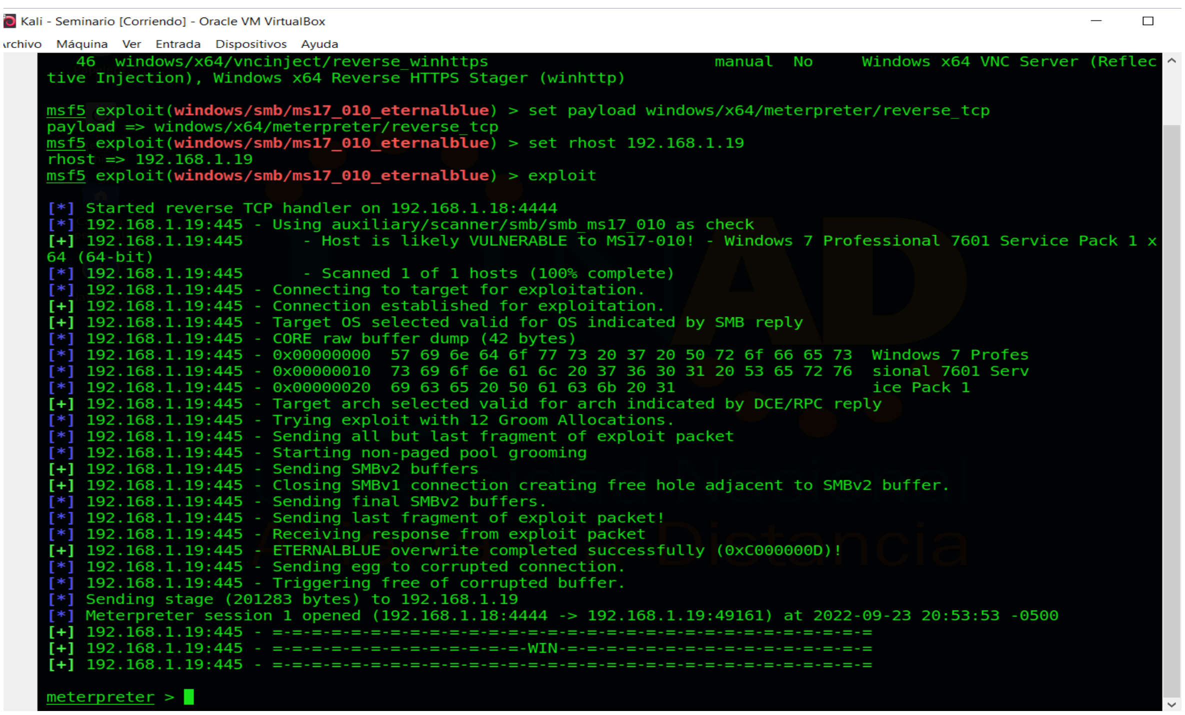
Ilustración 22 Payloads disponibles exploit eternalblue



Fuente: propia

A continuación, se digita la ip del **equipo objetivo Windows7 x64**

Ilustración 23 Explotación de la vulnerabilidad Windows7 x64



Fuente: propia

La explotación es exitosa y se establece sesión en el meterpreter para buscar en los directorios de la maquina objetivo el archivo solicitado **"winse20w0.exe".**

Ilustración 24 Ubicación archivo "winse2ow0.exe" Windows7 x64

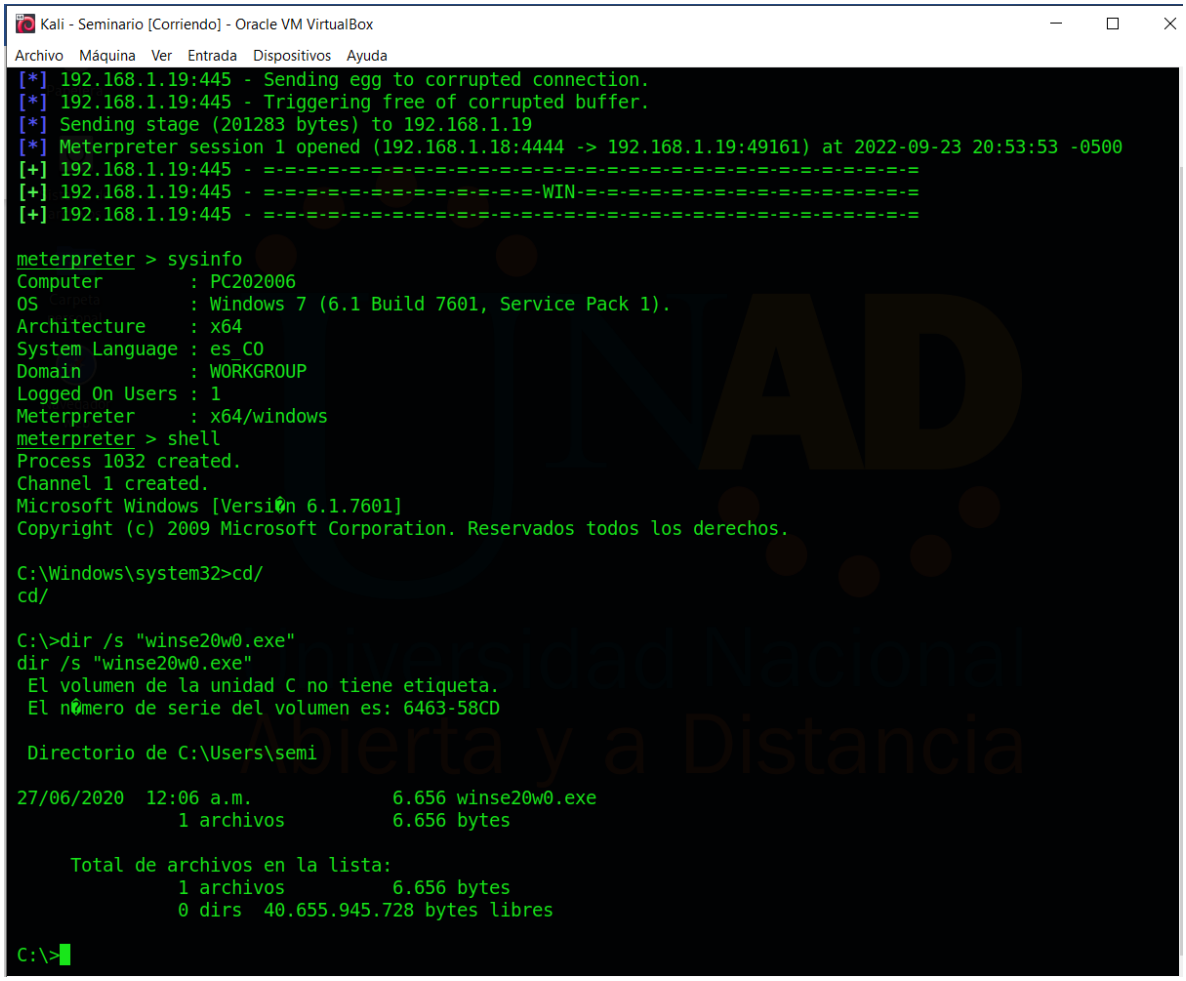
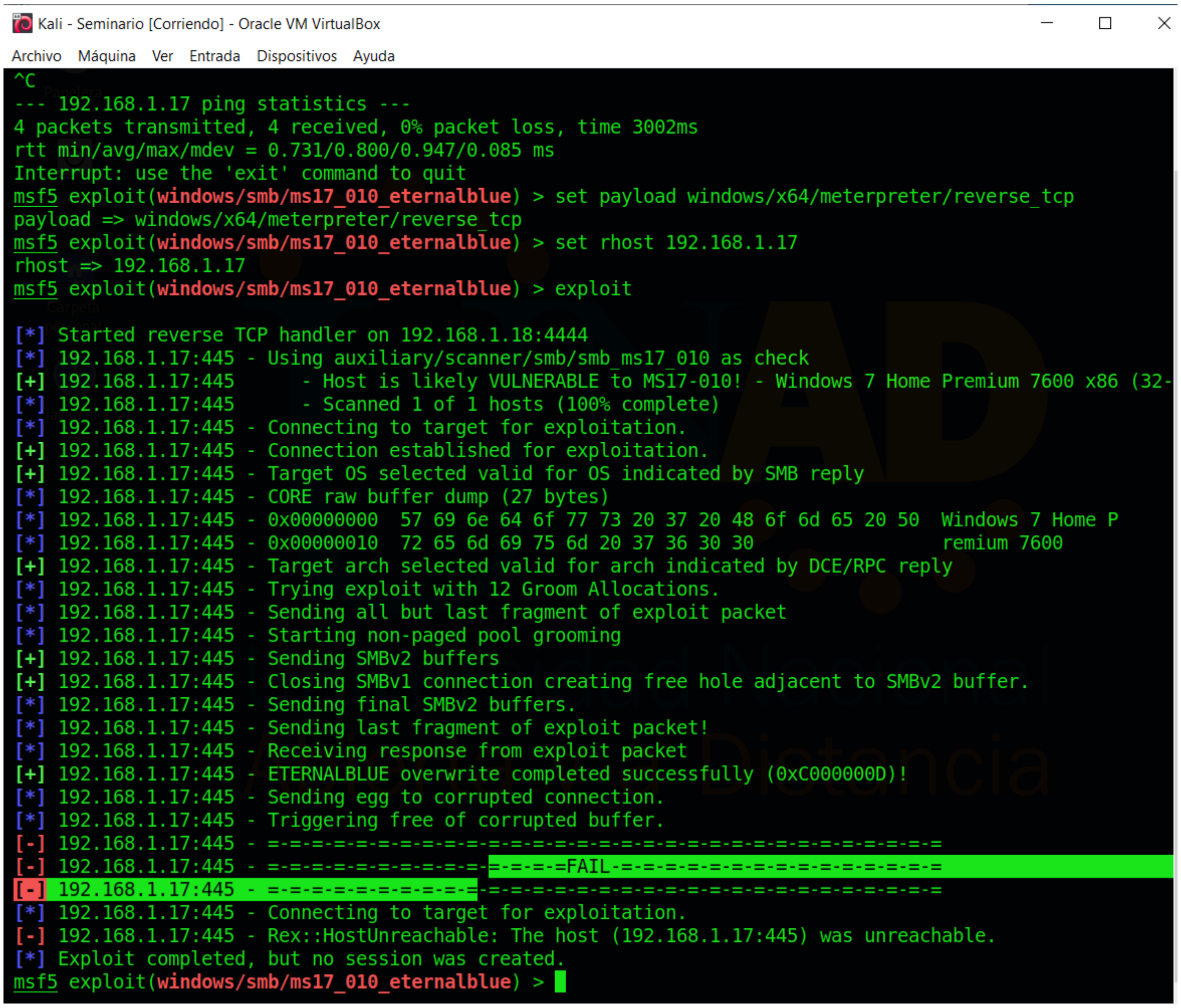

Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
[*] 192.168.1.19:445 - Sending egg to corrupted connection.
[*] 192.168.1.19:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.1.19
[*] Meterpreter session 1 opened (192.168.1.18:4444 -> 192.168.1.19:49161) at 2022-09-23 20:53:53 -0500
[+] 192.168.1.19:445 - =-=-=-=

Ilustración 25 Ejecución archivo "winse20w0.exe

Fuente: propia

De igual forma se realiza el procedimiento sobre la **maquina objetivo Windows7 x86**

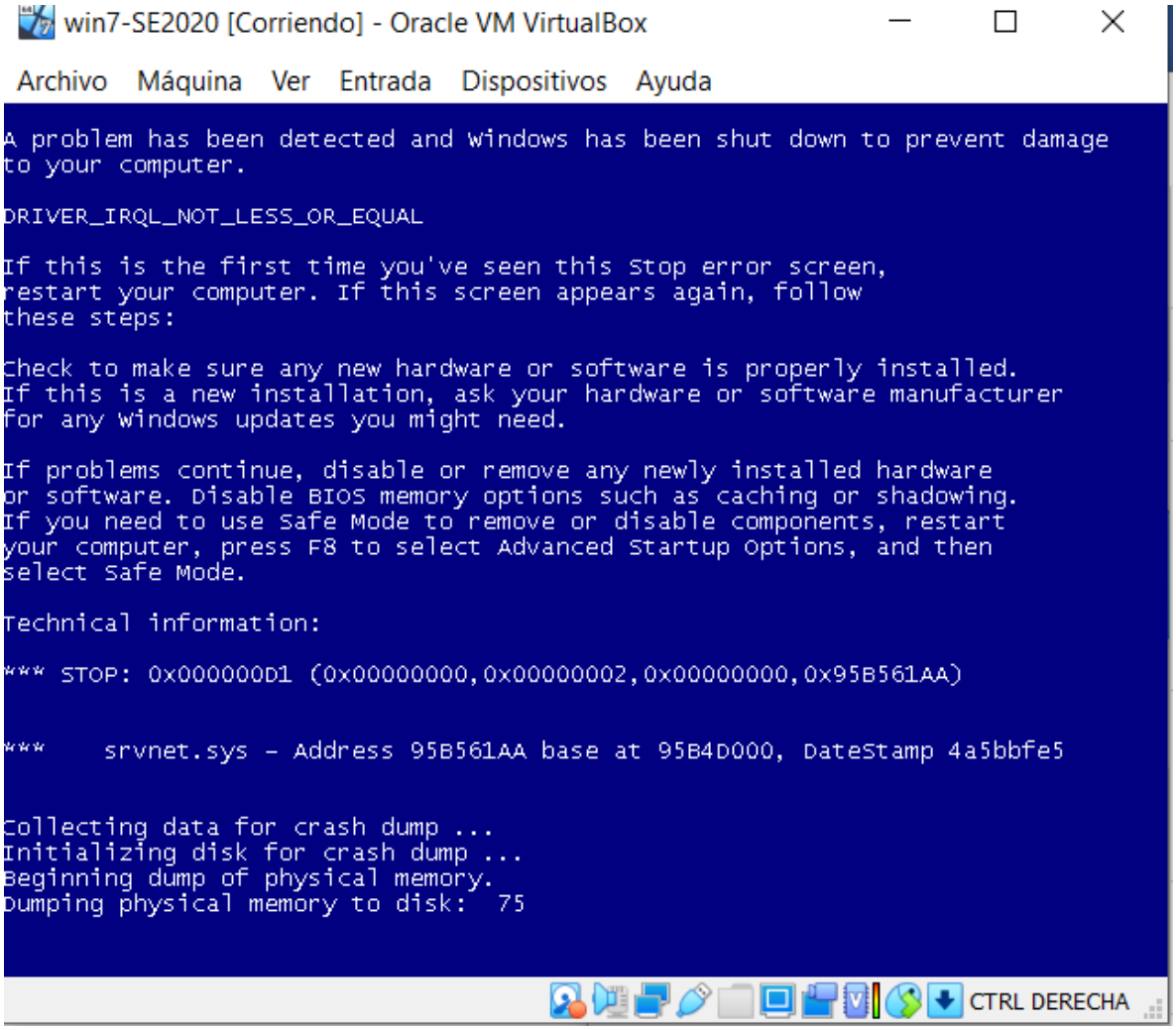
Ilustración 26 Explotación de la vulnerabilidad Windows7 x86



Fuente: propia

Al realizar el intento de la vulnerabilidad en este equipo **genera una pantalla azul** en la maquina objetivo Windows7 x86, **debido a que la carga útil no corresponde al sistema operativo.**

Ilustración 27 Pantalla Azul Windows7 x86



Fuente: propia

INFORME DE EXPLOTACIÓN DE LAS VULNERABILIDADES EN BANCO DE TRABAJO

- **Windows7 x64**

Después de realizado el análisis de las vulnerabilidades a esta máquina, se confirma la fuga de información, por medio del exploit ms17-010 el cual está documentada en las bases de datos del CVE-2017-0143.

CVE-2017-0143: El protocolo de red de capa de aplicación comúnmente utilizado en Microsoft Windows para proporcionar acceso compartido a archivos e impresoras. SMBv1.[13]

De esta manera se pudo validar con la herramienta metaexploit la ejecución en esta máquina del archivo ejecutable "**winse20w0.exe**".

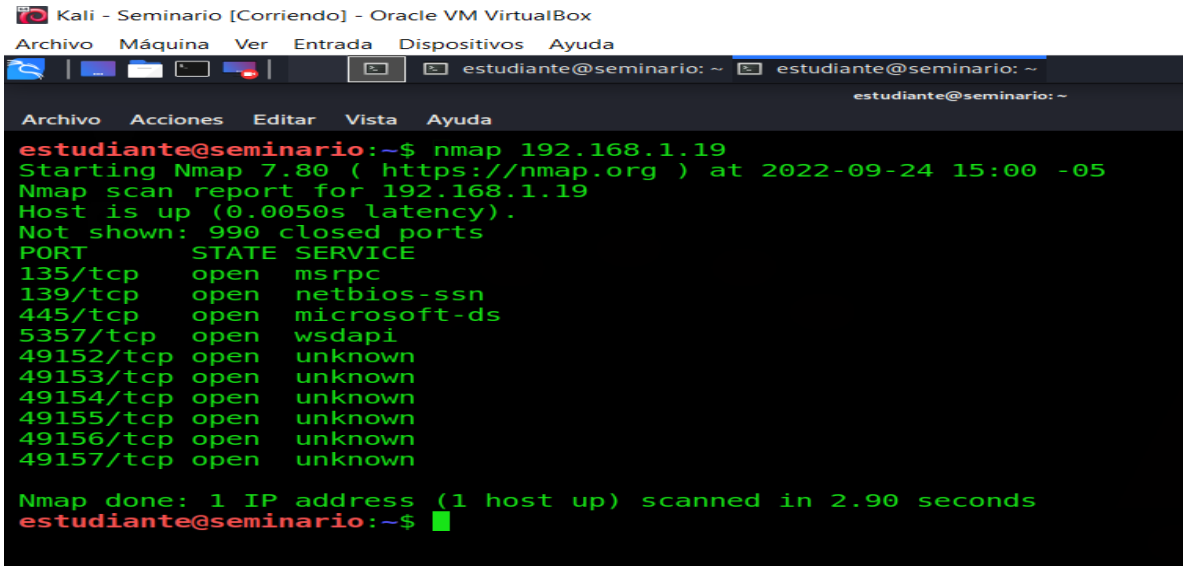
- **Windows7 x86**

Al ejecutar el mismo proceso de vulnerabilidad del exploit ms17-010 en está maquina no se puede continuar el proceso debido a que la maquina objetivo presenta pantalla azul debido a que la carga útil no corresponde a su sistema operativo.

EVIDENCIA DE LA EXPLOTACIÓN DE LA VULNERABILIDAD IDENTIFICADA

Como evidencia de la vulnerabilidad identificada en la maquina Windows7 x64 se procede a crear una cuenta administradora en está maquina objetivo.
Se procede a validar que puertos se tienen abiertos en la maquina objetivo

Ilustración 28 IPs Activas Windows7 x64



Fuente: propia

[13] CVE. (2022) CVE-2017-1182 [En Línea]Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Se procede a ingresar a crear la sesión desde Kali Linux con el meterpreter y se procede a crear la cuenta con los comandos requeridos según se visualiza en la siguiente ilustración.

Ilustración 29 Creación cuenta Windows7 x64

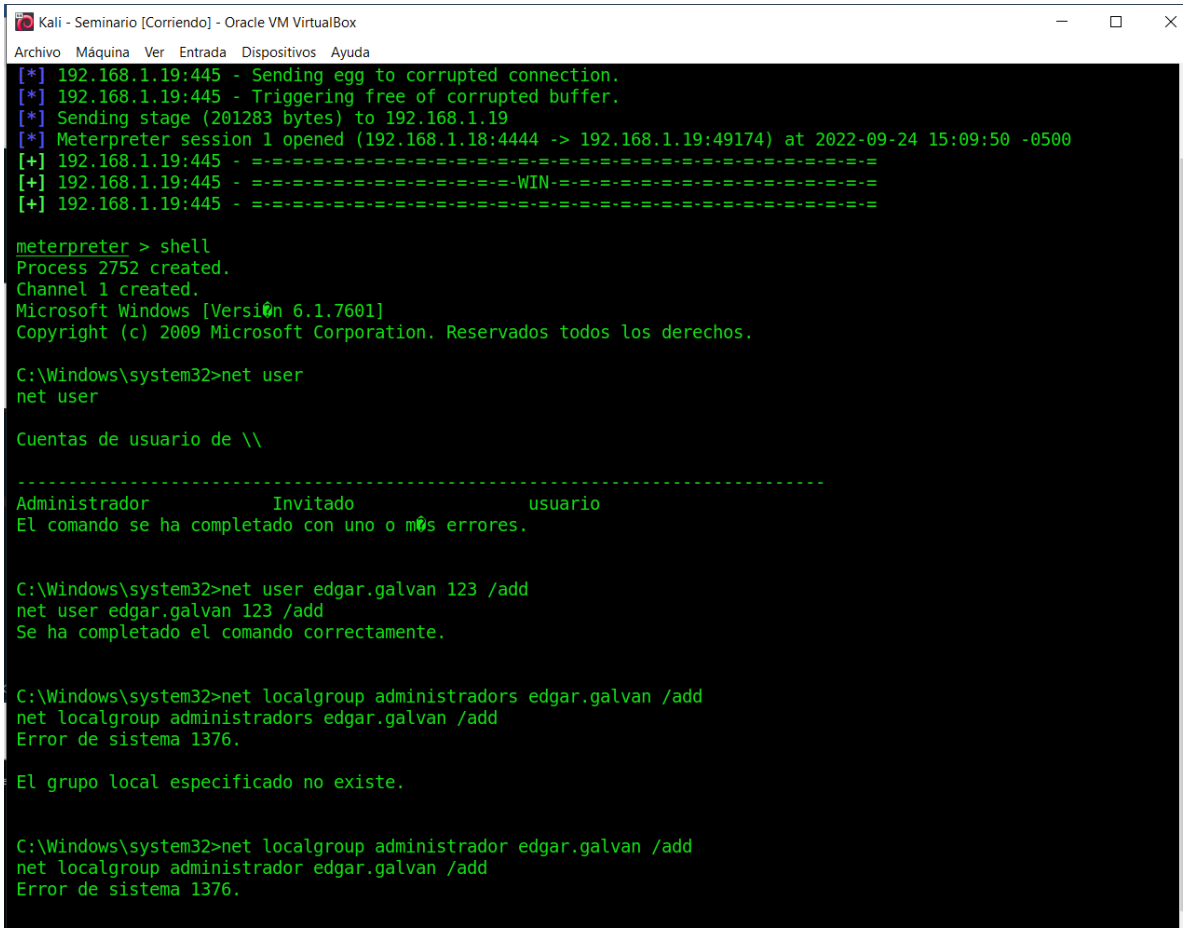
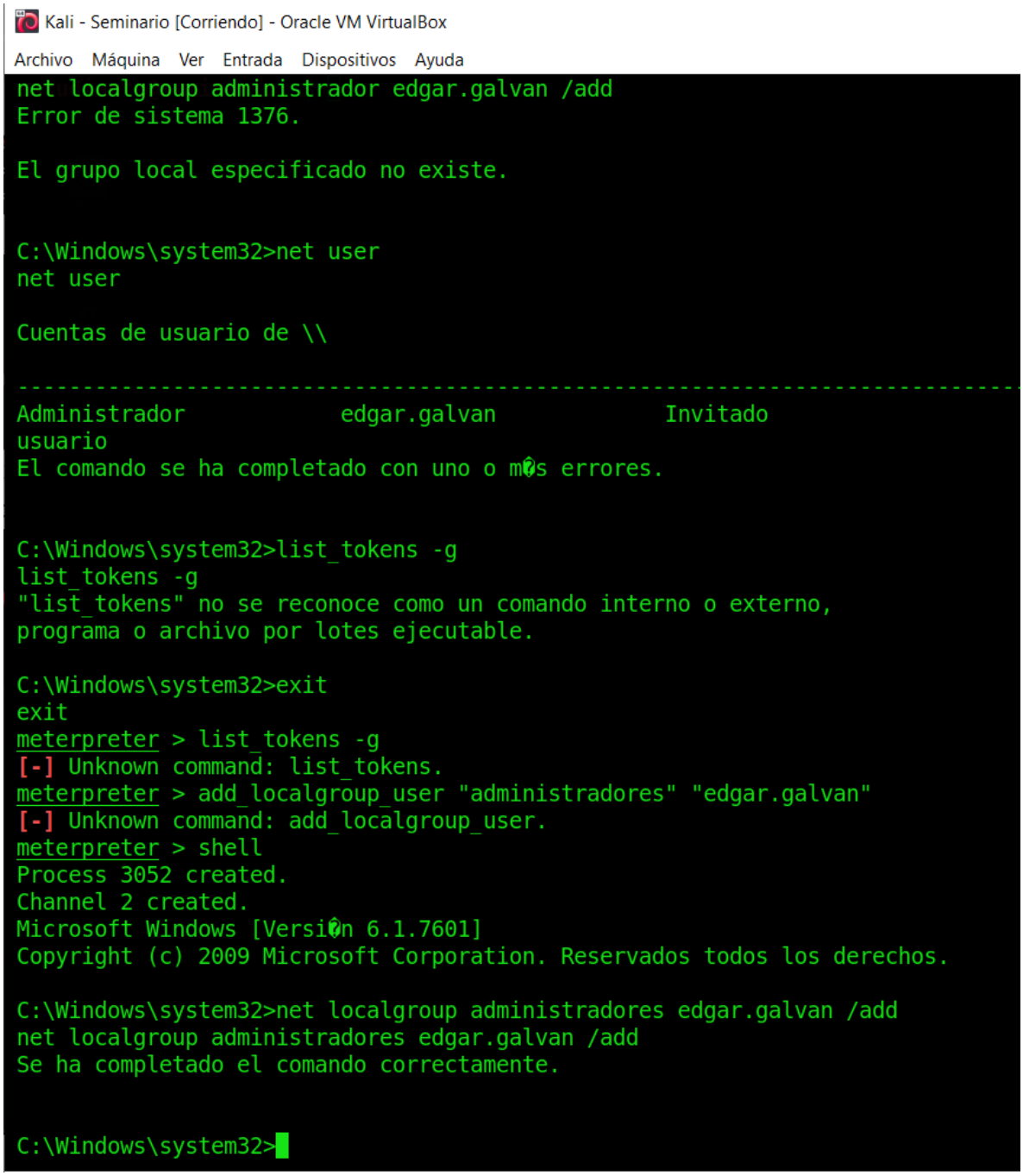

Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
[*] 192.168.1.19:445 - Sending egg to corrupted connection.
[*] 192.168.1.19:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.1.19
[*] Meterpreter session 1 opened (192.168.1.18:4444 -> 192.168.1.19:49174) at 2022-09-24 15:09:50 -0500
[+] 192.168.1.19:445 - =-=-=-=

Ilustración 30 asignación permisos administrador



Fuente: propia

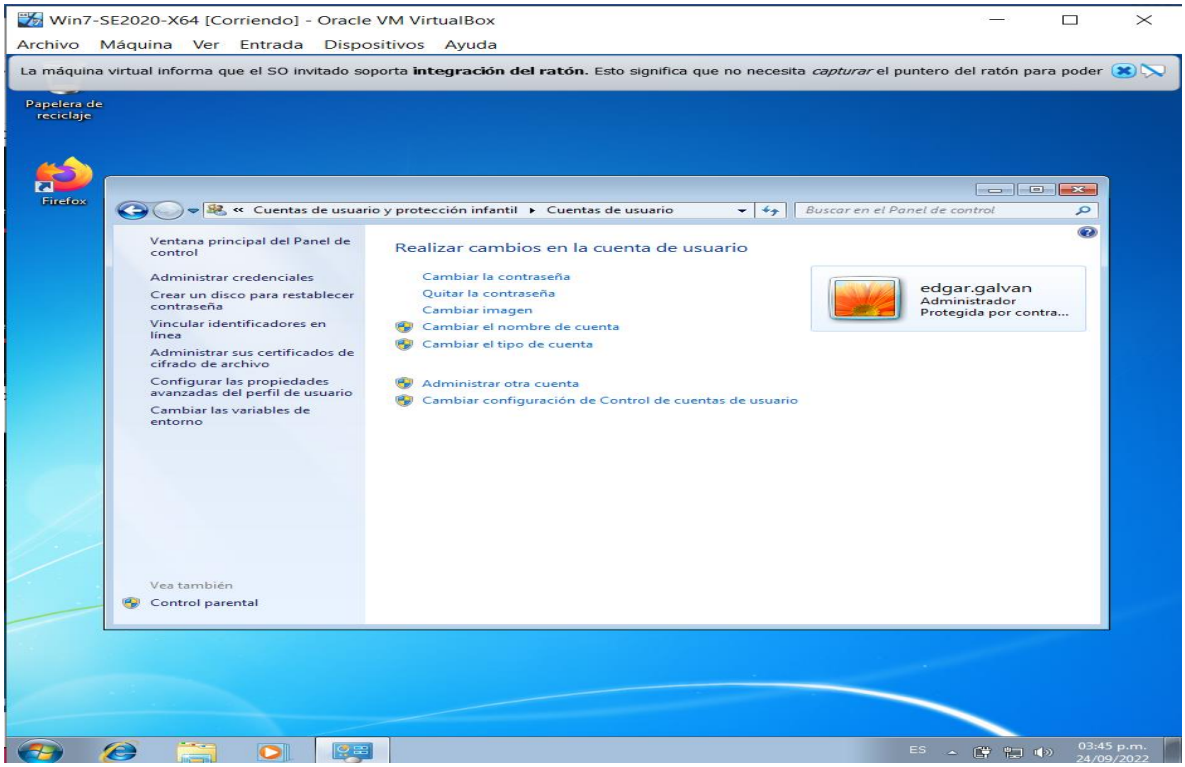
Como evidencia se visualiza en el escritorio de inicio de la maquina windows7 x64 la cuenta recién creada “Edgar.galvan”

Ilustración 31 creación cuenta edgar.galvan Windows7 x64

Fuente: propia

Se ingresa a la maquina objetivo y se visualiza el perfil administrador, asignado a esta cuenta

Ilustración 32 perfil administrador cuenta Windows7 x64



Fuente: propia

2. ANÁLISIS CON ACCIONES NECESARIAS PARA CONTENER UN ATAQUE EN TIEMPO REAL

Lo primera acción en la presencia de un incidente de ataque es notificarla al primer punto de contacto definido por la entidad de acuerdo con los protocolos o formatos establecidos previamente para este caso de eventos.
El punto de contacto debe identificar y clasificar el tipo de incidente presentado y analizar si compete a un incidente de SGI o de infraestructura TI y realizará el seguimiento de este, coordinando las diferentes actividades que se deban realizar para la contención del mismo.
Las siguientes acciones son:

- **Fase de Contención**: En esta fase se indaga la detección del ataque presentado, con la finalidad de no permitir que se propague o continue con la perdida de la información o de afectación de la infraestructura. Tan pronto se conozca la vulnerabilidad se deben tomar acciones como **bloquear la cuenta, apagar el sistema, desconectar el equipo de la red o deshabilitar los servicios**. Todas estás acciones dependen de la criticidad y el impacto del incidente
- **Fase de erradicación y Recuperación**: Después de contener la vulnerabilidad en la anterior fase se procede a erradicar eliminar cualquier rastro del incidente presentado. Procediendo posteriormente a la recuperación del daño efectuado haciendo **reinstalación del equipo y recuperación de datos**
- **Fase Post Incidente**: En esta fase se realiza un reporte con las lecciones aprendidas.[14]

[14] Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19). https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

ANÁLISIS SOBRE LAS FUNCIONALIDADES ENTRE EL EQUIPO DE BLUE TEAM Y EL EQUIPO CSIRT

Ilustración 33 Diferencias entre Blueteam y CSIRT

Blue Team	CSIRT
• Expertos en proteger de los ataques externos, los activos de la entidad desde adentro hacia afuera • Documenta todo lo que se debe proteger • Protege y evalúa los riesgos • Refuerza el acceso al sistema • Efectuar auditorías internas del sistema • Desarrollar un plan que permita proteger los activos a través de controles existentes	• Expertos en restituir las actividades con el impacto mínimo aceptable para las entidades • Controla y minimiza cualquier afectación de la información o infraestructura TI y preserva la evidencia. • Coordina las actividades para una recuperación pronta de las actividades que se pudieron ver afectadas • Previene eventos futuros que puedan ocurrir, registrando las lecciones aprendidas

Fuente: propia

ANÁLISIS SOBRE LA OPORTUNIDAD DE INTEGRAR CON CIS "CENTER FOR INTERNET SECURITY" COMO PROPUESTA DE HARDENIZACIÓN POR PARTE DE UN EQUIPO DE BLUE TEAM

CIS tiene el Multi-State Information Sharing and Analysis Center, el recurso confiable para la prevención, protección, respuesta y recuperación de amenazas cibernéticas.[15]

A continuación, se presentan las principales características y funciones de un SIEM:

Permite detectar, responder y neutralizar cualquier amenaza informática, su función principal es la de tener vigilancia total sobre la infraestructura TI de la entidad en línea, para detectar patrones fuera de lo común.
Sus principales características son:

15 CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. [En Línea]Disponible en: https://www.cisecurity.org/cis-benchmarks/

- Centraliza la información de seguridad
- Automatiza tareas
- Da respuesta inmediata a eventos y amenazas
- Reduce el tiempo de detección de ataques
- Da información inmediata y eficaz para realizar análisis forense
- Tiene Alertas de seguridad efectivas
- Análisis en tiempo real de logs.
- Realiza seguimiento de eventos.
- Maneja mejor el riesgo.
- Manejo de métricas de seguridad.
- Detección de activos.
- Tiene evaluación de vulnerabilidades.
- Detecta violaciones de seguridad.
- Posee monitoreo de comportamiento.

3. CONCLUSIONES

Esta actividad permitió, tener el contexto ético y legal de los equipos Red Team & Blue Team, lo cual permite tener un conocimiento claro de las consecuencias a la que se esta expuesto, si se infringe alguna norma, que pueden ir desde la perdida de la tarjeta profesional, como multas de dinero y prisión.

Los equipos RedTeam & BlueTeam, deben determinar estrategias y herramientas que sirvan de apoyo para la ejecución y cumplimiento, relacionados con procesos de identificación de fallos de seguridad en plataformas de Tecnologías de la Información - TI. Que permitan alertar a tiempo sobre posibles fugas de información y ataques a la infraestructura TI.

Por su parte los equipo BlueTeam, deben analizar y contener a partir de una serie de procesos y herramientas, las cuales se orientan a la contención de un ataque informático y a su posterior remediación. Asegurando el activo más importante de las organizaciones como lo es la información y su infraestructura tecnológica, garantizando el normal funcionamiento de sus actividades y protección de los datos.

4. RECOMENDACIONES

En este informe permite tener una claridad más detallada y practica de los equipos Red Team & Blue Team.

La importancia de estar preventivos a ataques que en cualquier momento se puedan presentar afectando la infraestructura TI o la información.

Conocer sus aspectos legales, las herramientas con las que se cuenta para analizar un ataque presentado en tiempo real, contener un ataque y lo más importante prevenirlo

La importancia de tener actualizados los equipos y utilizar las diferentes herramientas que permiten contener un ataque.

Es importante tener clara la funcionalidad de cada equipo Red Team & Blue Team, para simular atraques como el caso del equipo red y de contenerlos o prevenirlos como el equipo Blue.

A continuación, se presentan una serie de medidas de Hardenización, para evitar que se vuelva a presentar el ataque:

- Después de realizar el análisis a las maquinas expuestas y encontrar sus vulnerabilidades, se debe desconectar de la red de la entidad, para evitar la fuga de la información y más daños que se puedan afectar la infraestructura de TI.
- Se debe deshabilitar las conexiones de transferencia de archivos e información a través del puerto 445 TCP.
- Se debe proceder inmediatamente con la activación del Firewall.
- Deshabilitar el protocolo SMBv1. Actualizar a una versión posterior segura.
- Instalar un buen antivirus

Actualizar las maquinas Windows, instalando los parches faltantes. Especialmente con el parcheo de seguridad MS17-010, para protegerlos de la vulnerabilidad CVE-2017-0144. Iniciando con la descarga en el catálogo de Microsoft update

“Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows 7 sistemas basados en x64 (KB4012212)” relacionada con el escenario propuesto.

- Por último, se debe realizar backup de la información, para evitar pérdidas

5. BIBLIOGRAFÍA

Alcaldía de Bogotá. Guardianes de la información Penetration Testing. [En Línea]. 2018.[Consultado el 11 de octubre de 2022]. Disponible en: https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-los-guardianes-de-la-informacion-de-la-alcaldia-de-bogota

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

COPNIA. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [En Línea]. 2015. [Consultado el 10 de octubre de 2022]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica 4

CVE. CVE-2017-1182. [En Línea]. 2022. [Consultado el 10 de octubre de 2022]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Enter.co. Detrás de Buggly: la historia de la fachada Andrómeda [En Línea]. 2015. [Consultado el 10 de octubre de 2022]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira. (pp. 18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20P R%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

INCIBE. OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. INCIBE-CERT. [En Línea]. 2014.[Consultado el 8 de octubre de 2022]. Disponible en: https://www.incibe-cert.es/blog/owasp-4

INCIBE. Auditando la seguridad de tus sistemas. ¿Qué es el pentesting?. [En Línea]. 2019. [Consultado el 8 de octubre de 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditandoseguridad-tus-sistema

Mintic. Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). [En Línea]. 2012. [Consultado el 8 de octubre de 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

PandaSecurity. Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. ?. [En Línea]. 2018. [Consultado el 8 de octubre de 2022]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentestingherramienta-empresa/

Policía. Ley 1273 [LEY_1273_2009].Policía. (pp. 1-4). [En Línea]. 2009. [Consultado el 8 de octubre de 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

OAS. Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). [En Línea]. 2018. [Consultado el 8 de octubre de 2022]. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Link video

https://youtu.be/Nav1CZ1Ifpc