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

ELABORADO POR:

MAYERLY ROCÍO ENRÍQUEZ LÓPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

SEMINARIO ESPECIALIZADO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD

ARMENIA, QUINDIO

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

ELABORADO POR:

MAYERLY ROCÍO ENRÍQUEZ LÓPEZ

TRABAJO ESCRITO

TUTOR

JOHN FREDDY QUINTERO

Director de curso.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

SEMINARIO ESPECIALIZADO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD

ARMENIA, QUINDIO

RESUMEN

En el siguiente trabajo se dará a conocer los resultados obtenidos a través del desarrollo de las diferentes situaciones propuestas por la empresa The WhiteHose Security, con el fin de poner a prueba nuestros los conocimientos en seguridad informática y la forma en la que como profesionales actuaríamos ante posibles incidencias de seguridad informática.

En la primera situación la empresa pone a prueba nuestros conocimientos sobre las leyes colombianas que protegen la seguridad informática, también se realiza un montaje de un entorno de trabajo con Kali Linux y dos equipos más con Windows 7 en diferentes versiones, con el fin de usarlo para testing haciendo uso de las herramientas que ofrece este sistema operativo.

En la segunda situación, nos plantean un acuerdo de confidencialidad con algunas inconsistencias que violan la ley en muchos aspectos los cuales son identificados y se relaciona cada uno de los delitos en los que se estaría incurriendo.

En la Tercer situación, encontraras el desarrollo de un proceso de testing con el fin de identificar la vulnerabilidad utilizada por el atacante para penetrar nuestros sistemas y crear un usuario de tipo administrador. En este caso se mostrará cómo funciona la herramienta de escaneo de red Nmap, que nos permitió identificar el puerto por el cual entro el intruso a nuestro sistema.

En la cuarta y última situación, determinamos cómo actuar, que pasos seguir y que herramientas usar en el caso que estemos enfrentados a un ataque informático, exaltando la importancia de contar con planes de contención.

TABLA DE CONTENIDO

LISTA DE FIGURAS

GLOSARIO

DELITOS INFORMÁTICOS: es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. Ante el extendido uso y utilización de las nuevas tecnologías en todas las esferas de la vida (economía, cultura, industria, ciencia, educación, información, comunicación, etc) [1]

LEY: Regla o norma establecida por una autoridad superior para regular, de acuerdo con la justicia, algún aspecto de las relaciones sociales.[2]

CIBERSEGURIDAD: La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos. [3]

SOFTWARE: Se conoce como software, logicial o soporte lógico al sistema formal de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware. La interacción entre el software y el hardware hace operativo un ordenador (u otro dispositivo), es decir, el software envía instrucciones que el hardware ejecuta, haciendo posible su funcionamiento.[4]

VIRTUALBOX: Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual.[5]

VMWARE: Se trata de un sistema que permite operar con software, emulando a un sistema físico (un computador, un hardware, etc.) con unas características de hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a un computador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc. [6]

---

[1] (Fundación Wikimedia, 2020)
[2] (Languages.oup)
[3] (infosecuritymexico)
[4] (Fundación Wikimedia, 2021)
[5] (Fundación Wikimedia, 2021)
[6] (Fundación Wikimedia, 2021)

KALI LINUX: es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.[7]

BLUE TEAM: Equipo de seguridad informática que se encarga de la protección y defensa de la empresa, realizando una vigilancia constante de los comportamientos fuera de lo común que se den día a día, tanto a nivel de usuario como a nivel de redes y sistemas de información. También establecen las respuestas en caso de incidentes.[8]

RED TEAM: Es el equipo encargado de simular a los atacantes, haciendo uso de las mismas herramientas o similares a la de los atacantes con el fin de explotar las vulnerabilidades de seguridad informática, con el fin de dar las bases de información al equipo de blue team para que este sepa cómo defenderse ante posibles ataques.[9]

[7] (Fundación Wikimedia, 2021)
[8] (Unir La Universidad en Internet, 2020)
[9] (Unir La Universidad en Internet, 2020)

INTRODUCCIÓN

Como expertos en seguridad informática es de vital importancia como conocer que leyes y normas nos rigen en nuestro país con respecto a este tema, en Colombia todos los procesos penales descritos en el código penal que para el caso de seguridad de información se actualizo con la ley 1273 del 05 de enero de 2009.

Para este trabajo vamos a hacer uso de Kali linux que es una distribución de linux que está pensado en la auditoria de sistemas informáticos, por ende, tiene instaladas muchas herramientas para detección de vulnerabilidades en un sistema, los cuales serán de gran ayuda para la ejecución de nuestro escenario de trabajo.

Una de las herramientas con la que vamos a trabajar es Nmap que nos permite escanear la red en busca de puertos abiertos y aprovechar este para ejecutar ciertos comandos y crear un usuario administrados que nos dé total control de la maquina atacada.

Ninguna empresa está exenta a sufrir algún tipo de ataque de seguridad de la información y es de vital importancia contar con la ruta correcta de cómo proceder frente a estos, es por eso que las empresas pensando en el control de las incidencias de seguridad informática deben pensar en contar con un equipo especializado que les ayude con la detección de vulnerabilidades, cierre brechas de seguridad y establezca rutas de contención de ataques.

Existen varias tecnologías y herramientas que se han desarrollado para la contención de incidencias informáticas que les proporcionan a los especialistas de seguridad detectar, analizar, y ejecutar medidas que permitan evitar la propagación de los ataques. Como lo es SIEM o los diferentes programas de monitoreo que encontramos en el mercado tanto de uso gratuito como pago.

OBJETIVOS

OBJETIVO GENERAL

Desarrollar las actividades requeridas con las cuales se dé solución a cada una de las situaciones planteadas por la empresa The WhiteHose Security, con el fin de mostrar las capacidades profesionales en cuanto a seguridad informática se refiere.

OBJETIVOS ESPECÍFICOS

- ✓ Dar solución a la primera situación que plantea el montaje de un banco de trabajo para la elaboración de testing.
- ✓ Responder cada una de las preguntas sobre conocimientos básicos de seguridad informática
- ✓ Revisar acuerdo de confidencialidad entregado por la empresa y establecer las irregularidades legales que esté presente.
- ✓ Ejecutar Pruebas de intrusión en nuestro banco de trabajo para identificar las fallas de seguridad informática, que permitieron la intrusión del atacante.
- ✓ Establecer los pasos a seguir en caso de sufrir un ataque en tiempo real y que herramientas podemos usar como apoyo de nuestra labor como parte del equipo Blue Team de la empresa.

1. INFORME TECNICO

En el trascurso del tiempo laborado en la empresa The WhiteHose Security, se llevaron a cabo varias actividades enfocadas en entornos de trabajo los cuales fueron los siguientes:

1.1 SITUACIÓN PROBLEMA: MONTAJE BANCO DE TRABAJO

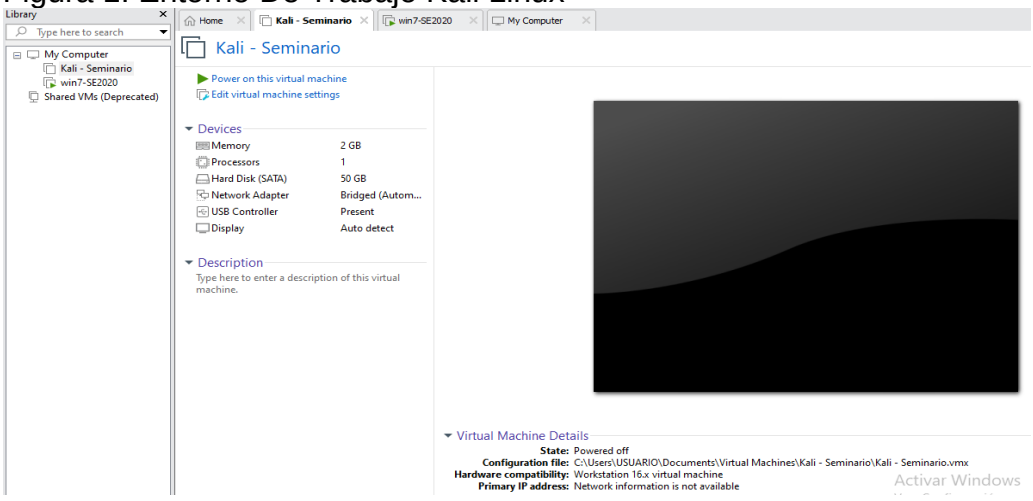
The Whitehouse Security requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de The WhiteHouse Security. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.

De manera simultánea The WhiteHouse security requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

- Montaje del Banco de Trabajo:

En una máquina virtual montamos los entornos de trabajo, uno con Kali linux que será nuestro sistema para hacer testeos de seguridad y otros dos equipos que simularán los equipos de la compañía los cuales tendrán instalados WIN 7 en diferentes versiones. En la Figura 1 se muestra la evidencia del entorno de trabajo Kali Linux.

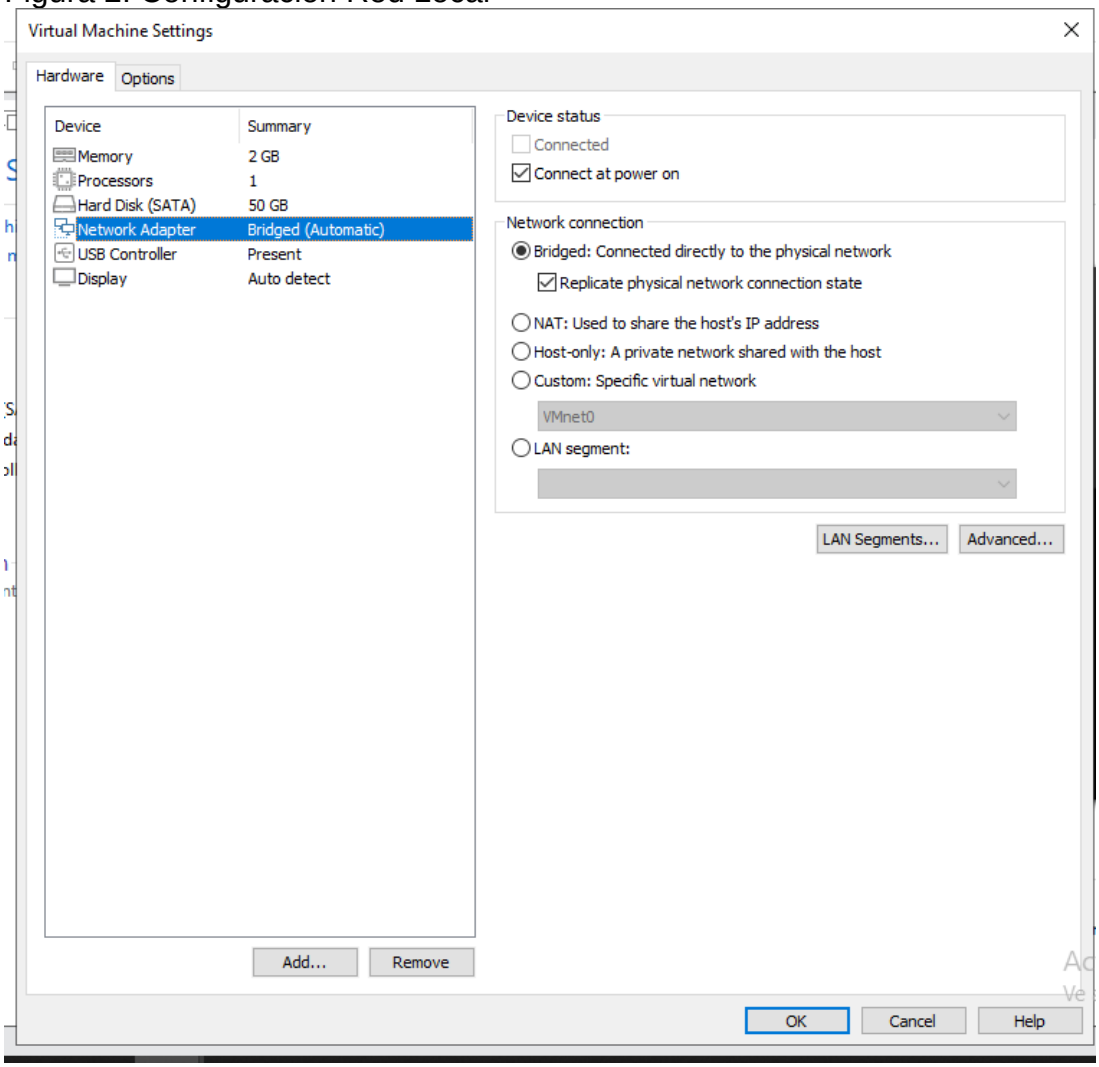
Figura 1. Entorno De Trabajo Kali Linux



Mayerly Rocío Enríquez López.

Configuración de a conexión a la red local, entramos a settings de la máquina virtual y seleccionamos la opción de conexión directa con la red física y que esta se replique en la máquina virtual, Evidencia Mostrada en Figura 2.

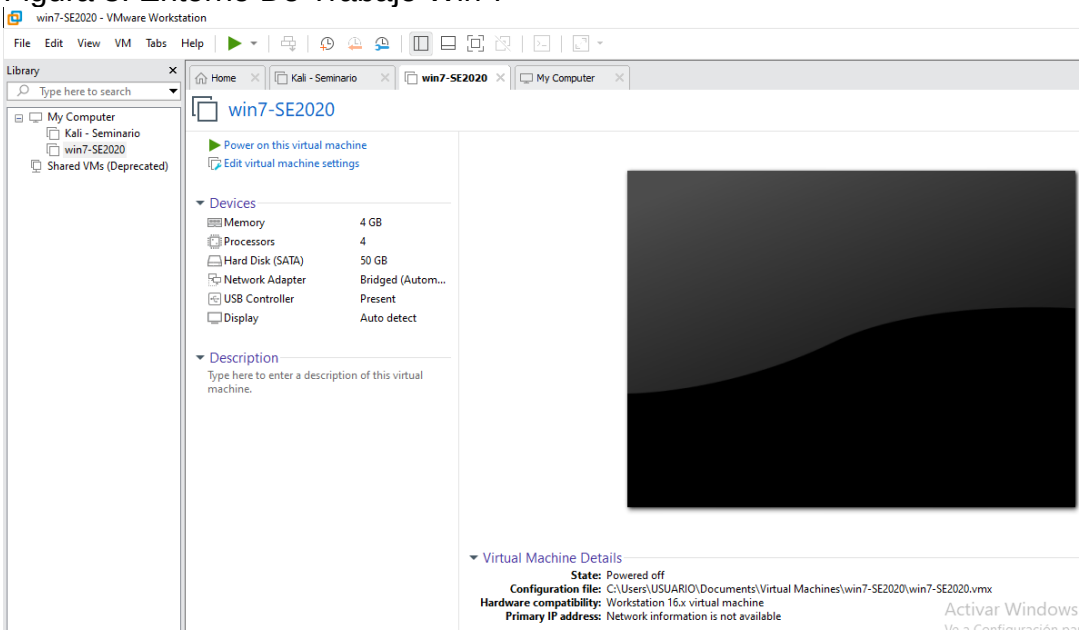
Figura 2. Configuración Red Local



Mayerly Rocío Enríquez López.

En la Figura 3 podemos ver como quedo configurado el entorno de Trabajo Windows 7 SE 2020

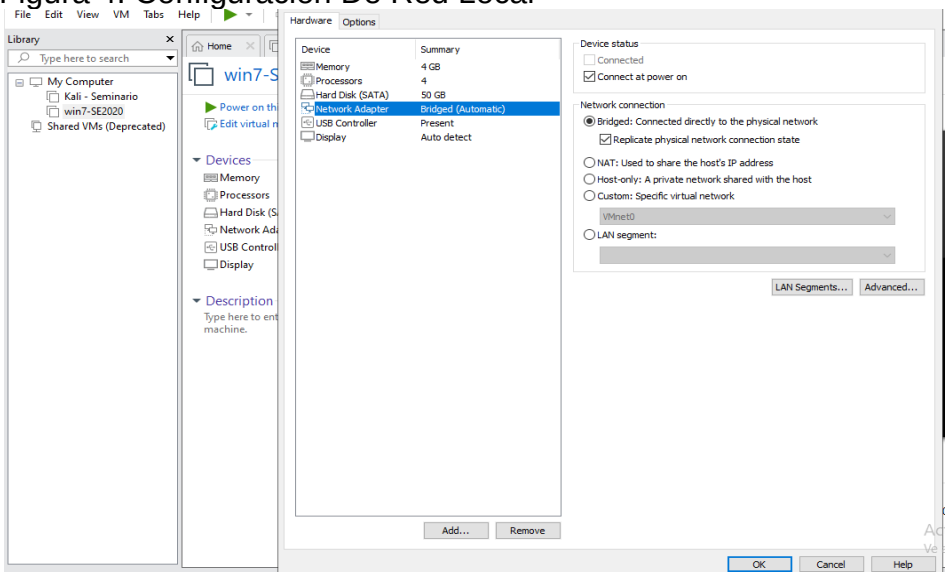
Figura 3. Entorno De Trabajo Win 7



Mayerly Rocío Enríquez López.

En la Figura 4 encontramos la configuración de la conexión a la red local.

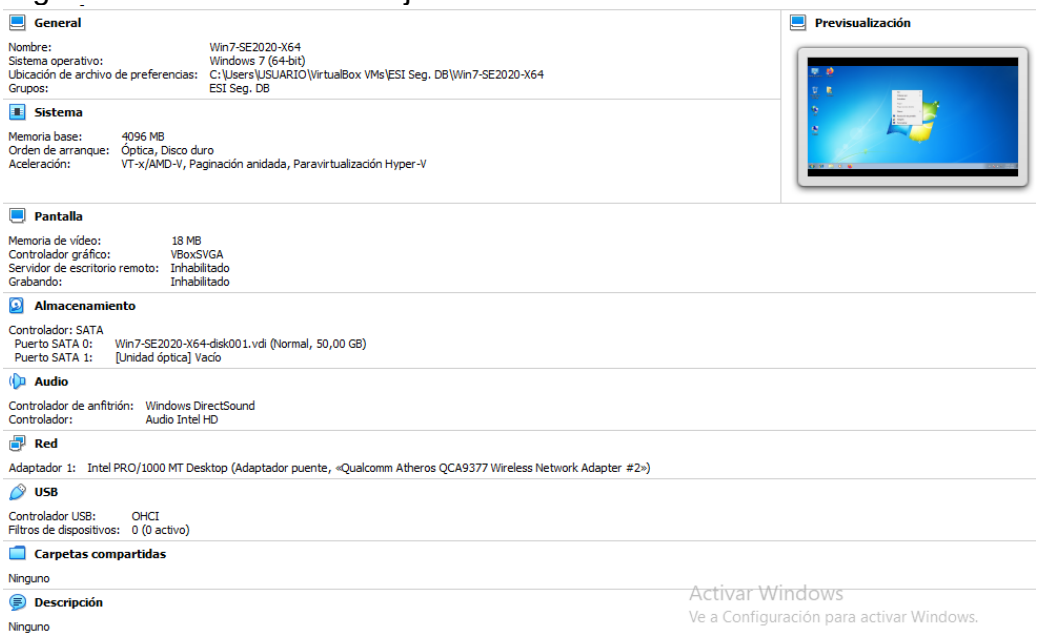
Figura 4. Configuración De Red Local



Mayerly Rocío Enríquez López.

En la Figura 5 encontramos las especificaciones del entorno de Trabajo Windows 7 64 BITS el cual se llevó a cabo en virtualbox.

Figura 5. Entorno De Trabajo Win 7 64 Bits

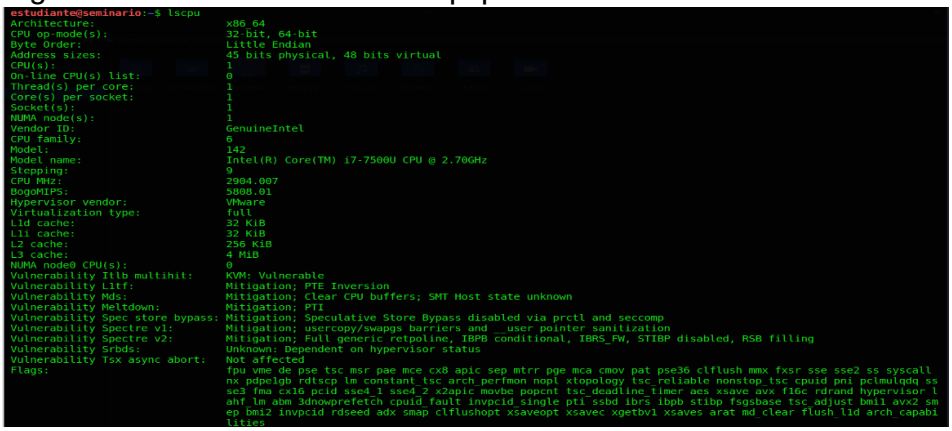


Mayerly Rocío Enríquez López.

Ahora vamos a consultar cada una de las características de los equipos configurados en las máquinas virtuales.

En la Figura 6 encontramos las características del sistema operativo KALI LINUX.

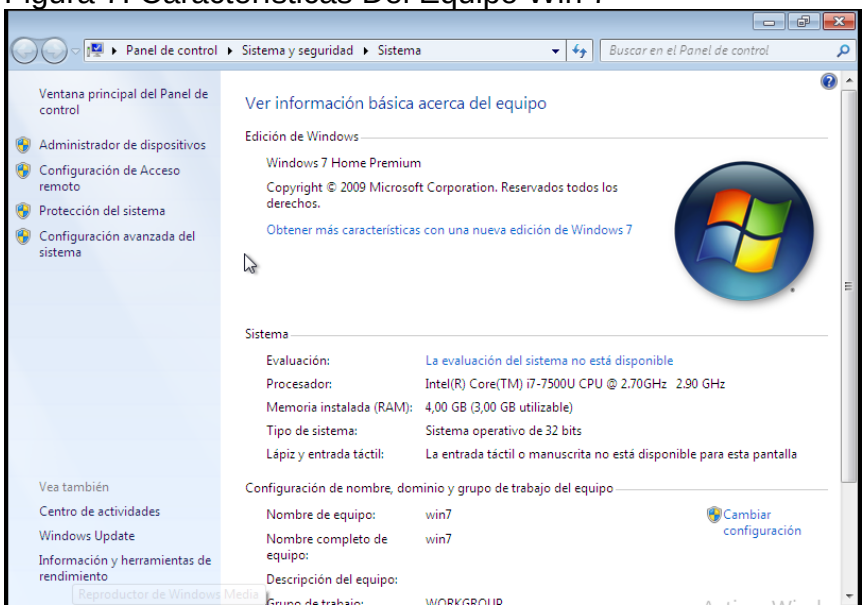
Figura 6. Características Del Equipo Kali Linux



Mayerly Rocío Enríquez López.

En la Figura 7 encontramos las características del sistema operativo WINDOWS 7 de 32 Bits

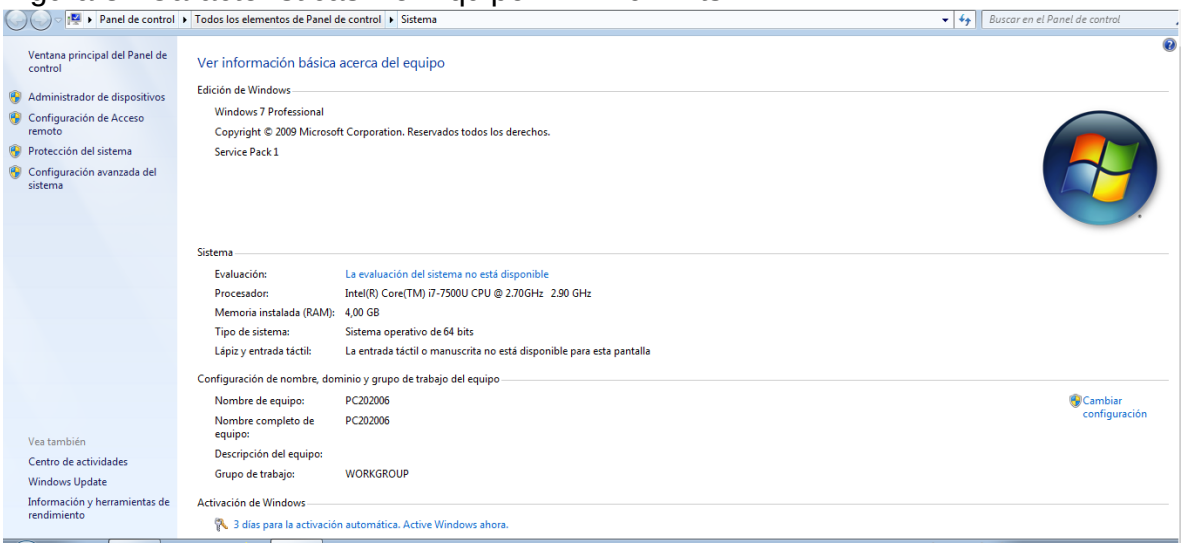
Figura 7. Características Del Equipo Win 7



Mayerly Rocío Enríquez López.

En la Figura 8 encontramos las características del sistema operativo WINDOWS 7 64 BITS.

Figura 8. Características Del Equipo Win 7 64 Bits

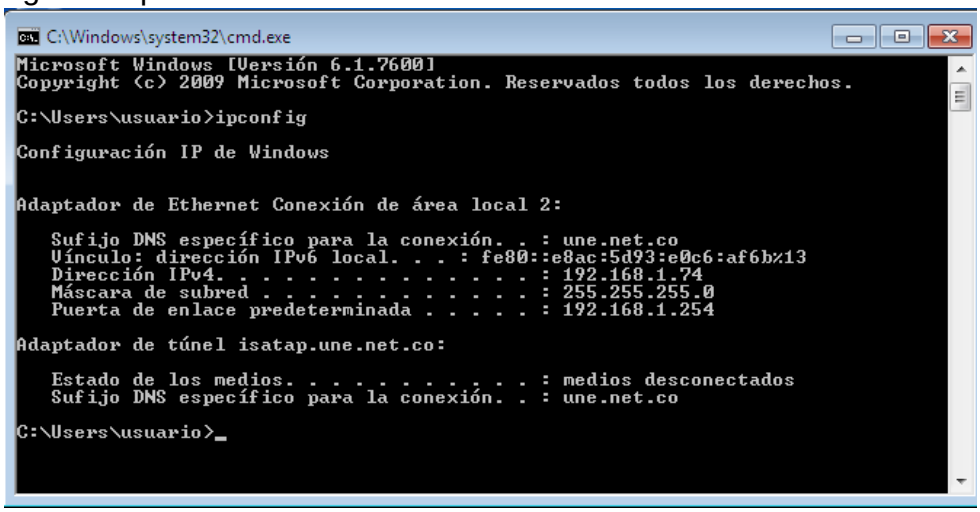


Mayerly Rocío Enríquez López.

Pruebas de conexión entra las maquinas Windows con Kali Linux.

KALI LINUX Y WINDOWS 7 32 Bits
Lo primero que debemos hacer para la prueba de conexión es identificar la IP de la máquina de Windows

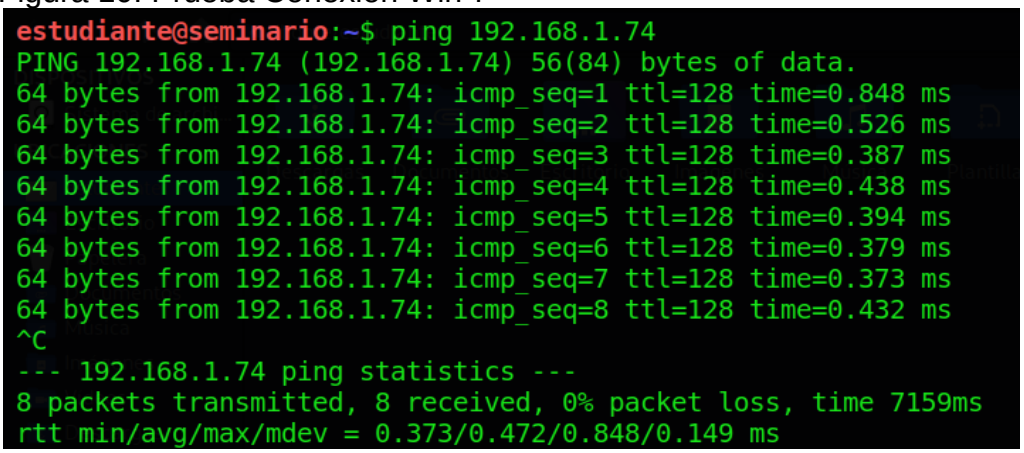
Figura 9. Ip Win 7



Mayerly Rocío Enríquez López.

En la siguiente Figura podemos ver como al hacer ping a la Ip obtenida de Windows 7 de 32 Bits este obtiene respuesta.

Figura 10. Prueba Conexión Win 7

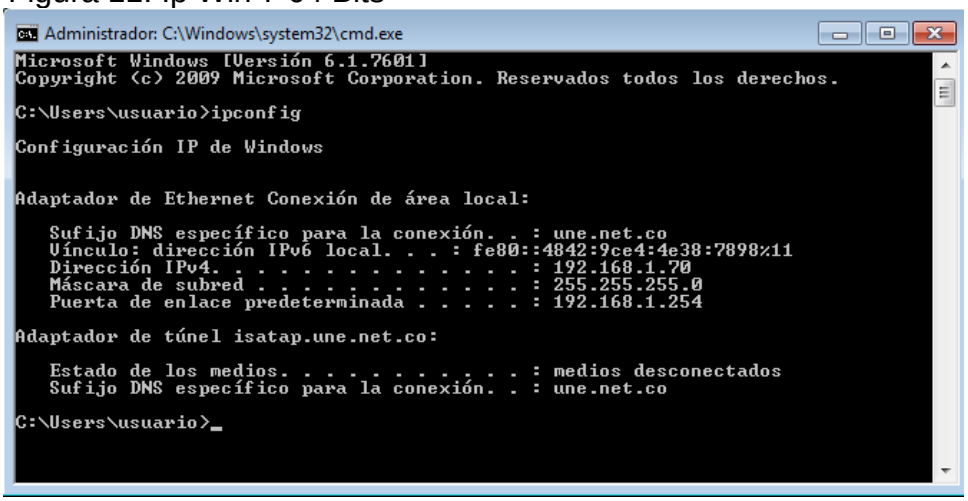


Mayerly Rocío Enríquez López.

KALI LINUX Y WINDOWS 7 64 BITS

Lo primero que debemos hacer para la prueba de conexión es identificar la IP de la máquina de Windows que se puede en la Figura 11.

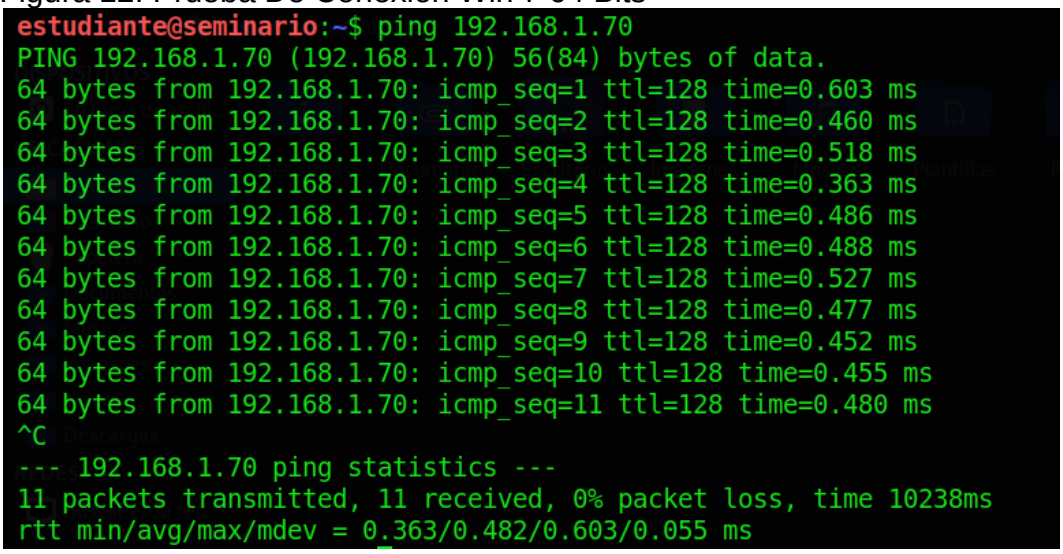
Figura 11. Ip Win 7 64 Bits



Mayerly Rocío Enríquez López.

A continuación, procedemos hacer ping a la IP de Windows 7 de 64 bits y vemos en la Figura 12 como obtiene respuesta.

Figura 12. Prueba De Conexión Win 7 64 Bits



Mayerly Rocío Enríquez López.

RESPUESTAS A ALGUNAS PREGUNTAS DE SEGURIDAD INFORMÁTICA.

LEYES, DECRETOS QUE EXISTEN ACTUALMENTE Y LAS CARACTERÍSTICAS PRINCIPALES DE CADA LEY EN COLOMBIA.

- LEY 1273 DEL 05 DE ENERO DE 2009

Esta ley modifica el codigo penal, dende se estipulan nuevas normas con respecto a la proteccion y preservacion de datos y los medios y/o herramientas tecnologicas que se utilecen para la recopilacion y almacenamiento de la misma, en esta ley se estipulan las acciones consideradas como delito y sus respectivos castigos tanto penales como fiscales.[10]

DEFINICION DE CADA UNA DE LAS ETAPAS DEL PENTESTING

Pentesting, es un método para la identificación de vulnerabilidades de un sistema informático y consta básicamente de 5 Fases:[11]

- Fase Recopilación de Información.

  Esta fase es la base para el proceso de auditoria del sistema con el que vamos a trabajar, se debe procurar conocer lo que más se pueda el sistema, una de las herramientas más comunes para recolección de información es Nmap, que nos permite hacer un rastreo de puertos para determinar que posibles puertos vulnerables.

- Fase Búsqueda de vulnerabilidades.
  Después de recopilar la información se debe proceder a identificar las vulnerabilidades, en esta fase debemos armar la estrategia de ataque al sistema, y establecer los objetivos de la misma, una de las herramientas usadas para este fin es Nessus, que es una de las herramientas más completas para la identificación de vulnerabilidades en el sistema, aunque es recomendable hacer este proceso de forma manual.

- Fase Explotación de vulnerabilidades.
  Después de detectar las vulnerabilidades, se debe iniciar uno de los procesos más complejos y es el de ejecutar acciones o ataques que permitan de una u otra forma violentar la seguridad de nuestro sistema, un ejemplo de ataque de que nos permite acceder al sistema

[10] (Congreso de Colombia, 2009)
[11] (Cyberseguridad.net, 2015)

es SQL injection, este ataque lo que nos permite es saltarnos el login de un sistema.

- Fase Post-explotación.
  La fase de post-explotación no es muy común en la implementación ya que consiste en tratar de acceder por completo al sistema obteniendo mayores privilegios sobre el mismo, tener acceso a la red y poder conectarnos a más sistemas que este conectados dentro de la misma red.

- Fase Elaboración de informes.
  En esta fase final, se procede a realizar un informe donde se debe presentar los resultados de la auditoria al cliente, recalcando la importancia de los datos obtenidos además de hacer énfasis de los procesos que cuentan con buen nivel de seguridad y los que deben mejorar, estos puntos a mejorar debe ir con sus respectivas acciones de mejora, como sugerencia este informe podría construirse en dos partes una con explicación más general y la otra con explicación técnica para los encargados de la parte informática de la empresa.

HERRAMIENTAS DE CIBERSEGURIDAD

Metasploit: es una herramienta diseñada para identificar vulnerabilidades, con el fin de evitar los riesgos de seguridad de la información.

Contiene información de programas que aprovechan las vulnerabilidades de un sistema, dichos programas se denominan exploits, además metasploit también permite crear exploits, cuyo propósito es realizar las pruebas necesarias para detectar los riesgos informáticos.[12]

Nmap: es una herramienta que al igual que Metasploit permite identificar las vulnerabilidades de un sistema, enfocada en detectar los dispositivos que se están ejecutando, encontrar puertos abiertos, además de servir como un sistema de monitoreo de host.[13]

Escanea los puertos disponibles y realiza pruebas enviando información y escuchando la respuesta para determinar los riesgos. Nmap identifica dispositivos que se ejecutan en la red.

[12] (Rizaldos, 2018)
[13] (marindelafuente, 2019)

OpenVAS: esta herramienta es de uso libre y al igual que las anteriores herramientas, este framework nos permite llevar a cabo la evaluación de vulnerabilidades de un sistema, esta herramienta ya se encuentra incorporada en Kali Linux.

Funciona a través de dos interfaces de servicio (OpenVAS Manager y OpenVAS Scanner) estos servicios son los encargados de llevar a cabo el filtrado y clasificación de los resultados del análisis y el escáner hace uso de una conexión de NVT que básicamente contiene las diferentes pruebas que sirven para detectar las posibles vulnerabilidades. [14]

Servicios en Línea:

Exploit DB: esta es una herramienta web, donde se almacenan diferentes exploits que podemos usar de forma gratuita para llevar a cabo nuestra prueba de penetración que ya hemos identificado previamente, exploit-db es un servicio público y por ende es importante que tengamos en cuenta que lo debemos usar para fines educativos o de testing y no para fines mal intencionados.

Esta herramienta te permite descargar los exploits que necesites para los testing de penetración además de poder escoger el sistema operativo en el que deseas correrlo, es una herramienta muy buena y de fácil manejo.

CVE: es una herramienta en línea que nos proporciona un listado de vulnerabilidades conocidas, donde a cada una le asigna un identificador único que adopto una nomenclatura estándar para hacer más fácil la identificación de las vulnerabilidades también anexa sus respectivas características, como por ejemplo versiones de software donde fueron identificadas y como poder solucionar cada una de ellas.

Cada nueva vulnerabilidad después de ser encontrada y para poder llevarse al listado de CVE, debe pasar por la revisión y análisis del equipo CVE, esto quiere decir que constantemente la información será actualiza.[15]

1.2 SITUACIÓN PROBLEMA: ANÁLISIS LEGAL

La organización WhiteHouse Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el

[14] (welivesecurity, 2014)
[15] (National Institute of standards, s.f.)

campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.
Para dar inicio, la organización WhiteHouse Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión "característica" de estos equipos.

Leyendo detenidamente en el acuerdo de confidencialidad se encontraron las siguientes irregularidades:[16]

- "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos", en este fragmente se están refiriendo a que alguna de la información suministrada para desarrollar el trabajo es obtenida a través de medios ilegales.

- Dentro de las obligaciones se encuentra esta anormalidad. "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros." Esta obligación es ilícita ya que al no denunciar posibles apropiaciones ilegales de información nos está haciendo cómplices de un delito, además de que muy posiblemente seamos nosotros quienes debamos desarrollar estas actividades ilícitas.

- Otra Obligación Ilícita es "Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.", es considerado ilegal porque primero que todo si tenemos conocimiento o nos enteramos de que en la empresa están ocurriendo procesos que atenten con la seguridad de la información de terceros para algún beneficio, debemos denunciar inmediatamente, ya que si no lo hacemos seriamos parte del delito.

[16] (UNAD - Universidad Abierta y a Distancia, 2020)

- “Responder por el mal uso que le den sus representantes a la información confidencial”. Me parece que por medio de esta obligación lo que buscan es librarse de toda responsabilidad de sus actos ilegales.

- “Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.” Esta obligación corrobora la intención de la anterior y es que nos hace responsable ante las autoridades de la información ilegal que encuentren en nuestro poder así esta haya sido suministrada por ellos.

- Esta es una irregularidad “Divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security.” ya que sabemos que si se trata de algo ilegal debemos denunciar inmediatamente y notificarle a la empresa seria darles un aviso del proceso de denuncia que se va hacer.

Teniendo en cuenta las irregularidades encontradas en el acuerdo de confidencialidad, los artículos de la ley 1273 que se podrían vulnerar en dicho acuerdo y porqué vulnera estos artículos de la ley 1273 son:

- Articulo 269C: interceptación de datos informáticos
- Artículo 269A: Acceso Abusivo A Un Sistema Informático.
- Artículo 269B: Obstaculización de sistemas informáticos o redes de comunicación
- Artículo 269F: Violación de datos personales.

Se está incurriendo en este delito ya que están manifestando que han obtenido información de forma ilegal, como por ejemplo las chuzadas es intercepción de información. Y el otro es claro que fue a través de acceso abusivo a sistemas de información.

A parte de esto la empresa con este acuerdo está tratando de librarse de cualquier penalidad que pudiesen tener en caso de que las autoridades encuentren dicha información ilegal en sus manos o en la de sus empleados.

Está claro que quien decida firmar dicho acuerdo y trabajar con esta empresa, y este no decida denunciar las ilegalidades que se estén cometiendo, será responsables de también del delito, puede ser por acción o por omisión.[17]

[17] (Congreso de Colombia, 2009)

1.3 SITUACIÓN PROBLEMA: ANÁLISIS RED TEAM

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. 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.

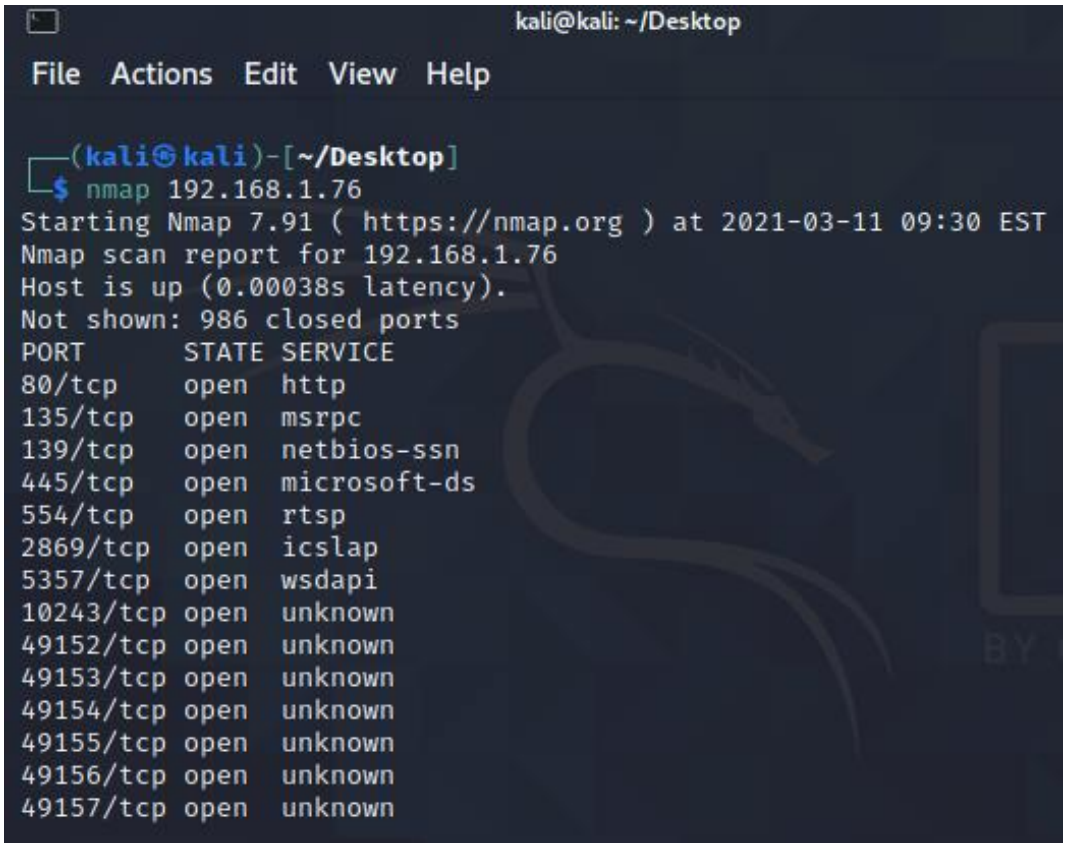
El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

Obteniendo información

La etapa inicial es obtener toda la información posible para iniciar las pruebas, contamos con que el equipo del pc que vamos atacar tiene instalado Windows 7 y tiene una herramienta llamada rejetto, al buscar en Google y YouTube se puede evidenciar que esta herramienta tiene un hueco de seguridad el cual le permite al atacante crear una reverse Shell y abrir una sesión de meterpreter

Ahora utilizo Nmap para escanear los puertos de la maquina con Windows 7 para obtener más información, el comando a ejecutar es el siguiente Nmap IP.

Figura 13. Consola Donde Se Ejecuta Comando Nmap



Mayerly Rocío Enríquez López.

En la imagen anterior vemos que el puerto 80 se encuentra abierto y por la investigación previa conocemos que Rejjeto abre el puerto 80, el puerto al parecer no se encuentra bloqueado por un firewall.

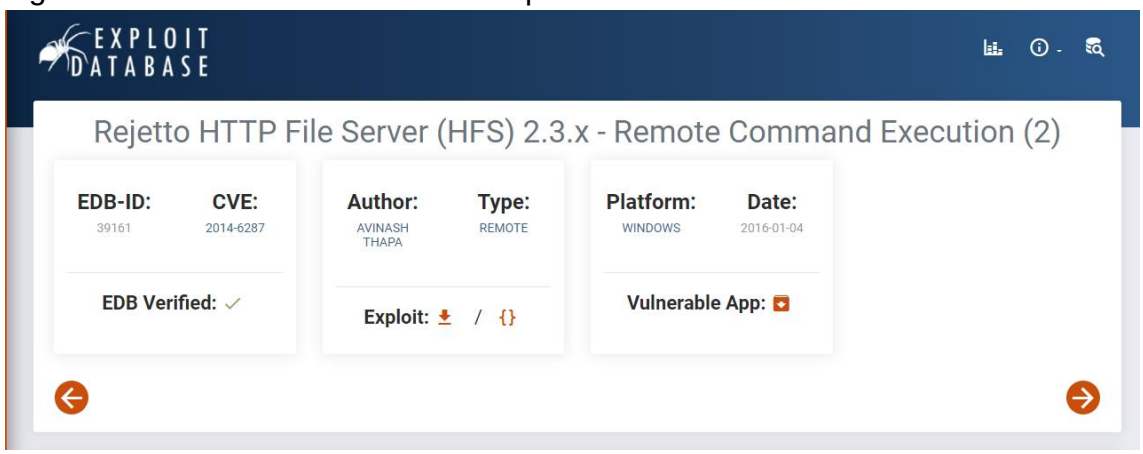
Análisis de vulnerabilidades y amenazas

Al buscar Rejjeto es exploit db encuentro que la aplicación tiene una vulnerabilidad Remote Command Execution.[18]

[18] (AVINASH THAPA, s.f.)

En la siguiente imagen vemos que ya tiene un código asignado por CVE 2014-6287 y que las plataformas vulnerables son las de tipo Windows.

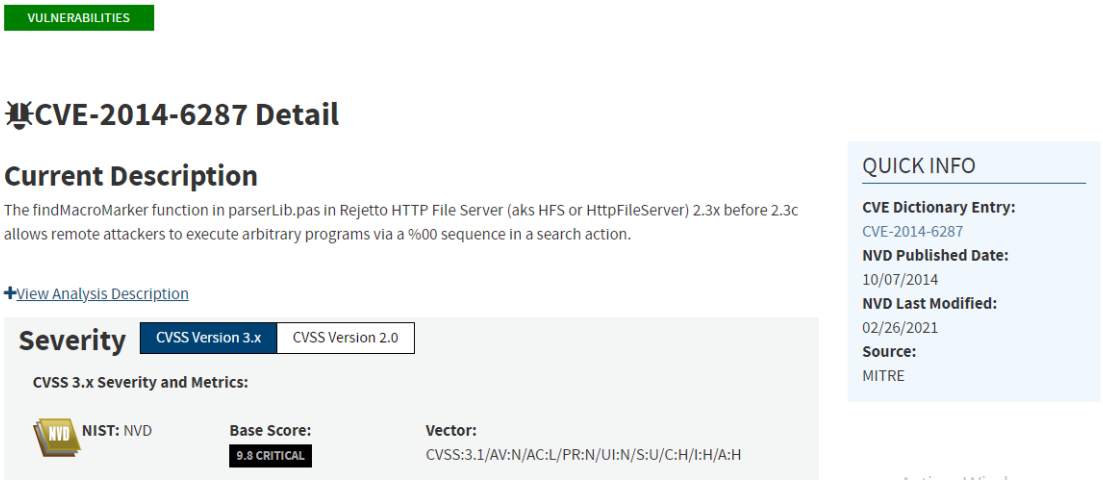
Figura 14. Análisis Por Medio De Exploit Database



Mayerly Rocío Enríquez López.

Ahora vemos en la imagen la descripción de la vulnerabilidad y como esta es aprovechada.

Figura 15. Descripción De La Vulnerabilidad Encontrada



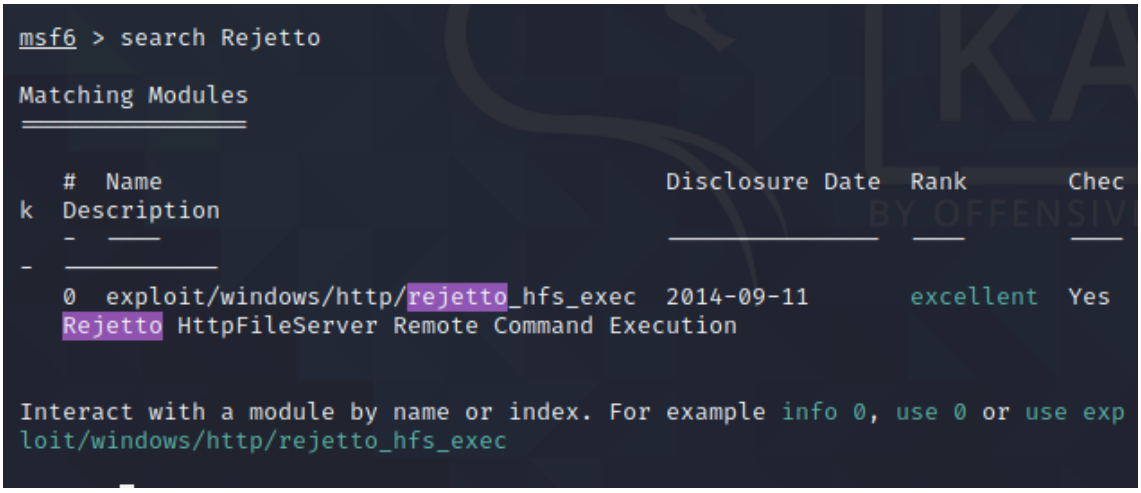
Mayerly Rocío Enríquez López.

Con la información anterior vamos a proceder a explotar la vulnerabilidad

Ahora podemos proceder a utilizar Metasploit framework para buscar que exploits se podrían utilizar para explotar la vulnerabilidad de Rejjeto, para eso abrimos desde Kali Linux Metasploit con el comando msfconsole –q o desde la interfaz de Kali

Ahora utilizamos el comando search Rejjeto el cual permitirá buscar en la base de datos interna de Metasploit.

Figura 16. Exploit que podemos utilizar para esta vulnerabilidad.



Mayerly Rocío Enríquez López.

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

Los datos que fueron utilizados para identificar el fallo de seguridad fueron

1- el nombre de la aplicación “Rejjeto”, con solo esta información ya es posible hacer una búsqueda en Google en buscar de posibles problemas de seguridad.
2- El tipo de sistema operativo en este caso Windows.
3- Finalmente indica que es posible conseguir una Shell reversa y una sesión de meterpreter.

con toda esta información y un poco de búsqueda en Google y las herramientas disponibles en Kali es posible obtener el contexto correcto de la situación y seguir con los testing.

HERRAMIENTA UTILIZADA PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA “MÁQUINA WINDOWS 7”

Las herramientas utilizadas para identificar los fallos de seguridad fueron

- ✓ Google (Permite encontrar si alguien más ya exploto la vulnerabilidad y si se encuentra en una base de datos como exploit db)
- ✓ Exploit db (Me indica que es posible la ejecución de comandos remotos con Metasploit)
- ✓ Nmap (Me permite saber que puertos se encuentran corriendo y que aplicaciones)
- ✓ Metasploit search (Me permite buscar los exploits disponibles para aprovechar la vulnerabilidad)

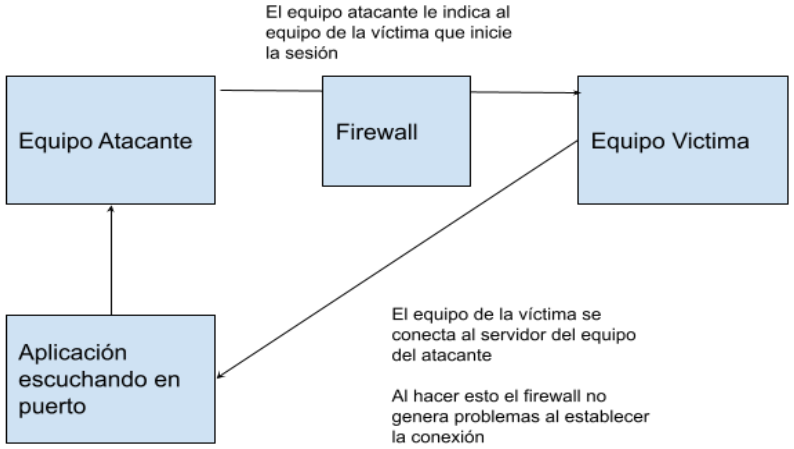
¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

El puerto que abre la aplicación del anexo es el 80 el cual es identificado también por Nmap.

CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64), HAGA USO DE GRÁFICOS PARA EXPLICAR EL ATAQUE.

Lo que entiendo que ocurre es que principalmente Kali no inicia de primero la conexión con el equipo que vamos atacar, es el equipo de la víctima quien recibe la orden y se conecta al equipo del atacante por lo que el firewall del sistema operativo no lo detecta y es posible hacer la conexión, cuando esta conexión se crea ya tenemos a nuestra disposición una Shell que puede ejecutar comando de manera remota. A continuación, se explica el procedimiento con un gráfico.

Figura 17. Gráfico Con El Proceso Del Ataque

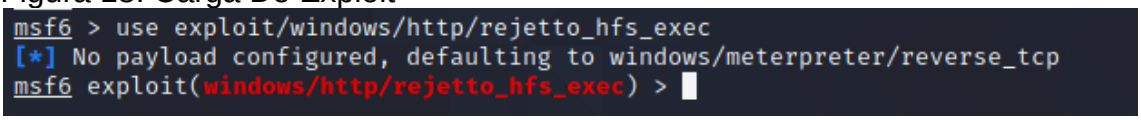


Mayerly Rocío Enríquez López.

PASOS Y EVIDENCIAS DE LA ACTIVIDAD DESARROLLADA PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS 7.

A continuación, vamos a explotar la vulnerabilidad para eso iniciamos Metasploit framework con msfconsole –q y cargamos el exploit que vimos en pasos anteriores, el exploit nos carga por defecto el payload.

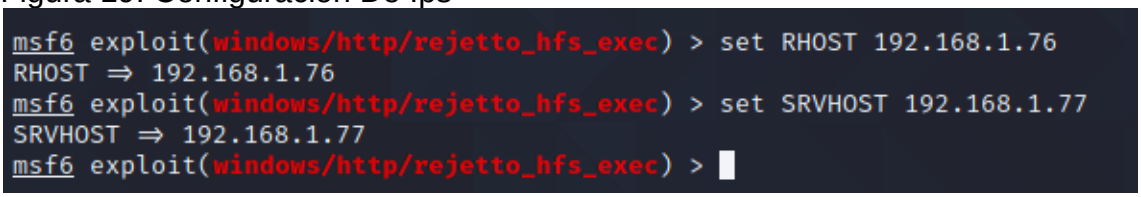
Figura 18. Carga De Exploit



Mayerly Rocío Enríquez López.

Ahora vamos a configurar la IP de la máquina del atacante y la IP de la máquina de la víctima para ello utilizamos el comando SET.

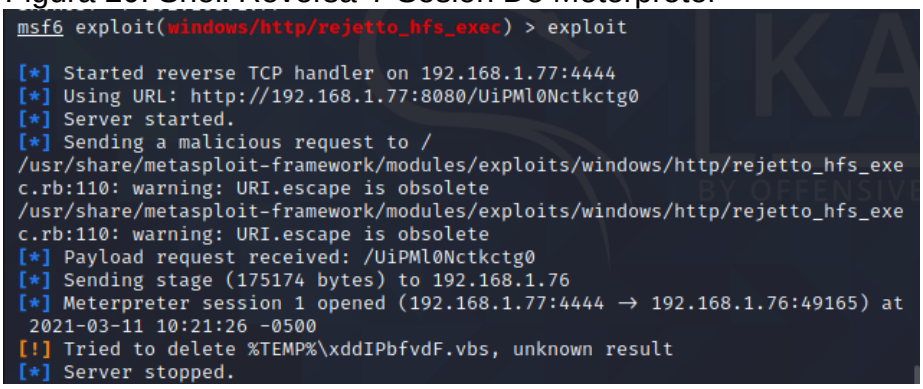
Figura 19. Configuración De Ips



Mayerly Rocío Enríquez López.

Luego que tenemos todo configurado escribimos el comando exploit el cual explota la vulnerabilidad, esto nos genera una Shell Reversa y una sesión del meterpreter, ahora estamos en el equipo de la víctima.

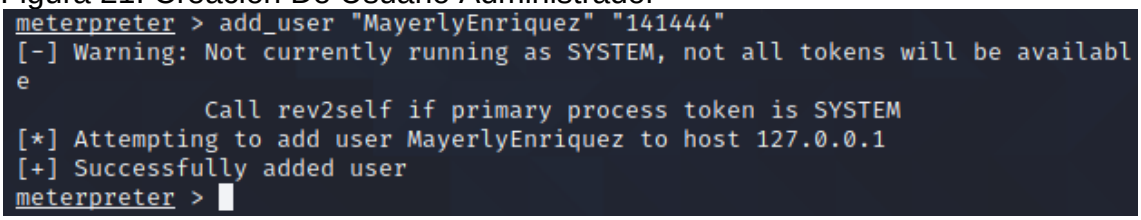
Figura 20. Shell Reversa Y Sesión De Meterpreter



Mayerly Rocío Enríquez López.

Creando el usuario administrador en el equipo de la víctima, para ello primero que todo vamos a utilizar la aplicación incognito la cual nos permite crear usuarios y agregarles grupos de seguridad, con el comando add_user “usuario” “password” lo podemos crear[19]

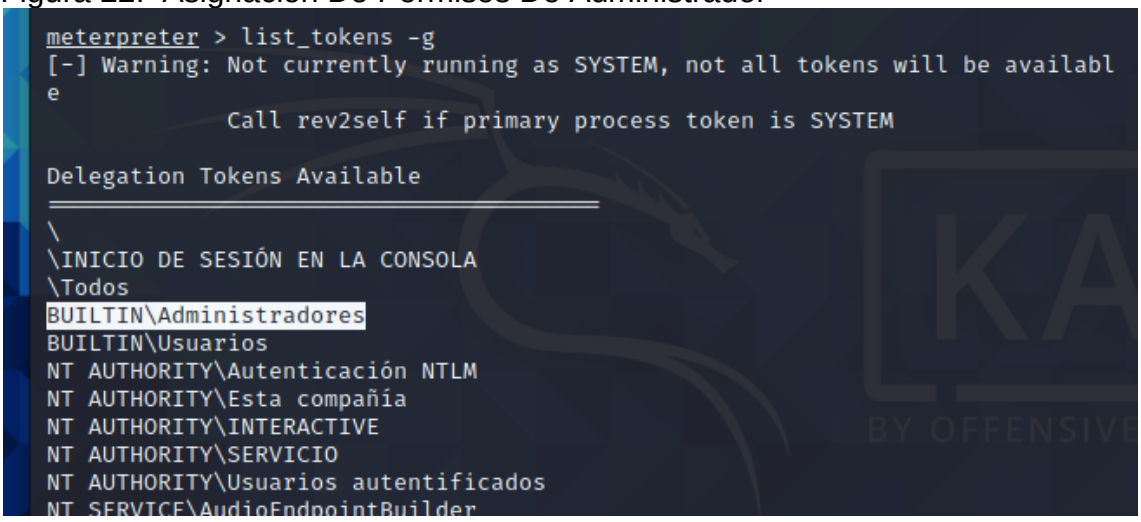
Figura 21. Creación De Usuario Administrador



Mayerly Rocío Enríquez López.

En la siguiente imagen procedemos a asignarle el grupo de administradores al usuario.

Figura 22. Asignación De Permisos De Administrador

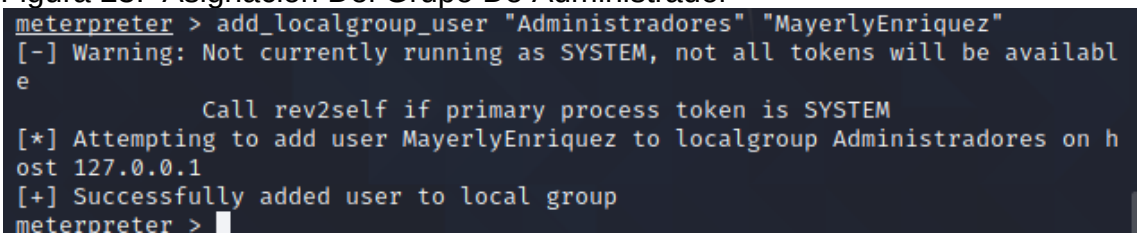


Mayerly Rocío Enríquez López.

Para lograr asignarle al usuario el grupo de administrador utilizamos el comando add_localgroup_user “Administradores” “Mayerly Enríquez” como vemos a continuación

[19] (agnaexto, s.f.)

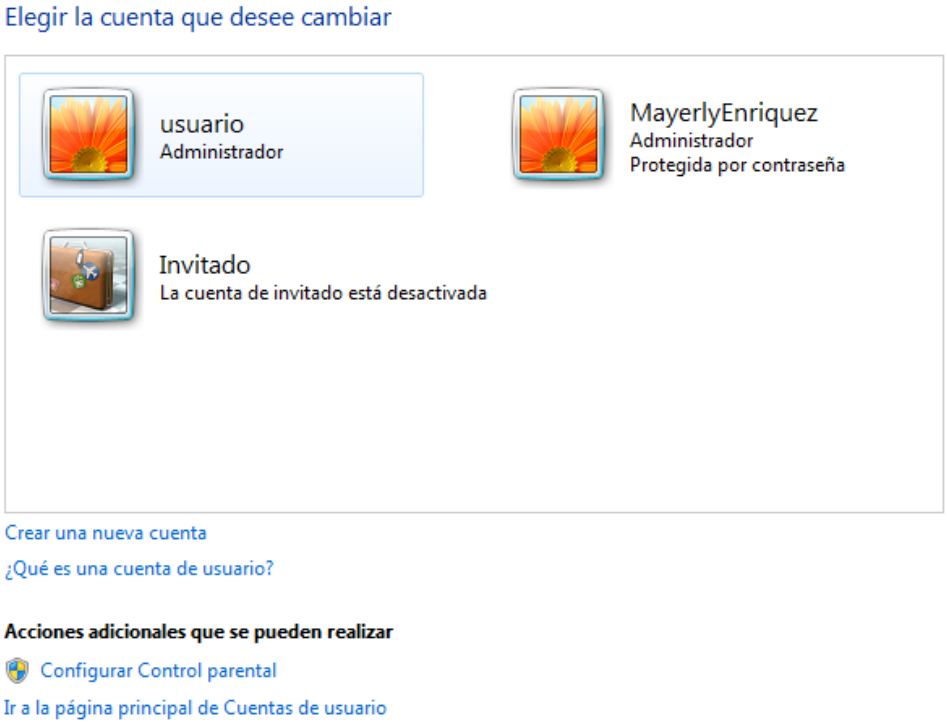
Figura 23. Asignación Del Grupo De Administrador



Mayerly Rocío Enríquez López.

Ahora si entramos en el PC de la víctima por la interfaz de Windows vemos que el usuario se creó y es un administrador del sistema.

Figura 24. Usuarios Activos En Pc De La Victima



Mayerly Rocío Enríquez López.

1.4 SITUACIÓN PROBLEMA: ANÁLISIS BLUE TEAM

WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad

anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

Lo primero que indagaría si me encontrase en un ataque en tiempo real, son los puertos que tengo abiertos en mi servidor, esto lo haría haciendo uso de la herramienta llamada Nmap, la cual me permite hacer rastreo de los puertos por los que posiblemente se efectuó el ataque.

Después de tener identificados los puertos proceder a cerrarlos, luego iría a cambiar las contraseñas de los usuarios del sistema atacado y verificaría si existen usuarios creados que no correspondan a la compañía, para proceder a eliminarlos.

- ✓ Las medidas de Hardenizacion que tomaría para evitar que este ataque vuelva a ocurrir serían los siguientes:
- ✓ Teniendo en cuenta que por donde entraron a ejecutar el ataque fue a través del puerto 80, lo primero que haría es cerrar dicho puerto y demás puertos que estén abiertos y que puedan usarse para próximos ataques.
- ✓ Cambiar las contraseñas de acceso guardadas por defecto en nuestro sistema.
- ✓ Identificar usuarios que no sean necesarios tener creados en nuestro sistema y eliminarlos o bloquear acceso.
- ✓ Identificar que Pcs no cuenta con firewall e instalarlos.
- ✓ Establecería ciertos protocolos de seguridad que deben seguir los usuarios del sistema o la red, por ejemplo, no instalar programas descargados de páginas de dudosa reputación, no usar dispositivos de almacenamiento USB sin antes ser analizados por el antimalware, cambiar periódicamente sus claves de acceso, entre otras.[20]

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

- ✓ Una de las principales diferencias entre blue team y CSIRT es que los equipos blue team se enfocan principalmente en la evaluación de la seguridad de la información en los sistemas de información y los equipos

[20] (CISET. Centro de Innovación, 2020)

CSIRT son quienes reciben y analizan las incidencias de seguridad informática y establecen las acciones de respuesta ante dichos eventos.

- ✓ Los equipos CSIRT ofrecen servicios más completos, mientras los blue team trabajan basados en la monitorización de los sistemas informáticos en busca de posibles vulnerabilidades y así establecer planes de mejora haciendo uso de diversas herramientas, los CSIRT además de hacer lo antes mencionado como la evaluación, auditoria y evaluación de la seguridad de los sistemas informáticos de la organización, también proporciona desarrollo de herramientas para la seguridad de la información.

- ✓ Muchos de los análisis de vulnerabilidades que se hacen en los blue team, provienen de los estudios realizados por los CSIRT, ya que ellos se encargan de armar un centro de respuesta a incidentes de seguridad de tecnologías de la información donde comparte la información para las auditorias.[21]

COMO UTILIZAR CIS

Los controles CIS los utilizaría como metodología de implementación de buenas prácticas de seguridad informática, ya que este nos brinda las acciones que debemos seguir en orden de prioridad es decir que nos marcan una ruta focalizada en los problemas de seguridad informática más comunes en las empresas.

Es una muy buena fuente, ya que los controles CIS son elaborados con información recolectada de diferentes sectores y con base a diversos incidentes de seguridad que han ocurrido en todo el mundo, es una comunidad global que nos ayuda a implementar dichos controles no solo de forma técnica si no que ya están enfocados al maco legal.[22]

FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE SIEM.

- ✓ Los sistemas SIEM, es una tecnología que le permite monitorizar entiempo real el comportamiento de los sistemas informáticos, detectando, respondiendo y neutralizando amenazas informáticas.
- ✓ Una de sus principales características es que SIEM permite tener control total de la seguridad informática de la empresa, ya que tiene acceso a todos los

[21] (UNIR La Universidad en Internet, 2020)
[22] (CIS Center for Internet Security)

eventos que ocurren dentro de la empresa lo que le permite actuar de forma eficaz.

- ✓ SIEM es una unión de dos tecnologías SEM y SIM, SEM se encarga de centralizar la información y permite analizarla en tiempo real. Y SIM se encargar del almacenamiento histórico de la información para luego analizarlas.
- ✓ Al contar con almacenamiento de información de amenazas de seguridad no solo permite controlar las más conocidas si no también las más difíciles de detectar.[23]

Dentro de sus funciones están las siguientes:

- ✓ A través de su alta velocidad y la información histórica a la que tiene acceso permite que la investigación de alertas de seguridad se lleve de forma más eficiente.
- ✓ Proporciona a los analistas de seguridad mayor visibilidad y capacidad de detección en amenazas, brindándoles la metodología y mejor modo de actuar.
- ✓ Monitoreo en tiempo real de las redes de la empresa
- ✓ Recoge información de la actividad de los usuarios no solo en los sistemas informáticos si no también en la red, lo que permite identificar posibles brechas de seguridad y comportamientos maliciosos.[24]

HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS

- ✓ Agnitum Outpost Free: Teniendo en cuenta que los Firewall son unas de las herramientas que más nos son útiles para la seguridad informática, tanto para prevención como contención en un ataque, Agnitum Outpost Free es uno de los mejores firewall del mercado y de los más potentes, este nos permite proteger y detectar las aplicaciones que están tratando de compartir información con el exterior, lo que nos permite controlar la actividad en nuestra red, y evitar que programas maliciosos propaguen su ataque.[25]

- ✓ Malwarebytes : Otro Herramienta importante para la contención de ataques informáticos son los antimalware, ya que además de protegernos de posibles

[23] (FIREEYE)
[24] (SOFECOM, Servicios integrales en IT, s.f.)
[25] (Martín, 2011)

ataques también permite remediar software malicioso en los dispositivos informáticos de manera individual, uno de los antimalware más recomendados es: Malwarebytes el cual nos ofrece excelente tecnología para la destrucción de malware, protección antivirus y eliminación detallada de malware y spyware.[26]

- ✓ Cyber Triage Lite, Es una herramienta de respuesta de incidentes, la cual recopila información de nuestros sistemas y permite que el análisis de dicha información sea efectivo para la detección de intrusos, mostrando la información en línea de tiempo y permite la generación de informes en HTML.[27]

[26] (Malwarebytes)
[27] (Cyber Triage, s.f.)

2. ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM.

Algunos aspectos que pueden aportar al desarrollo de las estrategias de los equipos red team y blue team.

Teniendo en cuenta que estos dos equipos se complementan es de vital importancia fomentar el trabajo en equipo, y que exista flujos de procesos de procesos especificaos dentro de las estrategias, para que cuando por ejemplo el equipo de Blue Team ejecute alguna barrera de seguridad estas se pongan a prueba por parte del equipo Red Team.

Es importante mantener una buena comunicación ya que si el equipo red team logra identificar una vulnerabilidad este debe ser comunicado al equipo Blue team para que establezca las actividades de bloqueo y respuesta ante esta nueva vulnerabilidad, pero para hacer su trabajo es importante que entienda como se exploto esta vulnerabilidad.

Un aspecto importante mantener bitácoras de que inconsistencias o ataques han sufrido en los últimos años y poder analizar y avaluar sus estrategias y como pueden mejorarse para que la respuesta a posibles ataques repetitivos se haga de una forma más eficiente. Con esto no solo nos permite evaluarnos si no que nos permitirá adaptar nuestras estrategias a las nuevas tecnologías de contención de ataques que el mercado vaya sacando.

Estar en constante búsqueda de nuevas formas de ataque, contención de los mismos y herramientas que les permitirá no solo estar al día en sus conocimientos si no a preservar la seguridad de la compañía con mayor eficiencia.[28]

[28] (Crowdstrike, 2020)

3. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN

Es recomendable cuando estamos trabajando en una estrategia de seguridad informática es que debemos tener en cuenta el factor humano tanto como en factor tecnológico, ya que la mayoría de los ataques parten del mal uso de los sistemas y los equipos tecnológicos, es por eso que dentro de la estrategia debe estar la concientización y sensibilización de la seguridad informática a los usuarios, y establecer las actividades u operaciones que se puedan convertir en una vulnerabilidad como por ejemplo:

1. Tener cuidad con los adjuntos del correo, que se aseguren que la fuente del correo sea confiable antes de abrir o ejecutar un adjunto de un correo de un origen desconocido.

2. Explicarles a los usuarios que existen redes de navegación seguras y que otras no son tan seguras y que por ejemplo si vamos hacer alguna transacción bancaria, se aseguren que en la URL diga https eso nos asegura que ese sitio donde voy a realizar mi transacción es confiable y seguro.

3. Normalmente los equipos de computo cuentan con un antivirus o antimalware que nos permite hacer una detección temprana de posibles intrusos, por eso se debe recomendar que cada vez que se haga uso de dispositivos de almacenamiento extraíbles estos sean escaneados por el antivirus, ya que se ha convertido en uno de los medios de mayor propagación de virus.

A nivel software también se tienen algunas recomendaciones:

1. Instalar las actualizaciones de nuestros sistemas operativos, ya que los desarrolladores del mismo, están constantemente liberando parches de seguridad del sistema.
2. Corroborar que los equipos de la compañía cuenten con un buen antimalware y firewall, y que estos estén actualizando su base de datos constantemente.[29]

Otra recomendación para endurecer las estrategias de seguridad en una organización es que se debe estar en constante evaluación, es por esto que se recomienda el uso de los controles CIS (Center For Internet Security), que nos brinda los pasos a seguir ante un ataque informático, no solo los ataques conocidos si no hasta los más complejos, ya que al ser una comunidad a nivel mundial cuenta

[29] (Diaz, 2018)

con la base de datos de los ataques de todo el mundo. Una de las funcionalidades más importantes de CIS es que ya proporciona el marco legal y como proceder en estos casos.[30]

Y por último existen varias herramientas que nos permiten estar en constante monitoreo de las redes, sistemas informáticos y aplicaciones con las que cuenta con la organización una de las que les puedo recomendar es Cyber Triaje que nos brinda un control en tiempo real y además nos permite llevar una bitácora de las incidencias presentadas.[31]

[30] (CIS Center for Internet Security)
[31] (Cyber Triage, s.f.)

4. CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.

Como expertos en seguridad informática debemos tener conocimiento tanto a nivel técnico como a nivel legal, ya que van muy de la mano a la hora de establecer la estrategia de seguridad que se va a implementar en la empresa, por eso es importante estudiar la ley 1273 de 2009, donde nos dan a conocer que actividades están contempladas como delitos y como serán sancionados quienes incurran en ellos.

Existen diversas herramientas que permiten hacer testing en nuestros sistemas como, por ejemplo, es muy usado Kali Linux que es un sistema operativo que trae incorporado una gran variedad de herramienta para Pentesting, lo que nos permitirá identificar vulnerabilidades y aplicar soluciones eficientes.

Otras herramientas muy valiosas son las de monitoreo de anomalías, lo que le permite al equipo de seguridad informática de la empresa tener control e flujo de información que se maneje a través de la red, aplicaciones y sistemas informáticos.

CONCLUSIONES

En Colombia existen normas tanto a nivel legal como ético, que nos da bases a la hora de tomar decisiones y además nos establece que actividades están consideradas como delito y que consecuencias estas nos podrían acarrear.

Es muy importante que como profesionales tengamos en cuenta que cuando llevemos a cabo nuestra labor profesional, está por ningún motivo debe atentar contra la integridad de un tercero y que estamos obligados a denunciar en el caso de tener conocimiento de algún proceso ilegal. Siempre y cuando contemos con las pruebas para esto.

Identificamos alguna de las diversas vulnerabilidades a las que estamos expuestos en nuestros sistemas informáticos y que, si no tomamos las medidas de seguridad necesarias, es muy fácil para un atacante entrar a nuestros sistemas y robar nuestra información, como en el caso estudiado, podríamos hasta perder control de nuestra maquina y el atacante a través de esta puede acceder información por ejemplo de toda una empresa.

También que Existen diversas formas de enfrentarnos a un ataque informático y la importancia que tienen el tener una ruta de contención de los mismos.

Adquirí conocimiento con respecto a las diferentes tecnologías que podemos usar para detectar, analizar y contraatacar los ataques informáticos de los que podamos ser víctimas, y que herramientas nos permitirán ejecutar el plan de contención.

RECOMENDACIONES

Como primera recomendación para esta empresa es establecer un buen equipo Red Team, que nos pueda ayudar con la detección y explotación de vulnerabilidades desde la perspectiva del atacante con el fin de que el equipo Pueda tomar esta información analizarla y establecer los procesos de contención y respuesta a los posibles ataques informáticos a los que estemos expuestos.

Recomiendo que se implementen los controles CIS (Center For Internet Security), que nos brinda los pasos a seguir ante un ataque informático, no solo los ataques conocidos si no hasta los más complejos, ya que al ser una comunidad a nivel mundial cuenta con la base de datos de los ataques de todo el mundo. Una de las funcionalidades más importantes de CIS es que ya proporciona el marco legal y como proceder en estos casos.

También es recomendable hacer uso de la herramienta SIEM, que nos permite tener control se nuestros sistemas, redes y aplicaciones con el fin de monitorear en tiempo real y poder almacenar históricamente las incidencias que se van presentando en el transcurso de la operación de la empresa.

REFERENCIAS

agnaexto. (s.f.). Crear Usuarios con Exploit. Recuperado el 25 de Marzo de 2021, de https://www.youtube.com/channel/UCo1q5zFEesitNOD9wYXlPCw

AVINASH THAPA. (s.f.). Eploit Database. Recuperado el 8 de Marzo de 2021, de https://www.exploit-db.com/exploits/39161

CIS Center for Internet Security. (s.f.). CIS Controls. Recuperado el 25 de Marzo de 2021, de https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

CISET. Centro de Innovación. (28 de Mayo de 2020). Hardening. Recuperado el 26 de Marzo de 2021, de https://www.ciset.es/publicaciones/blog/746-hardening

Congreso de Colombia. (04 de Enero de 2009). MINTIC. Recuperado el 05 de Febrero de 2021, de Ley 1273 de 2009: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Consejo Profesional Nacional de Ingenieria. (2015). COPNIA. Recuperado el 10 de Marzo de 2021, de Código de Ética: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Crowdstrike. (2020). RED TEAM VS BLUE TEAM CYBERSECURITY SIMULATION DEFINED. Recuperado el 07 de Abril de 2021, de https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

Cyber Triage. (s.f.). Free Incident Response Tools. Recuperado el 26 de Marzo de 2021, de https://www.cybertriage.com/landingfreeincidentresponse/

Cyberseguridad.net. (23 de Agosto de 2015). Cyberseguridad.net. Recuperado el 06 de Febrero de 2021, de https://www.cyberseguridad.net/index.php/455-las-fases-de-un-test-de-penetracion-pentest-pentesting-i

Database, E. (s.f.). Exploit Database. Recuperado el 8 de Marzo de 2021, de About The Exploit Database: https://www.exploit-db.com/about-exploit-db

Diaz, C. (2018). 15 Consejos de seguridad informática para empresas. Recuperado el 07 de 04 de 2021, de https://www.muycomputerpro.com/universo-lenovo/15-consejos-seguridad-informatica-empresas/

ENTER.CO -José Luis Peñarredonda. (9 de Diciembre de 2015). ENTER.CO. Recuperado el 18 de Febrero de 2021, de Detrás de Buggly: la historia de la fachada Andrómeda: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

FIREEYE. (s.f.). What is SIEM and how does it work? Recuperado el 03 de Abril de 2021, de https://www.fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html

Fundación Wikimedia. (23 de Noviembre de 2020). Delito informático:. Recuperado el 06 de Febrero de 2021, de https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

Fundación Wikimedia. (3 de Enero de 2021). Kali Linux. Recuperado el 3 de Febrero de 2021, de https://es.wikipedia.org/wiki/Kali_Linux

Fundación Wikimedia. (06 de Febrero de 2021). Software. Recuperado el 05 de Febrero de 2021, de https://es.wikipedia.org/wiki/Software

Fundación Wikimedia. (24 de Enero de 2021). VirtualBox. Recuperado el 05 de Febrero de 2021, de https://es.wikipedia.org/wiki/VirtualBox

Fundación Wikimedia. (14 de Enero de 2021). VMware. Recuperado el 05 de Febrero de 2021, de https://es.wikipedia.org/wiki/VMware

Fundación Wikimedia, I. (23 de Noviembre de 2020). Wikimedia. Recuperado el 06 de Febrero de 2021, de Delito informático: https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

Fundación Wikimedia, I. (02 de Septiembre de 2020). Wikipedia. Recuperado el 05 de Febrero de 2021, de Common Vulnerabilities and Exposures: https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

Fundación Wikimedia, Inc. (1 de Febrero de 2021). Equipo de Respuesta ante Emergencias Informáticas. Recuperado el 24 de Marzo de 2021, de https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Informáticas

Fundación Wikimedia, Inc. (06 de Febrero de 2021). Wikipedia. Obtenido de Software: https://es.wikipedia.org/wiki/Software

Fundación Wikimedia, Inc. (14 de Enero de 2021). Wikipedia. Recuperado el 05 de Febrero de 2021, de VMware: https://es.wikipedia.org/wiki/VMware

Fundación Wikimedia, Inc. (24 de Enero de 2021). Wikipedia. Recuperado el 05 de Febrero de 2021, de VirtualBox: https://es.wikipedia.org/wiki/VirtualBox

Fundación Wikimedia, Inc. (3 de Febrero de 2021). Wikipedia. Recuperado el 04 de Febrero de 2021, de Kali Linux: https://es.wikipedia.org/wiki/Kali_Linux

infosecuritymexico. (s.f.). infosecuritymexico. Recuperado el 27 de Marzo de 2021, de Ciberseguridad: https://www.infosecuritymexico.com/es/ciberseguridad.html#ciberseguridad

infosecuritymexico. (s.f.). infosecuritymexico. Recuperado el 26 de Marzo de 2021, de Ciberseguridad: https://www.infosecuritymexico.com/es/ciberseguridad.html#ciberseguridad

Ivan. (04 de Septiembre de 2017). Hacking Para Novatos. Recuperado el 6 de Febrero de 2021, de Hacking Para Novatos: https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/

Languages.oup. (s.f.). Ley. Recuperado el 05 de Febrero de 2021, de https://languages.oup.com/google-dictionary-es/

Malwarebytes. (s.f.). Recuperado el 29 de Marzo de 2021, de https://es.malwarebytes.com/mwb-download/

marindelafuente. (29 de Abril de 2019). Marin de la fuente. Recuperado el 06 de Febrero de 2021, de ¿Qué es Nmap? Por qué necesitas este mapeador de red: https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/

Martín, J. R. (08 de 05 de 2011). 10-firewalls-gratuitos-alternativos. Recuperado el 25 de Marzo de 2021, de Agnitum Outpost Free: https://www.emezeta.com/articulos/10-firewalls-gratuitos-alternativos

National Institute of standards. (s.f.). NATIONAL VULNERABILITY DATABASE. Recuperado el 08 de Marzo de 2021, de https://nvd.nist.gov/vuln/detail/CVE-2014-6287

Rizaldos, H. (22 de Octubre de 2018). Open Webinars. Recuperado el 06 de Febrero de 2021, de Qué es Metasploit framework: https://openwebinars.net/blog/que-es-metasploit/

Serrano, H. A. (05 de Enero de 2009). Lay 1276 5 enero de 2009. Bogotá, Cundinamarca, Colombia. Recuperado el 20 de Febrero de 2021

SOFECOM, Servicios integrales en IT. (s.f.). SOFECOM. Recuperado el 03 de Abril de 2021, de SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran: https://sofecom.com/que-es-un-siem/

UNAD - Universidad Abierta y a Distancia. (2020). Anexo 3. Recuperado el 22 de Febrero de 2021, de http://www.unad.edu.co

Unir La Universidad en Internet. (2020 de Enero de 2020). Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? Recuperado el 20 de Marzo de 2021, de https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

UNIR La Universidad en Internet. (27 de Enero de 2020). Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? Recuperado el 20 de Marzo de 2021, de https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

welivesecurity. (18 de Noviembre de 2014). Welivesecurity. Recuperado el 08 de Marzo de 2021, de Cómo utilizar OpenVAS para la evaluación de vulnerabilidades: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

Enlace video Sustentación: https://www.youtube.com/watch?v=4HkT_BpKVcU