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

ELABORADO POR :
DIEGO FERNANDO GONZALEZ THOLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA PLATA HUILA
2022

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

ELABORADO POR :
DIEGO FERNANDO GONZALEZ THOLA

TRABAJO ESCRITO

Nombre
JOHN FREDDY QUINTERO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA PLATA HUILA
2022

RESUMEN

Mediante cada una de las unidades planteadas se lograron abordar diferentes temas en base a la estrategia de aprendizaje basado en problemas, permitiendo afianzar conocimientos en cada uno de los contenidos ofrecidos para el desarrollo de las tres unidades en la etapa practica de la especialización, se abordaron temas referentes al contexto legal y ético, los cuales deben ser aplicados por unidades de red team o blue team en la ejecución de actividades diarias, se afianzaron conocimientos en las diferentes herramientas que permiten contrarrestar fallos de seguridad, permitiendo salvaguardar el activo más importante en la organización, la información de The WhiteHose Security, la organización sometió a prueba nuestras habilidades en seguridad, en donde se realizaron ataques en una máquina de prueba con el fin de penetrar la seguridad y explotar la vulnerabilidad encontrada en el sistema operativo de windows 7, también se plantearon situaciones en donde se incurre en la violación de una cuerdo de confidencialidad en donde se hizo claridad a que aspectos legales y que delitos se incurriría a raíz de las preguntas orientadoras planteadas.

CONTENIDO

LISTA DE FIGURAS

Pág.

GLOSARIO

Blue Team: Es un equipo de profesionales informáticos dedicados a la seguridad a la defensa el cual se dedican a estudiar e identificar diferentes patrones de ataques con el fin de contrarrestarlos, se encuentran disponibles para dar respuesta de forma emergente a incidentes de seguridad.

Red Team: son un grupo de especialistas de seguridad que emulan ataques en entornos controlados, vulnerando sistemas, y realizando diferentes técnicas de instrucción, exploits y técnicas hacking con el fin de simular un ataque real en una empresa, para luego pasar los resultados al grupo de defensa de la organización para la debida mitigación de los fallos vulnerado.

Hackers: Es un amante a la tecnología con grandes conocimientos avanzados de ingeniería e informática que investiga sistemas de comunicación con el fin de detectar vulnerabilidades que pongan en riesgo la información de usuarios para luego reportarlos y que sean corregidos.

Kali Linux : Es una distribución de GNU/LINUX, creada con funciones específicas de auditorías en seguridad informática, una completa suite que permite explotar fallos de seguridad en cualquier tipo de red desprotegida.

Pentesting: son diferentes técnicas de hacking utilizadas para realizar ataques informáticos

Hardening: traduce endurecimiento, esto hace referencia en el campo de la informática como el proceso de asegurar, robustecer un sistema, garantizando un nivel de seguridad más amplio ante cualquier ataque informático.

INTRODUCCIÓN

La creación de Equipos Estratégicos de Ciberseguridad (Red Team & Blue Team), surgen de la necesidad de proteger los sistemas de información, que a diario son atacados con distintas finalidades y en la mayoría de los casos con fines oscuros o criminales. Estos equipos tienen como misión, el desarrollar habilidades que les permitan planificar, ejecutar y solucionar todos aquellos problemas que se generen por un ataque informático. Para lograrlo deben encaminar todos sus conocimientos y seguir una hoja de ruta que les permita cumplir con los objetivos propuestos. Es por ello que este seminario abarca los principales temas que se deben tener en cuenta, para guiar las labores o procesos, que se deben dar dentro esta clase de equipos, con el fin de orientarlos y permitir que se cumplan con los objetivos propuestos. A continuación, se expone el desarrollo de todas las actividades propuestas en este seminario.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Lograr el desarrollo de habilidades, que permitan planificar, ejecutar y solucionar problemas, eventos, incidentes o ataques de ciberseguridad informática a un sistema o infraestructura TI, teniendo en cuenta siempre el código de ética y las leyes que rigen en este tema para no cometer delitos informáticos.

1.2 OBJETIVOS ESPECÍFICOS

- ✓ Desarrollar el uso de métodos o técnicas de intrusión para generar situaciones de ataque informático, con el fin de determinar las vulnerabilidades que presente un sistema informático.
- ✓ Identificar de manera rápida y ágil, aquellas acciones que generen indicios de un ataque informático.
- ✓ Identificar todas aquellas herramientas (software, hardware), que permitan contribuir a una mayor seguridad del sistema.
- ✓ Crear, mantener y actualizar el desarrollo de buenas prácticas de ciberseguridad, para fortalecer los sistemas informáticos.
- ✓ Conocer las leyes, que rigen en todo el territorio nacional sobre todas aquellas acciones que son consideradas como delitos informáticos, con la finalidad de no incurrir en ellas a la hora de ejecutar procesos que puedan vulnerar la seguridad de un sistema informático y vulnerar la integridad de las personas que resulten implicadas en estos asuntos.

2 INFORME TECNICOS

Con respecto a la **Unidad 1**, Contexto Ético, Legal Red Team & Blue Team, se llevaron a cabo tres procesos, por una parte las lecturas indicadas para esta unidad, suministradas por el tutor; también se realizaron lecturas a través de internet para ampliar la información con respecto de la leyes que existen en Colombia, con el fin de identificar las acciones que son tipificadas como delitos informáticos, el tema de las pruebas de penetración o pentesting, las herramientas utilizadas para este tipo de pruebas y finalmente la configuración del Banco de Trabajo, para la realización de la parte práctica de esta unidad. De las anteriores consultas y lecturas se obtuvo la siguiente información:

2.1 Normatividad sobre Delitos Informáticos:

Ley 1273 de 2009: "De la protección de la información y de los datos: cuya característica principal es preservar los sistemas que usan tecnologías de información y comunicaciones, así mismo quien incurra en estos delitos y en virtud al código penal colombiano tendrá penas de prisión y multas, otros delitos que se encierran en ésta ley y que también son penalizados son: Atentar en contra de la confidencialidad de las empresas, el acceso abusivo, la obstaculización del normal funcionamiento del sistema, la intercepción de datos informáticos, la suplantación de sitios web para hurtar información personal, transferir activos sin consentimiento"[1].

Ley 1581 año 2012: Caracterizada por clasificar y proteger los datos personales, en donde se define como dato personal de acuerdo con le ley 1581 (2012); "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas".

Documento CONPES 3854, 11 de abril de 2016: Sobre la política nacional de seguridad digital, cuyas características son la protección de las entidades estatales contra posibles ataques cibernéticos y la prevención de estos.

[1] LEY 1273 DE 2009. Formato PDF. {En línea} {08 de septiembre de 2020} disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009. pdf).

Decreto 1377 de 2013: Es un decreto para reglamentar la ley 1581 de 2012, se caracteriza por la protección de datos personales, tocando temas relacionados a la transferencia y transmisión de datos, el tratamiento de los datos, seguridad de la información en las organizaciones.

Ley 1712 de 2014: Transparencia y del Derecho de Acceso a la Información Pública y Nacional, se caracteriza por contar con unos principios que son de publicidad, transparencia, buena fe, facilitación, discriminación, gratuidad, celeridad, eficacia, calidad de la información, divulgación de la información, responsabilidad en el uso de la información, esta ley permite el derecho al acceso de la información pública publicada en los sistemas de información del estado.

Decreto 103 de 2015: Por el cual se reglamenta parcialmente la ley 1712 de 2014; se caracteriza por tener consideraciones en cuanto al derecho de la información pública y la protección de la misma, otra característica es que dicha información está a cargo de la secretaria de transparencia de la presidencia, del ministerio de tecnologías de la información y comunicaciones, entre otros, Así mismo; Dicha información se clasifica, se reserva, se publica y divulga adecuadamente.

2.2 Pruebas de Penetración o Pentesting

Son las prácticas que se realizan para atacar a un sistema informático, con el fin de encontrar fallos en el mismo.

2.3 **Etapas del Pentesting:**

- ✓ **Reconocimiento:** En esta etapa se busca toda la información de la empresa o entidad que sea de utilidad para poder ingresar al sistema, algunas de las herramientas útiles serían los buscadores como Google y algunas redes sociales que nos proporcionen información relevante de la misma como Facebook e Instagram.

- ✓ **Escaneo de puertos, servicios, OS:** En esta etapa se pretende conocer muy bien el sistema que queremos atacar, para lo cual se ejecuta un escaneo cuya finalidad sea encontrar los host activos en la red con mucha discreción y de la manera menos tediosa posible; Una herramienta de gran utilidad sería Nmap que se usaría para explorar la red.

- ✓ **Identificación de sistemas, puertos activos, servicios y usuarios:** La idea en esta etapa es realizar una identificación plena del sistema operativo, de los potenciales blancos en el sistema, de módems, de configuraciones inseguras, entre otros, con el objeto de realizar una exploración de las posibles entradas al sistema, para esto se hace uso de herramientas como Nmap

- ✓ **Análisis de vulnerabilidades:** El objetivo de la presente etapa es encontrar fallas en el sistema, por medio de las cuales podamos acceder más fácilmente a él, para ello se puede utilizar herramientas como: Nessus.

- ✓ **Explotación de vulnerabilidades:** Es aprovechar al máximo la vulnerabilidad detectada con antelación a fin de acceder al sistema, una herramienta utilizada puede ser Metasploit.

- ✓ **Informes:** Aquí se documenta todo el proceso detallando cómo se llevó a cabo la intrusión al sistema y qué herramientas se utilizaron en cada una de las etapas. Las herramientas que se usan en esta etapa deben ser formatos de fácil comprensión como por ejemplo SSL ”.[2]

[2] GUILLÉN ZAFRA, José Luis. “Introducción al pentesting”. Barcelona, 2017. 66p. {En línea} {30 de septiembre de 2020} disponible en (http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf)

2.4 **Herramientas Utilizadas para Pentesting :**

- ✓ **Nmap:** Es una herramienta gratuita y multiplataforma, útil para rastrear puertos, explorar la red, identificar sistemas informáticos y evaluar sus ventajas, se caracteriza por su flexibilidad, por identificar puertos abiertos, sistema operativo y la versión que utiliza un host determinado
- ✓ **Nessus** es un programa que contiene una base de datos de exploit para diferentes sistemas operativos, aunque es de paga se puede usar en simultánea con equipo limitados. Con este programa se idéntico la sospecha del fuga de información a través del puerto 80, el cual la empresa comparte recursos y por no estar actualizado los sistemas operativos muestra la falla de seguridad y el posible uso de exploit para explotar esa vulnerabilidad
- ✓ **Metasploit Framework** es la herramienta encontrada para explotar esta vulnerabilidad, ya con los datos recolectados como la actualización no instalada, el protocolo usado para compartir recursos y el informe de Nessus combinado con nmap se identifica la vulnerabilidad, se procede hacer la exploración en las maquinas víctimas.
- ✓ **OpenVas:** Esta herramienta multiplataforma utilizada para escanear y buscar vulnerabilidades de seguridad en un sistema informático “apoyándose en una base de datos
- ✓ **ExploitDB:** Este servicio sirve para beneficiarse de una vulnerabilidad de un sistema de información, un exploitDB es una herramienta para aprovechar un fallo de seguridad, cuyo objetivo radica en lograr acceso a un equipo.

2.5 **Proceso y Configuración del Banco de Trabajo**

Para el desarrollo de este punto se procedió a descargar y configurar el software virtualizador “VirtualBox” solicitado en el anexo 1 – Escenario 1 sobre el cual se trabajaron las actividades practicas con un alto nivel de complejidad.

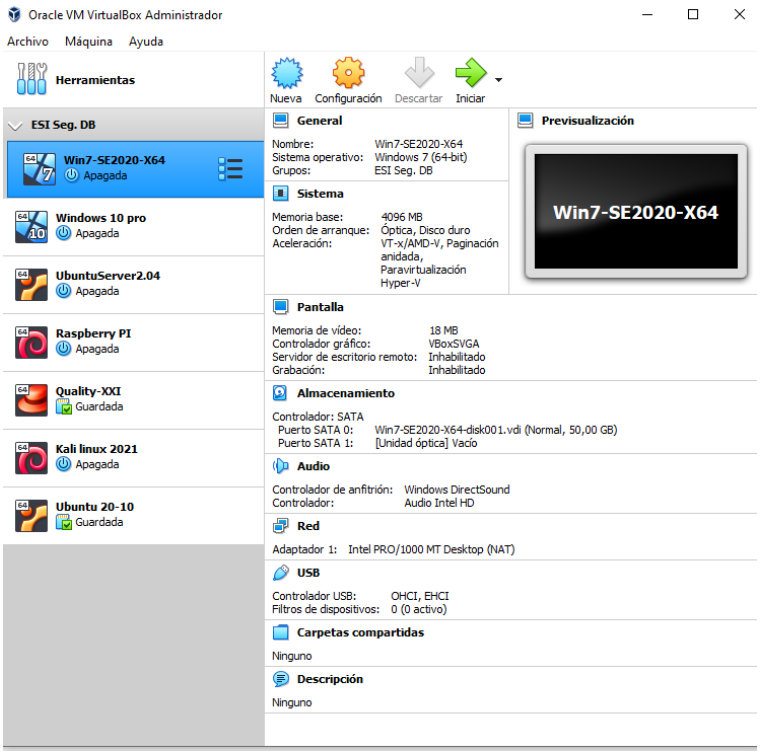
Luego de realizar la instalación del programa virtualizador, se muestra en la figura 1. La última versión actualizada de virtualbox.

Figura 1. Versión virtualbox.

Fuente: Autor

En la Figura 2. Se muestra las respectivas especificaciones técnicas configuradas en sistema operativo instalado windows 7 x64 , en virtualbox.

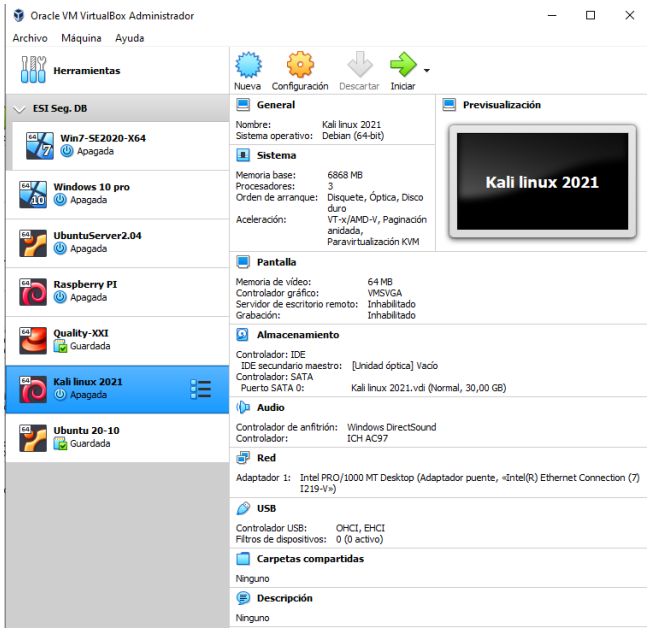
Figura 2. Entorno De Trabajo Win. 7 x64



Fuente: Autor

En la figura 3, se muestra detalladamente la configuración del banco de trabajo de la potente herramienta KALI LINUX , la cual nos permitirá realizar los ataques a la maquina instalada anteriormente.

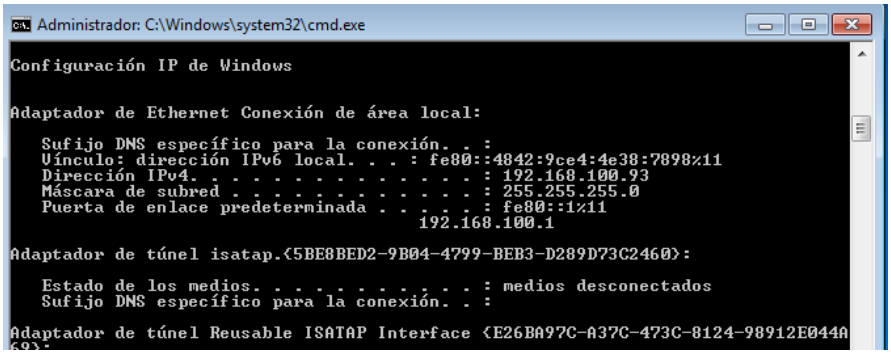
Figura 3. Características KALI LINUX



Fuente: Autor

Continuando el desarrollo de la actividad , lo primero que se realiza es verificar si existe comunicación entre las dos maquinas para realizar los ataques, nos dirigimos a la maquina windows y a través del CMD se digita la siguiente línea para verificar la IP de la máquina. Como se muestra en la Figura 4, se comprueba la IP de la maquina para ejecutar un ping desde Kali y comprobar comunicación entre ella.

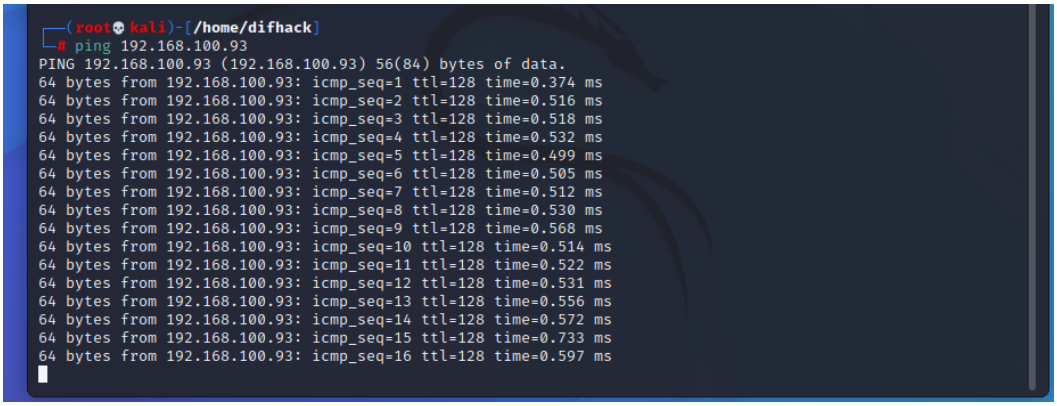
Figura 4. Verificación IP máquina de Windows.



Fuente: Autor

En la figura 5, se realiza un ping a la IP de la maquina windows para comprobar que exista comunicación, como se muestra en la imagen se idéntica que responde ha llamado confirmando que hay una conexión exitosa.

Figura 5. Ping a máquina windows desde Kali Linux



Fuente: Autor

3. ANÁLISIS LEGAL Y NO ÉTICO DEL CONTRATO ENTREGADO POR WHITEHOUSE SECURITY

El contrato fue realizado por un abogado que ya no labora para la organización y como profesionales de seguridad se realizaron diferentes análisis y se procedió a realizar diferentes señalamientos respecto a los fragmentos ilegales encontrados

Es claro que hay evidencia de un proceso ilegal y no ético, por parte de la organización White House Security. Ilegal porque lo legal hubiese sido que la organización redactara los nuevos contratos o que hiciera revisar los antiguos, para modificarlos en caso de irregularidades en los mismos; y no ético porque al tratarse de una empresa tan seria a nivel mundial, en el manejo de seguridad informática, no debería haber permitido la contratación de personal con contratos antiguos y con falencias, ya que fueron realizados por un abogado que no labora para la empresa y que fue despedido por llevar a cabo procesos ilícitos. Lo correcto en ese momento seria haber contratado un nuevo abogado para eldesarrollo de esta labor, o desde la gerencia hacer una revisión minuciosa de los

anteriores contratos, con la finalidad de modificarlos para garantizar tanto la seguridad de la organización como la de las personas contratadas. De acuerdo con lo expresado anteriormente menciono las cláusulas del acuerdo, que a mi entender pueden estar violando las leyes y el código de ética que rige para los Ingenieros.

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

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial."

Cuarta. Obligaciones de la parte receptora incisos:

- ✓ " No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."
- ✓ " Responder por el mal uso que le den sus representantes a la información confidencial."
- ✓ "La parte receptora se obliga a no transmitir, comunicar, revelar o de

cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por parte de Whitehouse Security.”

Apreciaciones:

Con respecto a la cláusula primera, Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.” Llama la atención que, de entrada, en la cláusula mencionada, aparece el término “procesos ilegales”, lo que conlleva a pensar que si se realizan procesos poco convencionales para realizar el trabajo.

Con respecto a la cláusula tercera, origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de sufuente o soporte y sin que requiera advertir su carácter confidencial.” Pareciera ser una cláusula clara acerca de donde proviene la información, pero esta cláusulano hace mención a la forma o a los procesos específicos que se hacen para poder obtener esa información y es ahí en donde se puede incurrir en las faltas que las Leyes Colombianas tipifican como delitos.

Con respecto a la cláusula cuarta, obligaciones de la parte receptora, inciso 7, “responder por el mal uso que le den sus representantes a la información confidencial”, me genera gran inquietud, pues si bien es cierto que a la hora de firmar un contrato se acepta todo lo que en él está contenido, es una cláusula para

tenerla en cuenta y analizarla muy detalladamente y lo que implica; pues al presentarse problemas de tipo ilegal, la responsabilidad también recae sobre el empleado y las consecuencias que se pueden originar de una situación como esta sería la detención y privación de la libertad por el tiempo que así lo considere la justicia y de acuerdo a la falta cometida, fuera de ello se puede perder el derecho a ejercer su profesión.

Se encontraron varios procesos iguales el cual fueron mencionados de acuerdo con los artículos de la ley 1273.

Los artículos que se vulneran en el acuerdo expuesto son:

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO: Para obtener la información que desean se aprovechan de la vulnerabilidad en elacceso a los sistemas de información.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS: Cuando se ingresa sin orden judicial previa, para interceptar datos informáticos en su origen, destino, o en el interior de un sistema informático.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES: Cuando sin estar facultados se crean páginas similares a las de una entidad y se envían correos, spam, ofertas de empleo y de esa manera las personas suministran información de tipo muy personal.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES: El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique, emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes. Desde mi punto de vista son los artículos que se pueden vulnerar y que están contenidos en la Ley 1273 para el territorio de Colombia. ”.[3]

[3] LEY 1273 DE 2009. Formato PDF. {En línea} {08 de septiembre de 2020} disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

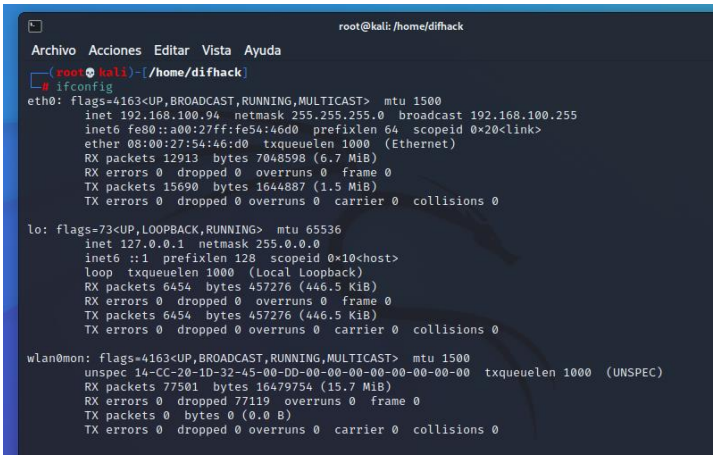
4. ANALISIS RED TEAM DE ACUERDO CON LA SITUACION PROBLEMA

La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Dentro de la investigación también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

Se desarrollo todo el procedimiento del pentest en busca de vulnerabilidades y posibles fallos en la maquina windows 7, donde se lograron excelentes resultados , se consiguió verificar que mediante el servidor web, existía una falla grave a través de su puerto donde fácilmente fue explotada la maquina y se logró interrumpir la seguridad en donde se puso en evidencia la información del equipo y se logró identificar el archivo .exe que estaba generando la fuga de información.

Como se puede visualizar en la Figura 6, se identificó en que red estaba la máquina Kali, con la línea ifconfig, se pudo identificar que el computador esta la misma red pública y segmento, la IP del Linux es la **192.168.100.94**

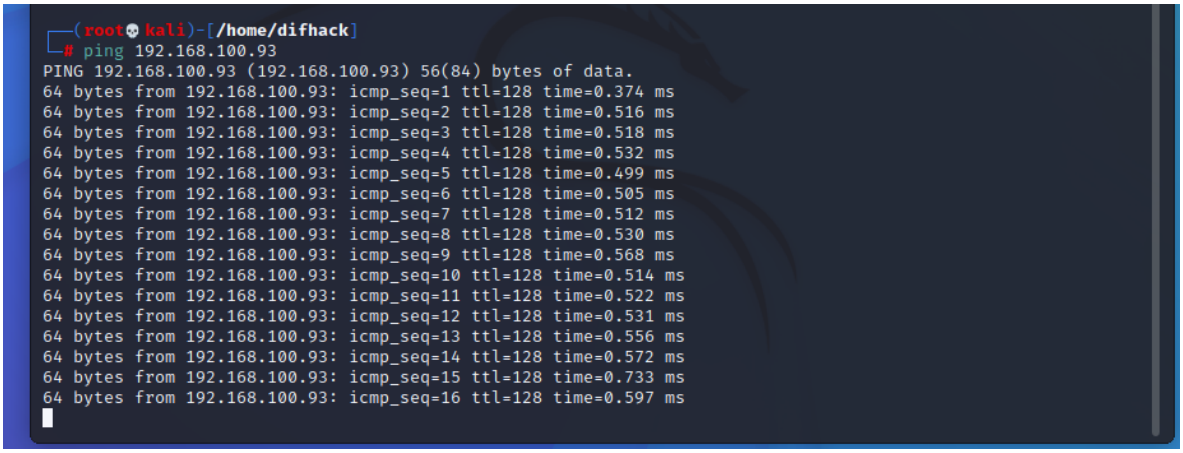
Figura 6. Verificación IP maquina Linux



Fuente : Autor

La figura 7, muestra el resultado de un ping a la maquina windows que se realizara el ataque con el fin de resolver el caso problema planteado, se demuestra que responde y existe comunicación con nuestro Kali Linux.

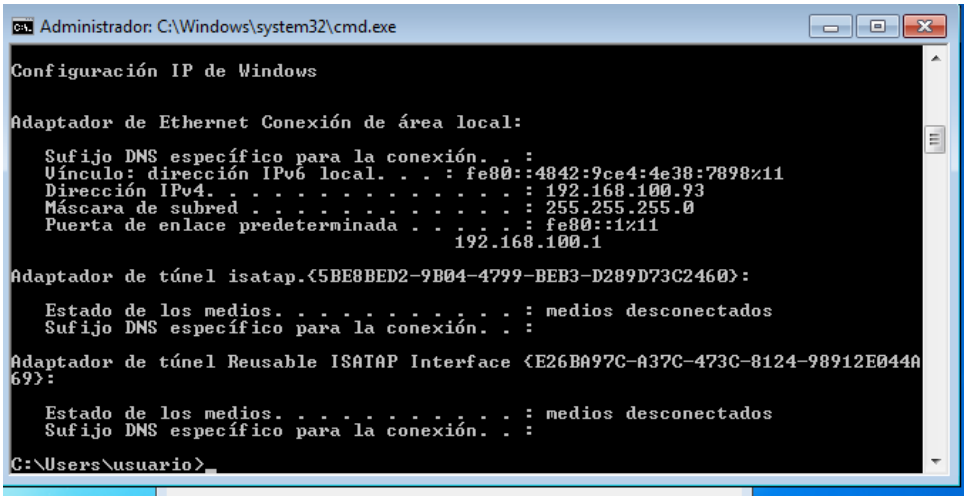
Figura 7. Verificación de comunicación entre las dos maquinas



Fuente : Autor

Figura 8, es el resultado donde se verifico que efectivamente la ip de la maquina windows es que termina en 93.

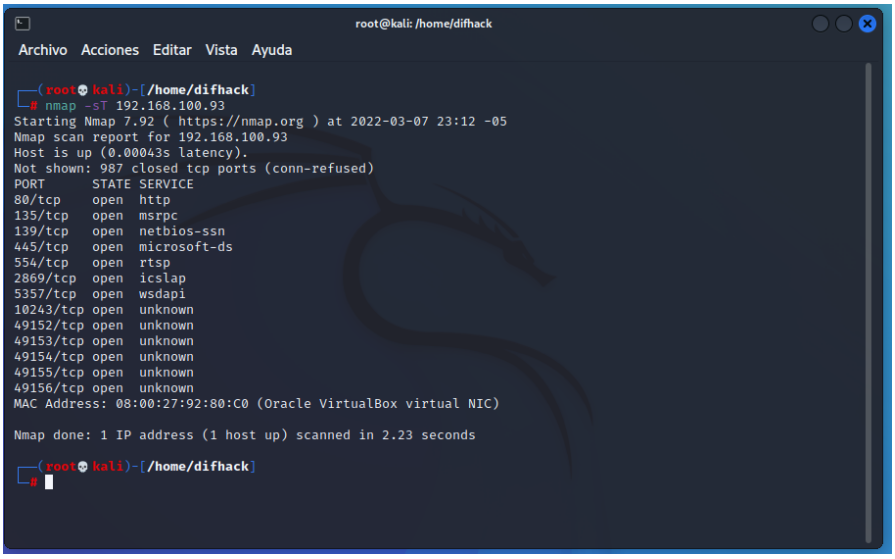
Figura 8. IP de maquina Windows (victima)



Fuente : Autor

La figura 9 muestra la utilización de la aplicación nmap en Kali Linux, permitirá visualizar en concreto que servicios y puertos tiene abiertos la maquina windows para perpetrar el ataque, para eso escribimos la siguiente línea de comando Nmap –sT 192.168.100.93, se utiliza un modificador –sT, para visualizar los servicio y puertos abiertos

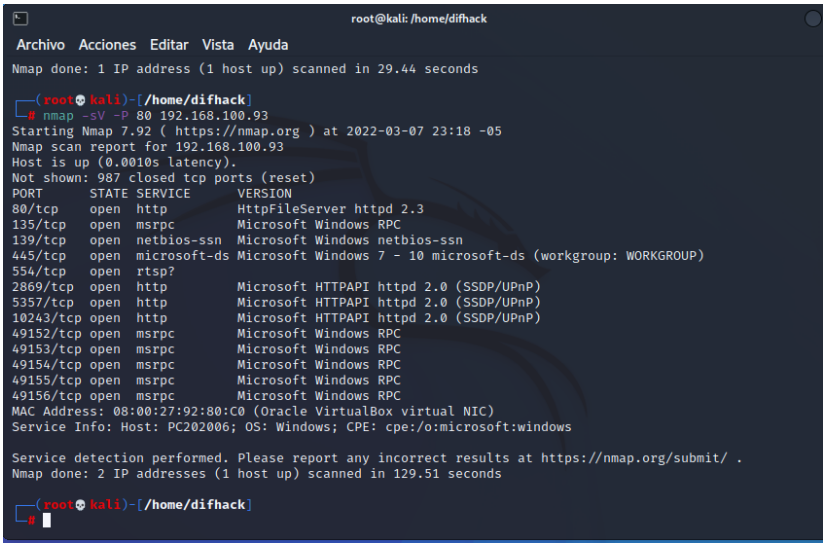
Figura 9. Verificación de servicios y puertos abiertos windows



Fuente : Autor

Mediante el escaneo se encontraron varios puertos abiertos, en especial el puerto 80/TCP servicio HTTP , como muestra la **figura 10** la línea digitada en la consola es de gran potencia y ayuda a identificar la versión de los servicios. La línea escrita en nmap –Sv –P 80 192.168.100.93 el digitador sV permite encontrar la versión que corre por el puerto, una vez ejecutado notamos gran cantidad de puertos abiertos con sus respectivos servicios, identificamos que el sistema operativo que corre en la maquina es windows 7, que por el puerto 80/TCP, existe una comunicación hacia el Httpfileserver Httpd 2.3 y demás puertos que pueden ser materia de vulnerabilidades y explotación de un atacante.

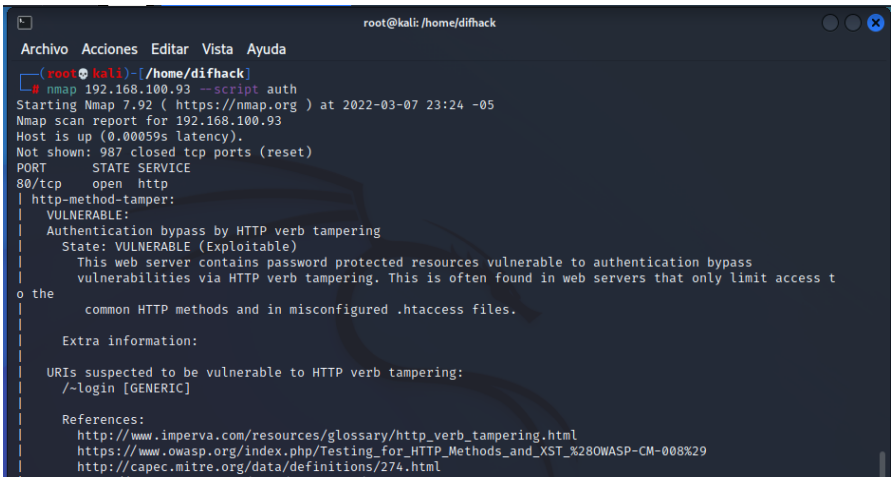
Figura 10. Identificado la versión de los servicios del puerto 80



Fuente : Autor

La figura 11, se evidencia la ejecución de una herramienta Script, viene integrada en nmap y ayuda a identificar y validar si dentro de los servicios que corren hay algún sistema que ejecute algún servicio de autentificación que puede ser clave a la hora de atacar, para eso vamos a escribir lo siguiente **Nmap 192.168.100.93 –script auth**

Figura 11. Ejecución de scrip de identificación de servicios con autentificación

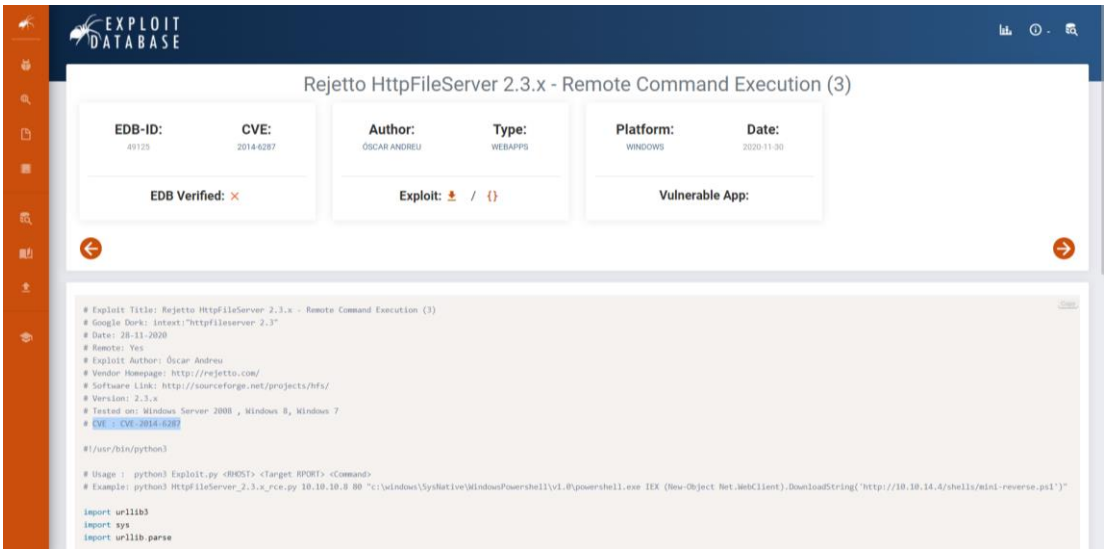


Fuente : Autor

En la Figura11 , también se logró identificar diferentes servicio y el estado del puerto 80/TCP http: vulnerable omisión de autentificación , identificamos vulnerabilidades Por manipulación de verbos HTTP, Estado: Vulnerable (Explotable) Por esta razón y por la investigación realizada se identifico que el puerto 80, es potencialmente explotable por su estado además el Rejjeto es el que genera el bug y abre el puerto 80 además se identifica que no está bloqueado por ningún firewall.

La figura 12, muestra el resultado de la busque de Rejetto en exploit db, encontrado que es potencialmente explotable y tiene código CVE asignado 2014- 6287, específicamente denominada Rejjeto HttpfileServer 2.3x – Remote Command Excution, se identifica que las maquinas explotables son de tipo windows.

Figura 12. Buscando rejetto en Exploit DATABASE



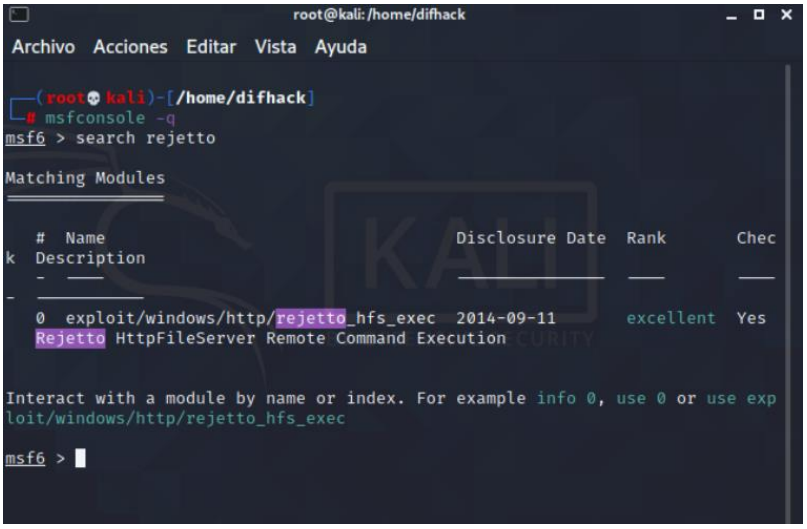
Fuente : Autor

La figura 12, muestra el resultado de la busque de Rejetto en exploit db, encontrado que es potencialmente explotable y tiene código CVE asignado 2014- 6287, específicamente denominada Rejjeto HttpfileServer 2.3x – Remote Command Excution, se identifica que la maquina explotable son de sistema operativo windows.

Luego de hacer una serie de investigaciones y con la información que nos arrojo la exploit data base, ya identificamos plenamente la vulnerabilidad según el código encontrado, nos disponemos a explotarla mediante la herramienta Metasploit framework.

La figura 13. Muestra cuando se ejecuta en el terminal de Kali Linux la línea de comando Msfconsole – q para abrir nuestro Metasploit, luego escribimos search Metasploit , esto lo que hace es una búsqueda exhaustiva en la base de datos para ver que exploit están disponibles para poder explotar la vulnerabilidad.

Figura 14. Muestra el exploit disponible para la vulnerabilidad.

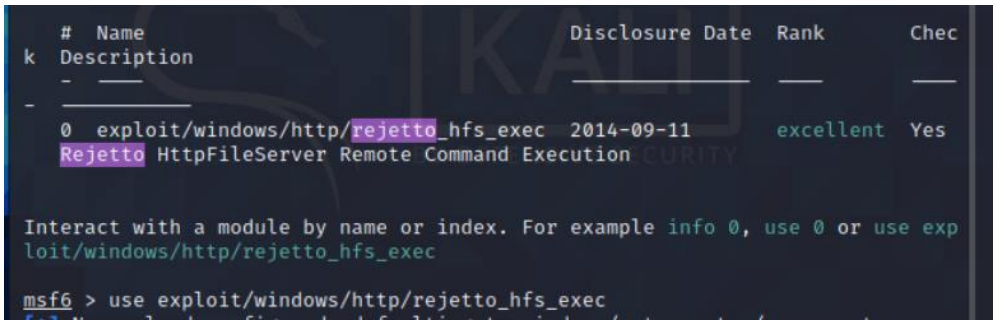


Fuente : Autor

La figura 14 muestra el exploit que podemos usar además indica que la vulnerabilidad rejetto del servidor corre en la maquina windows.

Ahora es tiempo de usar el exploit , para eso vamos a escribir la siguiente línea, use exploit/windowshttp/rejetto_hfs_exec, como muestra la **figura 17**, estamos dando la orden de ingresar al archivo raíz del exploit.

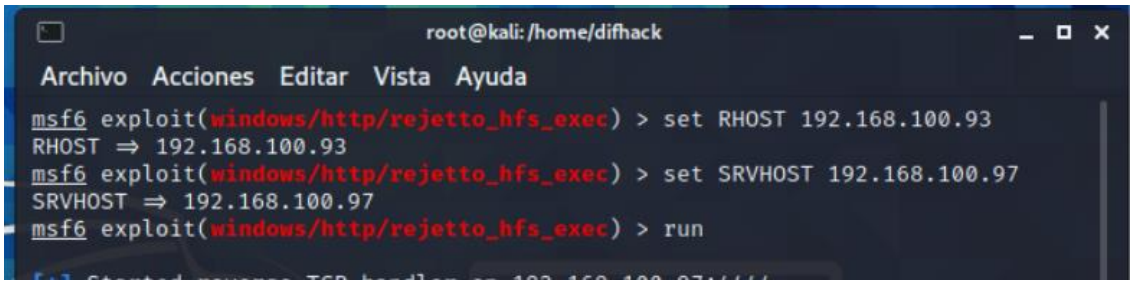
Figura 15. Cargue de exploit



Fuente : Autor

Es momento de asignar las IP de la maquina atacante y de la víctima, para eso vamos a utilizar el comando set, tal cual y se muestra en la **figura 18.**

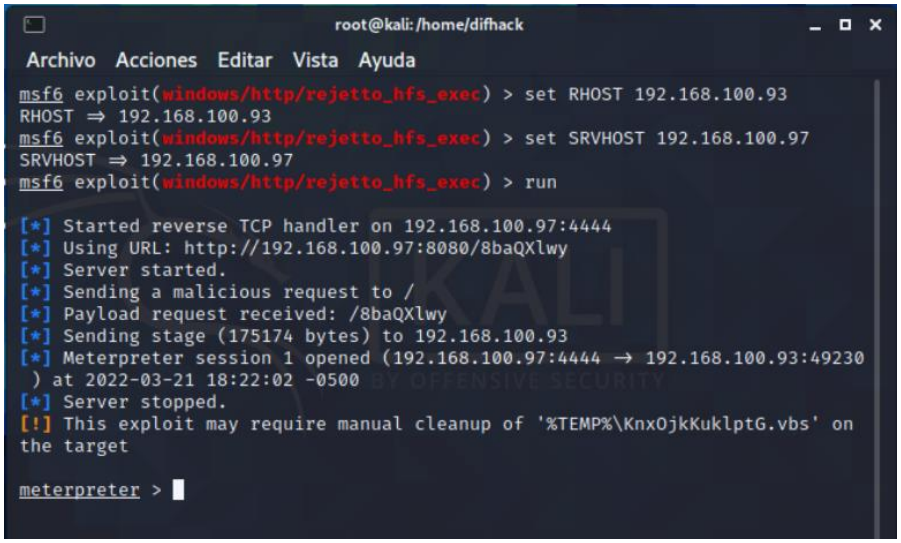
Figura 18. Configurando IP maquina atacante y víctima.



Fuente : Autor

Ya esta todo listo para desencadenar el ataque, para eso escribimos run o exploit y explotara el ataque, a raíz de esto se genera el Shell reversa y se crea una sesión meterpreter, hemos conseguido penetrar el sistema y como se muestra en la **figura 19** estamos en el equipo windows víctima.

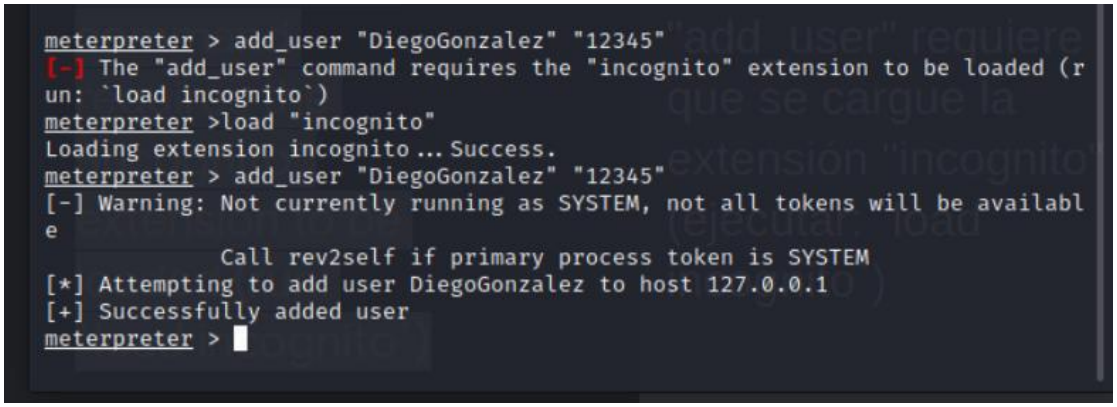
Figura 19. Ejecutando exploit - Shell reversa y Session Meterpreter



Fuente : Autor

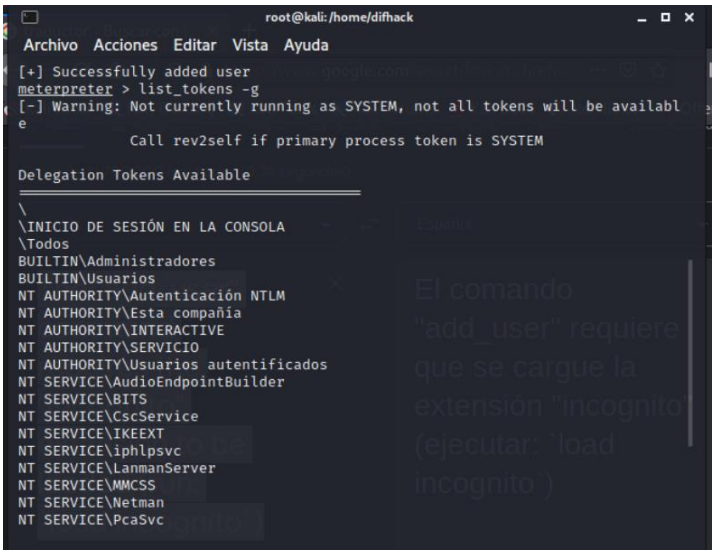
Ya dentro del sistema necesitamos crear el usuario administrador en el pc víctima, debemos usar la app en modo incognito, de esta forma podremos crear usuario y escalamos privilegios de seguridad, el comando que se debe usar es add_user “usuario” password” y enter para crear como se muestra en la **figura 20**.

Figura 20. Creando el usuario administrador PC Victima



En la Figura 20, se observa la línea de comando list_token -g la cual enlista los inicios de sección del sistema y la cual podremos desde aquí asigna al grupo de administradores un usuario de atacante.

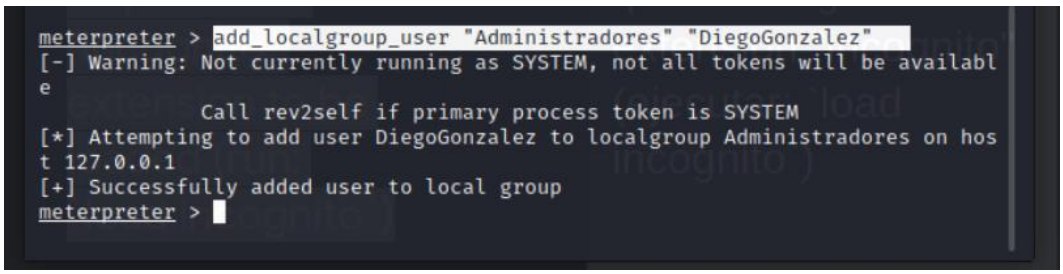
Figura 20. Privilegios como administrador



Fuente : Autor

Para conseguir asignarle un usuario al grupo administrador debemos utilizar el comando add_localgroup_user”administradores”DiegoGonzalez” como se enseña en la figura 21.

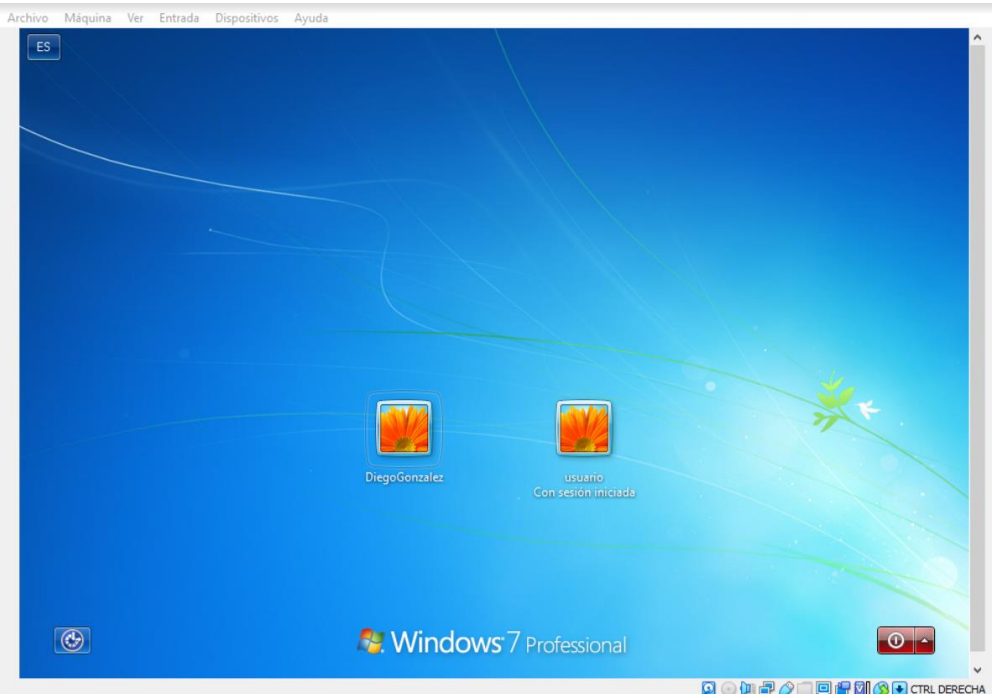
Figura 21. Creando el Usuario de administrador en el inicio de sección



Fuente : Autor

Para verificar si efectivamente el ataque tuvo éxito y todo salió bien, nos dirigimos a la máquina de la victima de windows y verificamos los usuarios activos. Como se muestra en la **figura 22,** se creo el usuario con contraseña y la penetración al sistema fue exitosa. Todo el ataque se realizó debido al puerto 80 que se encontraba abierto, esto fue a causa del servidor web rejetto que abrió el puerto cuando fue ejecutado en la maquina y creo la fuga de información en la organización.

Figura 22. Usuario administrador creado en la maquina W7



Fuente : Autor

5. ANALISIS BLUE TEAM DE ACUERDO CON SITUACION PROBELMA

Todo el ataque se realizó debido al puerto 80 que se encontraba abierto, esto fue a causa del servidor web rejetto que abrió el puerto cuando fue ejecutado en la maquina y creo la fuga de información en la organización. Mediante el desarrollo de la actividad se logro el objetivo de identificación de la vulnerabilidad que estaba permitiendo la fuga de información en la empresa, en ese sentido se dan a conocer diferentes herramientas para la identificación de sistemas, puertos activos, servicios y usuarios.

Para el desarrollo de las actividades propuestas en la **Unidad 3**, Análisis y Contención en Blue Team, se realizan las lecturas correspondientes para esta unidad y que comprende los temas de Contención de ataques; Hardening; Sistema SIEM (Información de seguridad y Gestión de Eventos); Herramientas Software y Hardware para la Contención de Ataques; además de las consultas realizadas en la Web para profundizar los temas, se finaliza el proceso de aprendizaje de esta unidad llevando a la práctica, el desarrollo de actividades que minimicen las vulnerabilidades del sistema y evitar de esta manera posibles ataques informáticos.

HARDENING: Conjunto de procesos, actividades u acciones que son realizadas o ejecutadas por el administrador del sistema operativo, con el fin de robustecer al extremo la seguridad de los equipos de informática. La finalidad del Hardening es evitar que se lleve a cabo un ataque y actuar de manera rápida y efectiva para frenarlo y así salvaguardar la información o los datos que se manejan.

PRACTICAS DE HARDENING:

- ✓ Verificar todas las configuraciones relacionadas con la seguridad del equipo, para comprobar su debida activación y en caso de no estarlo corregir la situación.
- ✓ Verificar las configuraciones y activaciones de las actualizaciones automáticas.
- ✓ Verificar si hay instalados programas de seguridad, entre ellos antivirus, antispyware o antispam.

- ✓ Verificar todas las claves que se manejen dentro del equipo para determinar si son las correctas o de lo contrario proceder a cambiarlas por claves más complejas.
- ✓ Verificar el manejo de todos los programas que se encuentren instalados en el equipo, determinando el uso y quien los maneja.
- ✓ Verificar las configuraciones relacionadas con la acción Acceso Remoto, limitando su uso y la cantidad de usuarios que pueden ejecutar esta acción.
- ✓ Verificar las configuraciones relacionadas con las cuentas de los usuarios.
- ✓ Verificar las configuraciones relacionadas con los backup, con el fin de que se hagan copias de seguridad.
- ✓ Verificar la configuración de la red.
- ✓ Verificar si el sistema cuenta con aplicaciones específicas que permitan monitorear la red.
- ✓ Verificar si el sistema cuenta con implementación de auditorías.
- ✓ Verificar si el sistema cuenta con un sistema de detección de intrusos.
- ✓ Verificar la configuración de Firewall.
- ✓ Verificar que el sistema operativo ha sido instalado de manera segura y correcta.

SISTEMA SIEM (Información de Seguridad y Gestión de Eventos)

Tecnología del tipo software que puede detectar, responder y contrarrestar o neutralizar amenazas informáticas de manera muy rápida. Su objetivo principal y de acuerdo con su concepto es la evitar y frenar a toda costa que los sistemas de información sean atacados. Esta herramienta es capaz de prevenir los ataques antes de que se realicen. La importancia de este tipo de tecnología radica, en que a diario surgen miles y miles de formas para atacar todo tipo de sistemas de información, que pueden proceder bien sea de fuentes internas o externas.

CARACTERISTICAS DE UN SISTEMA SIEM

- ✓ Recolectar información de diferentes dispositivos.
- ✓ Normalizar la información recolectada, organizándola por fecha y hora, para que sea más fácil realizar las búsquedas en posibles listas u otro tipo de archivos a la hora de necesitarla.
- ✓ Analizar la información.
- ✓ Tener un módulo de gestión para que a través de este se puedan administrar las soluciones que se generen por amenazas.

HERRAMIENTAS PARA LA CONTENCION DE ATAQUES

- ✓ FIREWALL HARDWARE
- ✓ FIREWALL SOFTWARE
- ✓ ANTIVIRUS

FIREWALL HARDWARE: dispositivo físico electrónico externo de red y autónomo que conecta diferentes redes gracias a una interfaz de red integrada. Este cortafuego revisa todos los datos que ingresan de internet, dejando pasar los paquetes de datos que son seguros y bloquea automáticamente los paquetes de datos que representan peligro, garantizando con ello la seguridad de la red. Este tipo de cortafuego siempre está activado, requieren de una configuración experta, se usan principalmente para proteger de manera segura y robusta a las redes locales de empresas, para muchos son dispositivos complejos y la administración de los mismos suele ser también compleja de realizar.

FIREWALL SOFTWARE: es una aplicación que se puede instalar en una computadora, también se les conoce como desktop firewall o software firewall, son aplicaciones básicas que generalmente se instalan en pequeñas instalaciones como un equipo de cómputo en un hogar o en un lugar de trabajo muy pequeño. La función de este cortafuego es la monitorear todos los puertos abiertos en un servidor web y

verifica la información de cada puerto. El firewall tiene una lista de aplicaciones para ingresar a internet en ciertos puertos por lo tanto si la aplicación está utilizando un puerto específico, el software verifica el contenido de los datos que están ingresando y si son seguros los dejara pasar hacia la computadora, pero si una aplicación no verificada intenta ingresar a la información el sistema bloqueara la información entrante y saliente y realizara una notificación al usuario que el programa está intentando acceder a internet.

Los firewall gratuitos se incluyen con el sistema operativo y normalmente son de uso personal, son fáciles de instalar, ya vienen activados, es la herramientas más básica debe tener todo PC para garantizar condiciones de seguridad básicas.

Se puede tener ambos firewall instalados e activados, puesto que el hardware protege al sistema del mundo exterior y el software protege al sistema de manera interna de otros sistemas que resulten ser dañinos para el mismo.

Entre los mejores Firewall gratuitos para sistemas Windows se encuentran:

- ✓ TinyWall
- ✓ Netdefender
- ✓ Glasswire
- ✓ PeerBlock

ANTIVIRUS: son aplicaciones diseñadas para prevenir, bloquear, detectar y eliminar archivos dañinos que se descargan en el computador cuando se navega por internet y que están diseñados para atacar, dañar y modificar un sistema informático, comprometiendo la seguridad de este. Su función es la de proteger el sistema de los virus que existen y eliminar este tipo de amenazas.

La instalación de un buen antivirus junto con los firewall permite una mejor protección a un sistema informático y garantizan la seguridad del mismo.

Entre los antivirus reconocidos están:

- ✓ Bitdefender
- ✓ Norton
- ✓ Panda
- ✓ McAfee
- ✓ BullGuard

6. PRACTICA PARA EVITAR VULNERABILIDADES DEL SISTEMA (MAQUINA VIRTUAL WINDOWS 7 64 bits)

Para evitar vulnerabilidades en el sistema se desarrollan las siguientes acciones:

- ✓ Activar Cortafuegos.
- ✓ Activar Windows Defender.
- ✓ Activar Actualizaciones Automáticas.

Tener en cuenta las recomendaciones que arroja el sistema:

Instalar los correspondientes parches de seguridad, aunque el soporte técnico de Win7 finalizo el 14 de enero de 2020, de todas maneras, se lleva a cabo el proceso de instalar todas las actualizaciones del sistema operativo, garantizando con ello la seguridad del sistema y minimizando los riesgos de vulnerabilidad del mismo.

7. CONCLUSIONES

Al finalizar el desarrollo del presente informe se concluye que:

- ✓ La seguridad de un sistema informático es tema de vital importancia dentro de cualquier organización, ya que garantiza la protección de los datos o información manejados dentro de la misma.

- ✓ En toda organización es necesario que se constituya o exista el área de seguridad informática, conformada por el personal idóneo, para llevar a cabo todas las tareas que impliquen única y exclusivamente, el manejo de la seguridad del sistema informático.

- ✓ El equipo o personal encargado del área de seguridad, en todo momento deberá tener plenos conocimientos, de todos los temas en cuanto a seguridad informática se requieren, para el adecuado manejo y administración de la seguridad del sistema.

- ✓ El equipo o personal encargado de la seguridad del sistema, deberá tener las habilidades necesarias para proponer y ejecutar estrategias, que permitan neutralizar los ataques informáticos, utilizando para ello todas las herramientas y acciones adecuadas que permitan frenar los mismos.

- ✓ Al hacer parte de un equipo de trabajo para la seguridad de un sistema, o parte del personal responsable de la seguridad del sistema, se requiere que se tenga conocimiento sobre las normas que se tipifican como delitos informáticos, con el fin de no incurrir en ese tipo de conductas, garantizando con ello la seguridad de la información y la integridad de quienes están relacionados estrechamente, con el sistema informático.

8. RECOMENDACIONES

Con el fin de mejorar la seguridad de los sistemas informáticos dentro de cualquier tipo de organización se recomienda:

- ✓ La creación de un equipo de trabajo, con personal capacitado para el manejo exclusivo de la seguridad del sistema, en caso de que la organización no maneje este tipo de recursos.

- ✓ Se propone la capacitación cada cierto tiempo, con el fin de que las personas encargadas del manejo de la seguridad del sistema estén actualizadas con todos los temas, que tienen que ver con seguridad informática.

- ✓ Se propone que el personal encargado de la seguridad establezca un manual para el desarrollo de buenas prácticas de seguridad, en las que apliquen todas las acciones y herramientas necesarias para garantizar la seguridad del sistema.

- ✓ Se propone la ejecución de auditorías para el equipo o área encargada de la seguridad del sistema, con el fin analizar cada una de las labores realizadas para mantener la seguridad del mismo y que permitan determinar si cumplen con los objetivos propuestos para tal fin.

- ✓ Se proponen capacitaciones para todos los usuarios del sistema, con el fin de educarlos en la importancia de la seguridad informática y en el manejo de herramientas sencillas que pueden manejar para contribuir al mejoramiento de la seguridad del sistema.

- ✓ Se propone al equipo de seguridad, llevar a cabo prácticas o procesos, que permitan la intrusión o penetración al sistema, con el fin de evaluar el nivel de seguridad en la red de la organización.

9. BIBLIOGRAFÍA

National Institute of standards. (s.f.). NATIONAL DATABASE VULNERABILITY. Recuperado el 20 de marzo de 2022, de https://nvd.nist.gov/vuln/detail/CVE-2014- 6287

HACKERUNA.COM. ¿Qué Es Hardening? {En línea} {16 de marzo de 2022} disponible en: (https://hackeruna.com/2018/04/18/que-es-hardening/).

GUILLÉN ZAFRA, José Luis. "Introducción al pentesting". Universidad de Barcelona, 2017 {En línea} {16 de marzo de 2022} disponible en (http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf)

SOFECOM. SIEM, La Tecnología Capaz de Detectar y Neutralizar las Amenazas Informáticas Antes de que Ocurran. {En línea} {16 de marzo de 2022} disponible en: (https://sofecom.com/que-es-un-siem/).

NSIT. ¿Qué es SIEM en Seguridad Informática? Alcance e Implementación {En línea} {En línea} {17 de marzo de 2022} disponible en: (https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/).

LEY 1273 DE 2009. Formato PDF. {En línea} {17 de marzo de 2022} disponible en: https://www.sic.gov.co/recursos_user/documentos/norma/Ley_1273_2009. pdf).

Crowdstrike. (2020). BLUE TEAM CYBERSECURITY DEFINED. Recuperado el 15 de marzo de 2022, de https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

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

CODIGO PENAL. Formato PDF. {En línea} {En línea} {17 de marzo de 2022} disponible en: (https://www.vertic.org/media/National%20Legislation/Colombia/CO_Codigo_Penal_Colombia.pdf).

Cyber Triaje. (s.f.). Free Incident Tools. Recuperado el 21 de Marzo de 2022, de https://www.cybertriage.com/landingincidentresponse

ENTER.CO. Detrás de Buggly: la historia de la fachada Andrómeda. {En línea} {17 de marzo de 2022} disponible en: (https://www.enter.co/cultura-digital/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/).

BYTE MIND. Escaneando la Red con Nmap en Kali Linux. {En línea} {17 de marzo de 2022} disponible en: https://byte-mind.net/escaneando-la-red-con-nmap/).

IPS: Sistema de Prevención de Intrusos. (s. f.). Infotecs.mx. Recuperado 4 de octubre de 2022, de https://infotecs.mx/blog/ips-sistema-de-prevencion-de_intrusos.html

Guía de referencia de Nmap (Página de manual). (s/f). Nmap.org. Recuperado el de 11 de marzo de 2022, de https://nmap.org/man/es/index.html

NVD - CVE-2014-6287. (s. f.). Nist.gov. Recuperado 22 de marzo de 2021, de https://nvd.nist.gov/vuln/detail/CVE-2014-6287

10. LINK DEL VIDEO DE SUSTENTACIÓN

https://www.youtube.com/watch?v=XFSM6q-Npbs