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

ROGER GARIBELLO MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

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

ROGER GARIBELLO MARTINEZ

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
BOGOTA
2021

CONTENIDO

pág.

INTRODUCCIÓN ***8***

OBJETIVOS ***9***

1.1 OBJETIVOS GENERAL **9**

1.2 OBJETIVOS ESPECÍFICOS **9**

2 DESARROLLO DEL INFORME ***10***

3. FASE RECOLECCIÓN DE INFORMACIÓN ***14***

3.1. FASE ANÁLISIS DE VULNERABILIDAD **17**

3.2. FASE EXPLOTACIÓN **18**

4. SITUACIÓN PROBLEMA: ANÁLISIS RED TEAM ***20***

4.1. SITUACIÓN PROBLEMA: ANÁLISIS BLUE TEAM. **27**

5. ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM.30

6. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE ORGANIZACIÓN.31

BIBLIOGRAFÍA ***34***

TABLA DE ILUSTRACIONES

Pág.

Ilustración 1. Desactivar fireware y actualizaciones Win 7 x64 14
Ilustración 2. Desactivar fireware y actualizaciones Win 2020 x86 14
Ilustración 3. Identificación de enrutamiento 15
Ilustración 4. Dispositivos conectados a la red 192.168.1.0 15
Ilustración 5. Análisis de puertos y servicios Win 7 x 64 16
Ilustración 6. Análisis de puertos y servicios Win 7 x 86 17
Ilustración 7. Análisis puertos y servicios. 17
Ilustración 8. Ejecución de NESSUS 18
Ilustración 9. Consola msf exploit. 18
Ilustración 10. Exploit rejetto 2.3 19
Ilustración 11. Estado de configuración SET. 19
Ilustración 12. Consola Donde Se Ejecuta Comando Nmap Fuente propia 21
Ilustración 13. Análisis Por Medio De Exploit Database 22
Ilustración 14. Descripción De La Vulnerabilidad Encontrada 22
Ilustración 15. Exploit que podemos utilizar para esta vulnerabilidad 23
Ilustración 16. Carga De Exploit 24
Ilustración 17. Configuración De Ips. 25
Ilustración 18. Creación De Usuario Administrador 25
Ilustración 19. Asignación De Permisos De Administrador. 26
Ilustración 20. Usuarios Activos En Pc De La Victima 26

GLOSARIO

VULNERABILIDAD: es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

AMENAZA: toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

INFORMACION: Activo intangible en el cual se manejan identificaciones, datos personales, cuentas, datos empresariales y corporativos, propiedad intelectual, conocimiento comercial, formulación de productos o servicios.

DELITO INFORMATICO: Accionar que va en contras de las leyes establecidas y que mediante el manejo y conocimiento informático se aprovecha de las deficiencias en la seguridad de la información, para hacer uso abusivo a la información o bienes de terceros

ENTORNO DE PRUEBA: Laboratorio controlado en el cual se recrean las condiciones deuna posible, falla de sistema, vulnerabilidad del sistema, o un ataque, con el fin de entenderlo, detallarlo, definirlo y proporcionar las herramientas para su mitigación

MAQUINA VIRTUAL: Entorno de virtualización mediante el uso de diferentes herramientaslas cuales permiten a partir de un solo dispositivo físico contar con particiones virtuales enlas cuales pueden convivir diferentes sistemas operativos, de este modo se pueden realizar pruebas de vulnerabilidad a aplicaciones y archivos.

EXPLOIT: Uso de la vulnerabilidad en una aplicación, sistema informático, archivo, la cualse aprovecha de manera no autorizada.

METASPLOIT: Metasploit Framework es una plataforma modular de pruebas de penetración basada en Ruby que le permite escribir, probar y ejecutar código de explotación. Metasploit Framework contiene un conjunto de herramientas que puede utilizar para probar vulnerabilidades de seguridad, enumerar redes, ejecutar ataques y evadir la detección

METERPRETER: Meterpreter es un payload de Metasploit que proporciona un shell interactivo desde el cual un atacante puede explorar la máquina objetivo y ejecutar código.

RESUMEN

Por medio de este documento se presenta un resumen de las etapas anteriores en el curso seminario especializado red team & blue team, en los cuales se plantearon diferentes situaciones en las cuales un especialista en seguridad de la información debe valerse de sus conocimientos, experiencia y manejo de herramientas para validar, identificar, comprender, y buscar soluciones que conduzcan a la corrección y mitigación de vulnerabilidades tanto a nivel de sistemas operativos como a nivel de aplicaciones, teniendo en cuenta la multiplicidad de amenazas que pueden presentarse en una organización buscando los puntos débiles para ser aprovechados como puede ser una fuga de información, accesos no autorizados, privilegios de administrador y creación de usuarios, lo que impacta directamente en los pilares de la seguridad de la información.

PALABRAS CLAVE: red team & blue team, fuga de información, Mitigación, Vulnerabilidad, Sistemas operativos, aplicaciones, amenazas, seguridad de la información.

ABSTRACT

Through this document, a summary of the previous stages in the specialized seminar course red team and blue team is presented, in which different situations were raised in which an information security specialist must use their knowledge, experience and management of tools to validate, identify, understand, and seek solutions that lead to the correction and mitigation of vulnerabilities both at the operating system level and at the application level, taking into account the multiplicity of threats that can arise in anorganization by looking for weak points to be taken advantage of, such as information leakage, unauthorized access, administrator privileges and user creation, which directly impacts the pillars of information security.

KEY WORDS: red team & blue team, leak, mitigation, vulnerability, operating systems, applications, threats, information security.

INTRODUCCIÓN

Para un especialista en seguridad informática es importante la identificación de los efectos y en especial de las causas frente a incidentes de seguridad empleando el análisis de las situaciones, la investigación y la creación de pruebas a partir de creación y montaje de laboratorios, además del empleo de las diferentes herramientas, entornos y posibilidades que puedan ser útiles para encontrar la solución o soluciones para corregir y mitigar las

causas y efectos tanto de las vulnerabilidades como de las amenazas que buscan la pérdida de los pilares de la información y en muchos casos evitar un delito informático.

Actualmente se presentan múltiples fuentes de información confiable las cuales deben ser consultadas frecuentemente para estar actualizado frente a las nuevas vulnerabilidades y amenazas a las cuales se ven expuestos los diferentes sistemas informáticos, este tipo de fuentes por lo general brinda la manera de mitigar o corregir la vulnerabilidad eliminando una posible amenaza y permitiendo proteger y mantener los pilares de la información en una organizació

OBJETIVOS

1.1 OBJETIVOS GENERAL

Desarrollar las actividades propuestas, alcanzando las competencias y destrezas requeridas identificando posibles vulnerabilidades y como se pueden fortalecer y corregir posibles fallos de seguridad identificados al interior de una organización.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar los aspectos legales de la seguridad de la información en Colombia
- Reconocer posibles actuaciones que incurran en delitos informáticos
- Hacer uso de entorno de prueba virtual y realizar uso de herramientas
- Identificar fallo de seguridad especifico que se presenta en entorno de prueba
- Documentar los pasos específicos para encontrar el fallo de seguridad en el entorno de prueba
- Investigar tipo vulnerabilidad y replicar ataque mediante uso de herramientas especializadas.
- Corregir posibles vulnerabilidades mediante hardening del sistema propuesto.
- Proponer herramientas de tipo GLP que permitan mejorar la seguridad de la información sin acarrear costos asociados a licenciamiento.

2 DESARROLLO DEL INFORME

A continuación, se puede observar la primera situación problema, a la que nos vimos enfrentados en el reclutamiento para trabajar con la empresa WhiteHouse Security y está relacionada con el Análisis del Acuerdo de Confidencialidad.

Después de leer el acuerdo de confidencialidad que posee WhiteHouse Security para firmar con los participantes del reclutamiento, desde la óptica ética y legal podemos resaltar lo siguiente:

Fragmentos sacados textualmente del acuerdo de confidencialidad.

- Sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.
- Datos secretos como “datos de chuzadas, interceptación de información accesos abusivos a sistemas informáticos”.
- No denunciar ante las autoridades actividades sospechosas de espionaje

Argumentación sobre aspectos no éticos e ilegales.

- En ninguna circunstancia, un acuerdo de confidencialidad de una organización puede estar por encima de las leyes colombianas.
- Todo profesional experto en seguridad informática tiene el compromiso de divulgar ante las autoridades competentes (Fiscalía, Policía, Ejército, entre otras), cualquier proceso ilegal del cual tenga conocimiento, sin tener como prerrequisito la autorización de la entidad en donde labora.
- Ningún particular ni empresa privada en Colombia, está autorizado para realizar algún tipo de chuzada y espionaje, debido a que es un delito.

Esta labor, sólo pertenece a algunas entidades del Estado como la Fiscalía, el ejército y la policía, entre otros; las cuales pueden realizar interceptaciones a teléfonos, correos electrónicos, redes sociales, etc;

Con el fin de conseguir información para un caso en particular o reserva de Estado. Ley 1273 de 2009.

Por medio de la cual se realizan modificaciones en el Código Penal, creando un nuevo bien jurídico denominado como “de la protección de la información y de los datos” En el cual se deben preservan los sistemas que utilicen las tecnologías de la información y las comunicaciones de una manera integral.

Dentro de la ley N.º 1273 se tienen contemplados algunos de los delitos informáticos que se cometen y tipifica algunos de ellos.

Clausula primera y segunda, clausula cuarta, parágrafo 3. En el artículo 269A se enuncia el acceso abusivo a un sistema informático, se tiene en cuenta para todo lo que tiene que ver con accesos no autorizados, incluyendo lo que se denomina como “chuzada”, procedimiento en el cual se utilizan diferentes herramientas

- En el artículo 269B indica que no se debe generar indisponibilidad operdida de acceso sistemas informáticos, a información o bases de datosy a redes de telecomunicaciones.

- En la Clausula segunda se viola el Artículo 269C el cual Habla de lano legalidad de interceptación de datos informáticos, en ningún punto yasea origen o destino, además que contempla la no interceptación de ondas electromagnéticas.

- El Articulo 269D indica que es ilegal cualquier tipo de daño a nivel desoftware y hardware, sea memoria o funcionamiento, para tener en cuenta ante ataques.

- En el artículo 269E se indica el no uso de software malicioso o malware, pero no indica claramente cuáles son los tipos de Malware.

- El Articulo 269F contempla la protección de datos personales contenidos en bases de datos, ficheros, los cuales no pueden ser sustraídos, vendidos, interceptados.

- La suplantación de sitios Web con el fin de obtener datos personaleseste enunciado en el artículo 269G, atiende a personas que clonen paginas legales o realicen desvió de información para beneficio propio.

- En los artículos 269 I y J se contempla el hurto por medios informáticos y la transferencia no consentida de activos.

- Existiendo procesos poco confiables en el anexo 3, usted como experto en ciberseguridad aplicaría a este trabajo en WhiteHouse Security, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.

  R/ Como la empresa Whitehouse Security está buscando un especialista en seguridad informática, lo primero que solicita es la revisión del acuerdo entre las partes, por lo cual se logran evidenciar inicialmente unas posibles faltas a las leyes colombianas y ética profesional, como es un ejercicio de identificación, se le argumenta a la empresa Whitehouse Security los términos y cláusulas que pueden estar en contra de la legalidad, con base en esta información ellos pueden verificar y analizar teniendo en consideración la argumentación de un experto en seguridad informática, en caso de que el contrato sea revisado y ajustado acepta ningún tipo de modificación no aceptaría la posibilidad de un trabajo en el cual se puedan llevar a cabo actividades delictivas, criminales o que vayan en contra de la ley, no solo eso, también me considero un profesional integro que valora y respeta su conocimiento, como lo indica el código de ética el cual se apoya en la ley 842 de 2003: “busca que los ingenieros, profesionales afines y auxiliares, actúen con compromiso y honestidad en aras de brindar a la ciudadanía un ejercicio ético de su profesión.

  Además, desisto de un empleo en el cual pueda verme implicado en acciones ilícitas cometidas sin conocimiento, ya sea de mi parte o de compañeros de trabajo, ya que realizar actividades ilegales con el fin de cumplir las razones laborales no me exonera de la culpa. En el Código emitido por el COPNIA el cual se indica como el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo.

DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31.

Esta el parágrafo que indica “Son deberes generales de los profesionales los siguientes”:

> f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, deque tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder; Si en caso de que estas acciones sean llevadas a cabo con plenoconocimiento, estaré incurriendo en un delito implicando no solo mipersona, sino la profesión y mi círculo familiar, social, académico, laboral.De nuevo en el Código emitidopor el COPNIA, Código de Ética para el ejercicio de la Ingeniería en generaly sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES

Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 34.

Este parágrafo indica, “Son prohibiciones especiales a los profesionales respecto de la sociedad”:

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

En el caso de que un profesional incurra en participar de cualquier clase de delito en el desarrollo de sus funciones va en contra del código de ética, y en detrimento de su profesión, además en caso de un delito está obligado legalmente a revelar información. En el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares en su Capitulo II, DE LOS DEBERES Y OBLIGACIONES DE LOS.

b) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo. Por último, se dejan en claro las faltas graves que un profesional de la ingeniería en este caso un especialista en seguridad informática debe evitar. En el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, se contemplan las faltas gravísimas contempladas en el artículo 53 de la ley 842 de 2003. Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta unible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones. Cualquier violación gravísima, según el criterio del Consejo respectivo.

En Colombia tenemos la ley Deberá buscar la noticia del caso “OPERACIÓN ANDROMEDA BUGGLY” en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.3 de 20091, la cual hace referencia a la protección de la información y de los datos.

Según esta ley, el acuerdo de confidencialidad vulnera los siguientes artículos:

Artículos

- Artículo 269A: Acceso abusivo a un sistema informático
- Artículo 269C: Interceptación de datos informáticos

Argumentación

- The WhiteHouse Security indica que va a acceder a sistemas de información de otras entidades (a través de chuzadas, accesos abusivos, interceptación, espionaje) para obtener algún tipo de información, indudablemente sin contar con la autorización de estos últimos ni contar con orden judicial del Estado. Por lo indicado anteriormente, evidentemente se violan estos dos artículos.

3. FASE RECOLECCIÓN DE INFORMACIÓN.

Para la exposición de esta fase nos dedicamos a acumular toda la información creíble que la firma tenga desocupado identificando los sistemas y programas en funcionamiento que ella tiene La material que se emplea para vendimia de información es NMAP en me permite equilibrar puestos abiertos o cerrados adentro del procesos de trabajo y características propias de cada indiviso de ellos enservicios Además se procede a inutilizar le fireware de Windows para potencia embolsarlas operaciones requeridas para separación de vulnerabilidades que requieren el proyecto y su concerniente estudio de operaciones en el uso.

Paso 1: Desactivación de firewall de las máquinas virtuales.

Ilustración 1. Desactivar fireware y actualizaciones Win 7 x64.

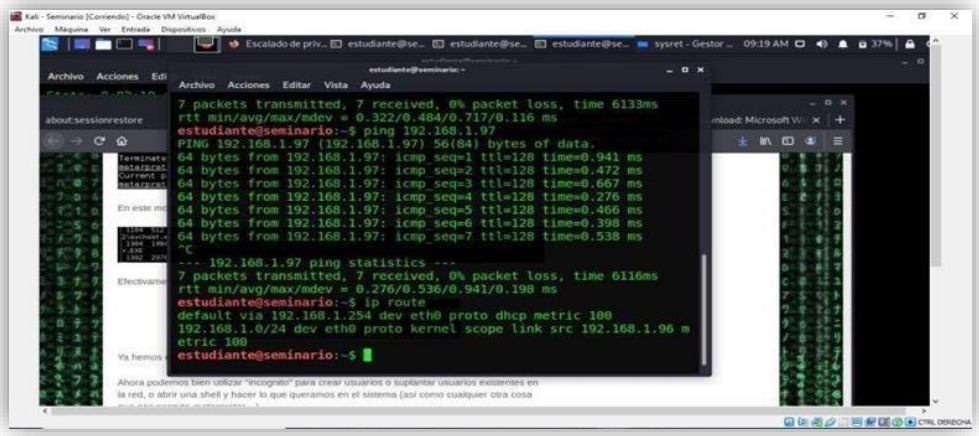
Fuente: Elaboración propia.

Ilustración 2. Desactivar fireware y actualizaciones Win 2020 x86.

Fuente: Elaboración propia.

Paso 2: Identificación de enrutamiento.

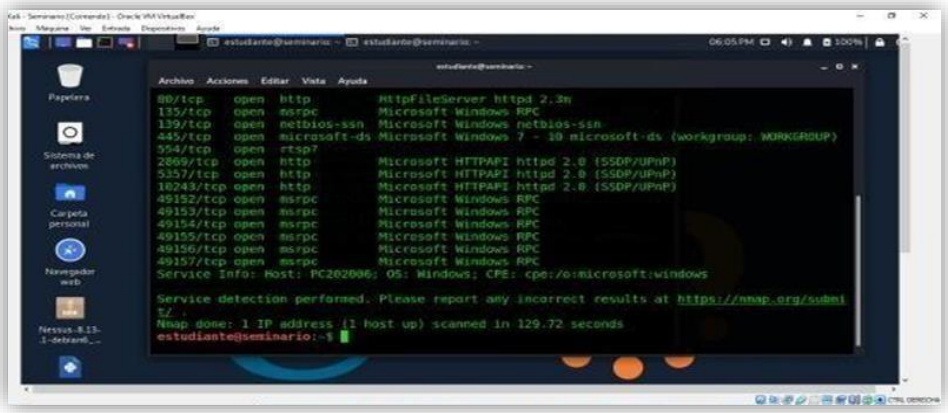
Ilustración 3. Identificación de enrutamiento.



Fuente: Elaboración propia.

Paso 3: Que dispositivos están conectados a la red.

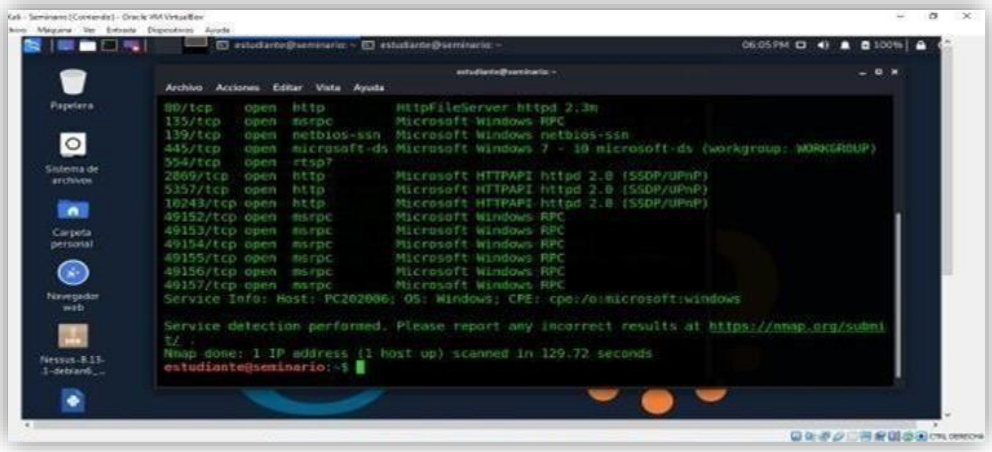
Ilustración 4. Dispositivos conectados a la red 192.168.1.0.



Fuente: Elaboración propia.

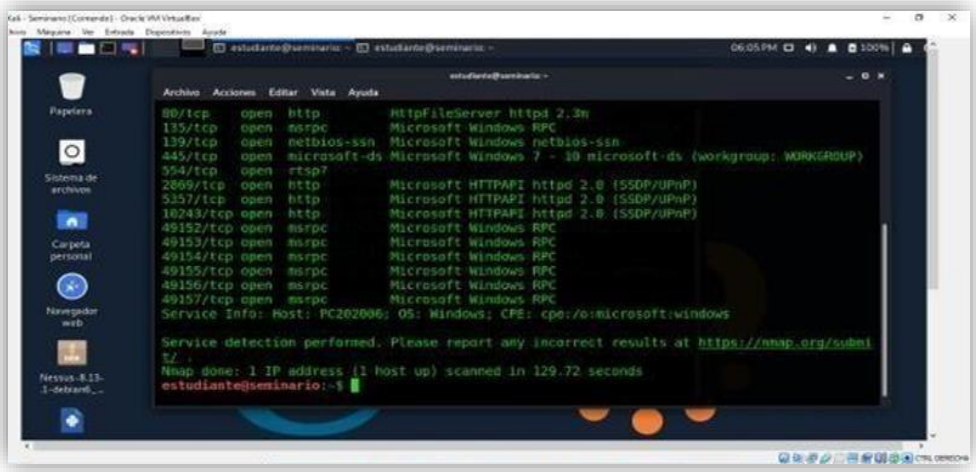
Paso 4: Identificación de puertos y servicios win7 x64.

Ilustración 5. Análisis de puertos y servicios Win 7 x 64.



Fuente: Elaboración propia.

Ilustración 6. Análisis de puertos y servicios Win 7 x 86.



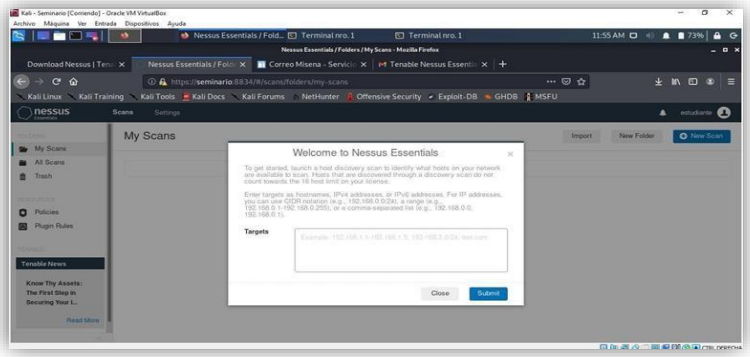
Fuente: Elaboración propia.

3.1. FASE ANÁLISIS DE VULNERABILIDAD.

En esta fase se valoran los casos exitosos de nuestras estrategias de penetración a través del análisis y proactividad de vulnerabilidades. En este momentoes cuando nos damos cuenta de si el proceso de penetración es eficiente y eficaz. Las herramientas que utilizamos para este proceso fue NESSUS – NMAP, las cuales me permiten identificar según el factor de vulnerabilidad las características de riesgos y estabilidad del sistema:

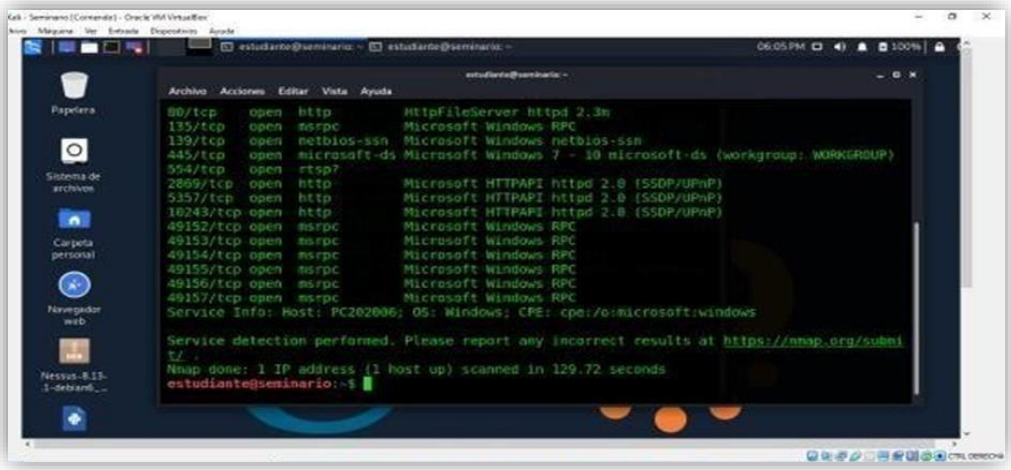
Paso 1: Entorno análisis de vulnerabilidades NESSUS

Ilustración 7. Entorno operación NESSUS.



Fuente: Elaboración propia.

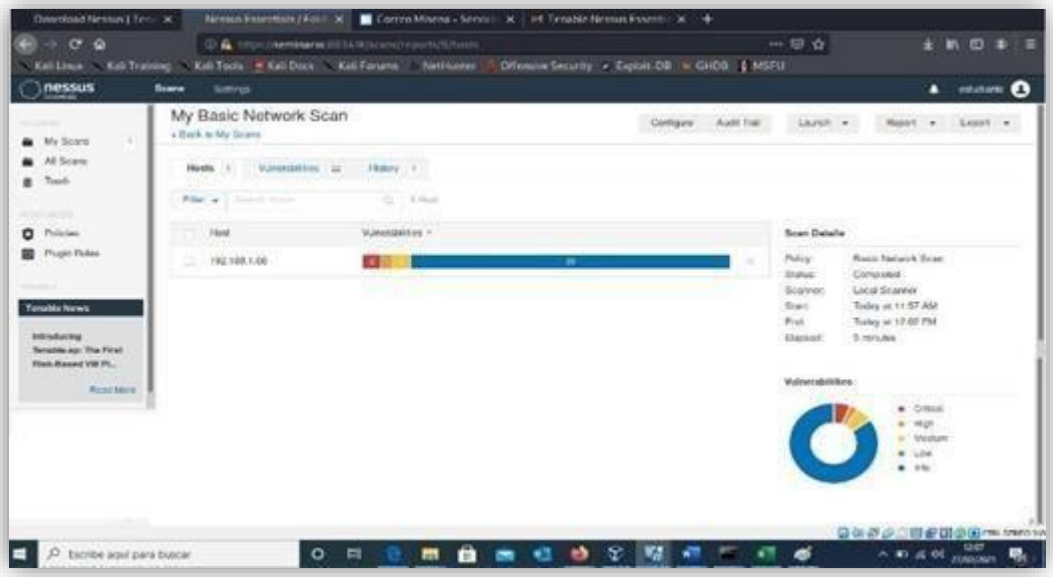
Paso 2: Nuevamente verificamos puertos y servicios para la utilizar la aplicación en los procesos de análisis de vulnerabilidad.



Fuente: Elaboración propia.

Paso 3: Ejecución de análisis de NESSUS.

Ilustración 8. Ejecución de NESSUS.

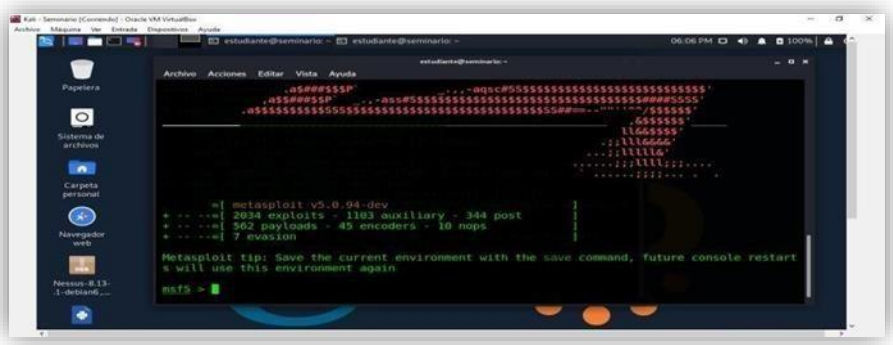


Fuente: Elaboración propia.

3.2. FASE EXPLOTACIÓN.

Paso 1: Ingreso desde la consola para realizar el exploit.

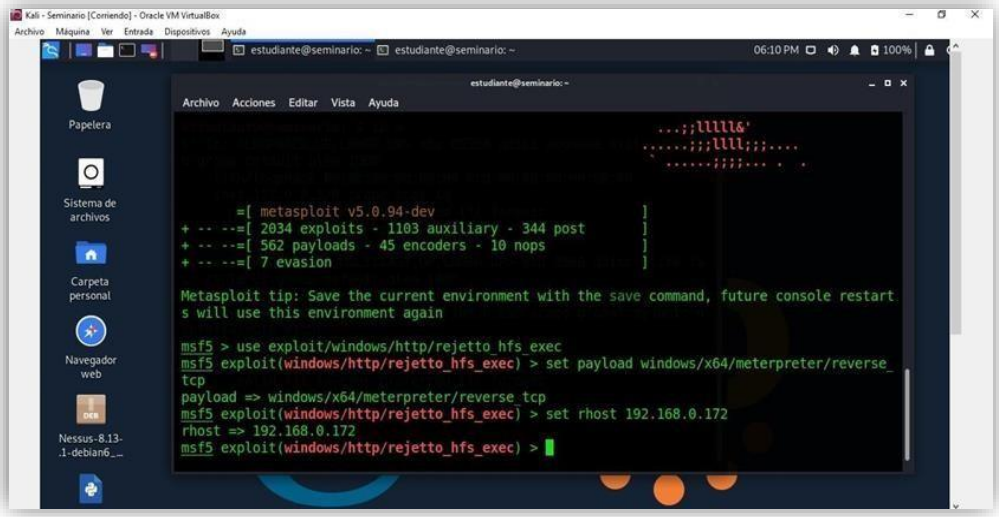
Ilustración 9. Consola msf exploit.



Fuente: Elaboración propia.

Paso 2: Usamos el exploit rejetto 2.3, en este caso se procede a setear el payload: windows/x64/meterpreter/reverse_tcp. Posteriormente realizamos elseteo del rhost: 192.168.0.172.

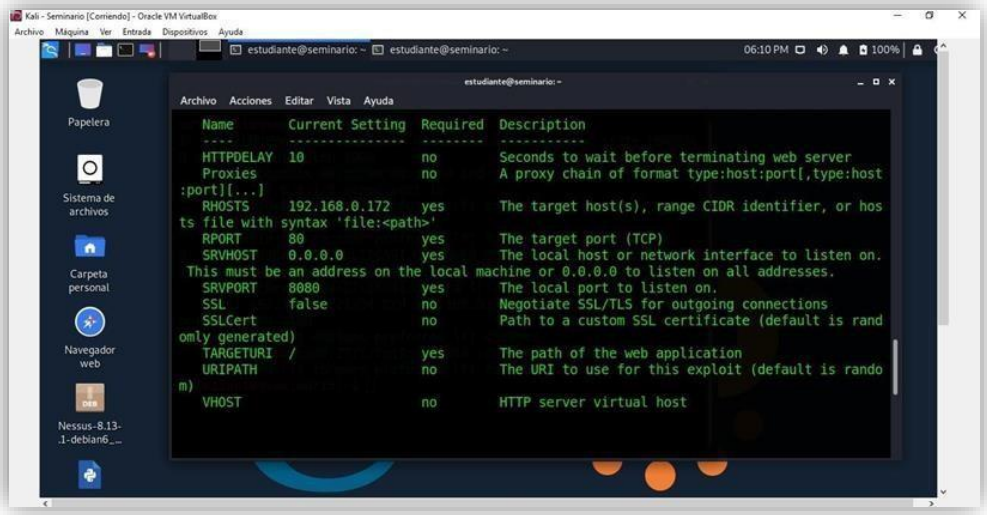
Ilustración 10. Exploit rejetto 2.3.



Fuente: Elaboración propia.

Paso 3: Verificamos que la configuración del set quedo acorde a lo establecido.Show options.

Ilustración 11. Estado de configuración SET.



Fuente: Elaboración propia.

4. SITUACIÓN PROBLEMA: ANÁLISIS RED TEAM.

La primera tarea del equipo rojo es determinar la forma o proceso a través del cual ocurren una serie de fugas de información, y estas fugas se manifiestan en los dispositivos informáticos dentro de la organización. La información preliminar obtenida por el equipo fue que se instaló una aplicación llamada rejetto v en la máquina donde se filtró la información. 2.3 En Windows 7 con arquitectura X64, esta aplicación parece tener un exploit relacionado, que puede causar shell inverso y sesiones abiertas de Meterpreter. La encuesta también investigó la escalada de privilegios causada por la creación de usuarios de tipo administrador del sistema. El equipo forense genera una copia del servidor y se la proporciona como experto. Debe verificar posibles agujeros de seguridad. Si es explotado, debe crear un usuario con su nombre y apellido. El usuario debe ser administrador. Esto es para mostrar el PoC a la alta dirección. Información mutua.

Obteniendo información

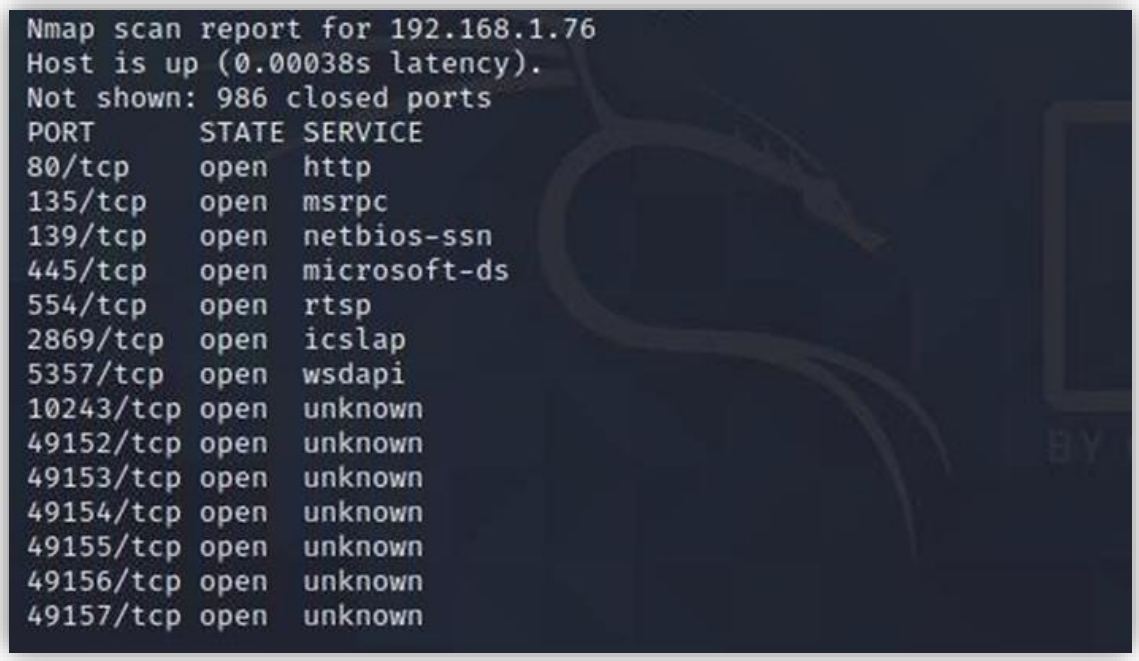
La actividad inicial es importante toda la información posible para iniciar las pruebas realizadas, contamos con los equipos que vamos atacar tiene instalado Windows 7 y tiene una herramienta llamada rejetto, al buscar en Google y

YouTube se puede evidenciar que esta herramienta tiene un hueco de seguridad del 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.

En la imagen que vemos que el puerto 80 se verifica que está abierto y por la investigación previa conocemos que Rejjeto abre el puerto 80, el puerto al parecer.

Ilustración 12. Consola Donde Se Ejecuta Comando Nmap Fuente propia.

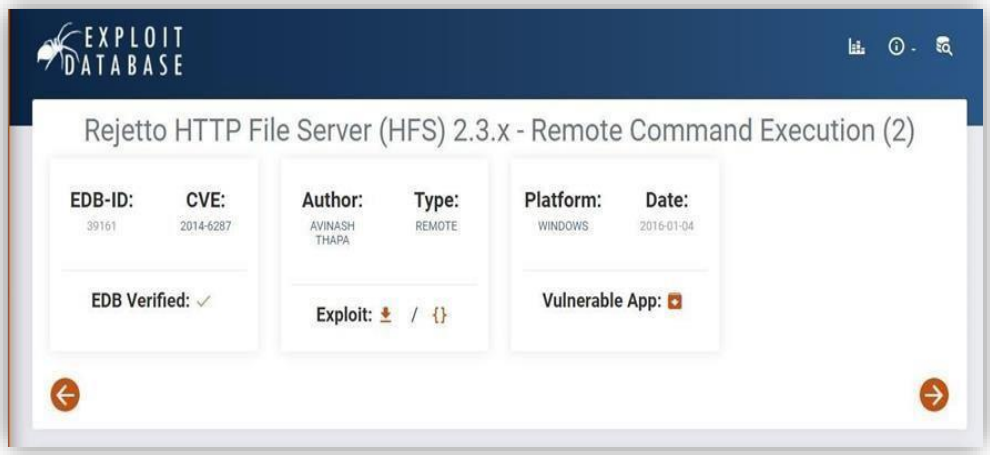


Fuente: Elaboración propia.

no está bloqueado por un firewall.

En la imagen vemos que ya tiene un código por las plataformas vulnerables son las de tipo Windows.

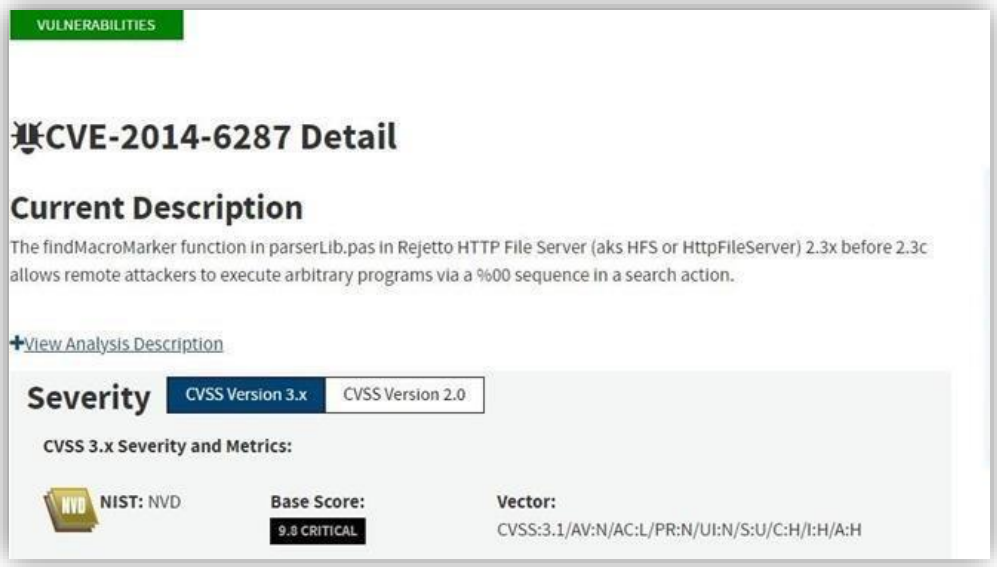
Ilustración 13. Análisis Por Medio De Exploit Database.



Fuente: Elaboración propia.

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

Ilustración 14. Descripción De La Vulnerabilidad Encontrada.



Fuente: Elaboración propia.

Con la información anterior vamos a proceder a explotar la vulnerabilidad.

Utilizamos Metasploit framework para buscar que exploitss podrían utilizar con elcomando msfconsole.

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

Ilustración 15. Exploit que podemos utilizar para esta vulnerabilidad.

Fuente: Elaboración propia.

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 se puede búsqueda en Google en Buscar vulnerabilidades.
2- El tipo de sistema operativo en este caso Windows.
3- Se es posible conseguir una Shell reversa y una sesión de meterpr

HERRAMIENTA UTILIZADA PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD

Las herramientas utilizadas para identificar los fallos de seguridad fueron.

- ✓ Google (Puede encontrar si alguien más encontró la vulnerabilidad y si seencuentra en una base de datos)
- ✓ Exploit db (se verifica que es posible la ejecución de comandos remotos)
- ✓ Nmap (Me permite saber que puertos se encuentran corriendo y queaplicaciones)

Metasploit (Me permite buscar los exploits disponibles para aprovecharla vulnerabilidad)

¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

Los puertos que abren es el 80 el cual es identificado también por Nmap.

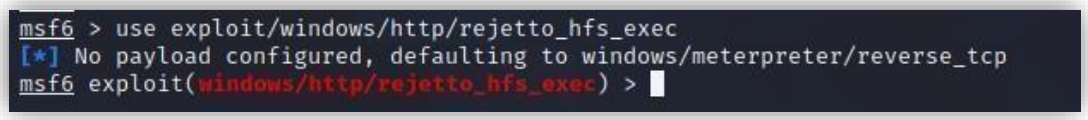
CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64), HAGA USO DEGRÁFICOS PARA EXPLICAR EL ATAQUE.

Lo que entiendo es que Kali no inició primero una conexión con el pc que estamos atacando, pero la computadora de la víctima recibe el comando y se conecta a la computadora del atacante, por lo que el firewall del sistema operativo no lo detectay establece la conexión. Posiblemente, cuando Se crea esta conexión, ya tenemosun Shell que puede ejecutar comandos de forma remota. El siguiente diagrama explica el proceso.

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

Se carga el exploit que verificamos en pasos anteriores,el exploit nos carga por defecto el payload.

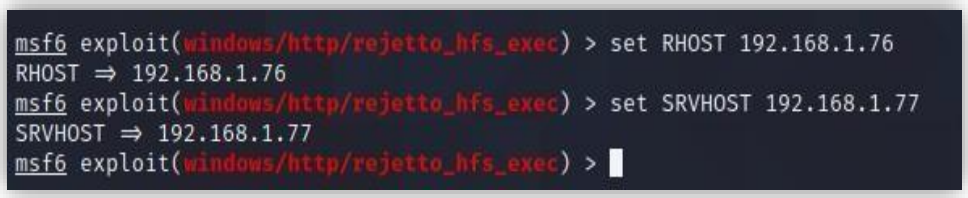
Ilustración 16. Carga De Exploit.



Fuente: Elaboración propia.

Ahora vamos a ver la IP del del atacante y la IP del equipo de la víctima para ello digitamos el comando SET.

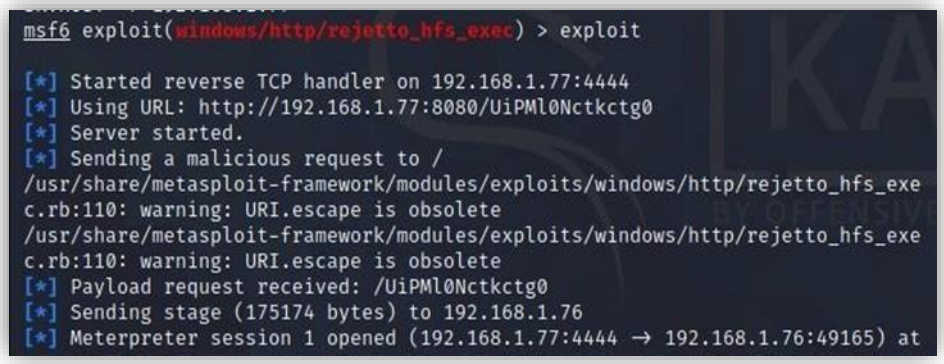
Ilustración 17. Configuración De Ips.



Fuente: Elaboracion propia.

Ahora configuramos escribimos el comando exploit el cual ve la vulnerabilidad, estoy realiza una Reversa y una sesión ahora estamos en la máquina.

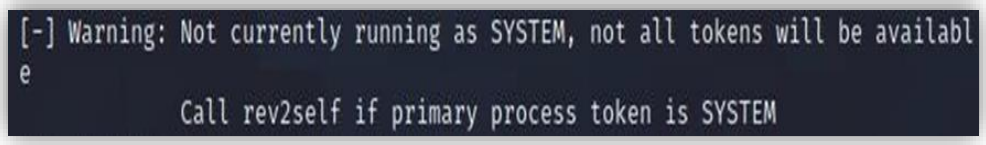
Ilustración 19. Shell Reversa Y Sesión De Meterpreter.



Fuente: Elaboración propia.

Creamos un usuario administrador en la máquina de la víctima, para realizamos loque 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

Ilustración 18. Creación De Usuario Administrador.



Fuente: Elaboración propia.

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

usuario.

Ilustración 19. Asignación De Permisos De Administrador.

Fuente: Elaboración propia.

Para crear el usuario el grupo de administrador escribimos el comando add_localgroup_user.

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.

Ilustración 20. Usuarios Activos En Pc De La Victima.

Fuente: Elaboración propia.

4.1. 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. Lamáquina que se debe analizar es la Windows 7 X64 analizada en la actividad WhiteHouse Security requiere que sus miembros de Blueteam controlen eimplementen ataques informáticos en tiempo real. La máquina a analizar es la Windows 7 X64 analizada en la actividad Anterior. La organización necesita realizar un análisis detallado de lo que está sucediendo a nivel técnico del "sistema operativo y red". A través de la información recopilada, se espera que, dentro de sus conocimientos profesionales como miembro del equipo azul, pueda controlar el ataquepara evitar que genere cambios dentro de la organización Mucho daño. WhiteHose Security te informa que no tienes el presupuesto para usar herramientas de pago, por lo tanto, los expertos en ciberseguridad deben elegir un conjunto mínimo de herramientas con licencia GPL. Si me encuentro en un ataque en tiempo real, lo primero que quiero preguntar son los puertos que abro en el servidor, y usaré una herramienta llamada Nmap para hacer esto, que me permite rastrearlos.

Después de determinar los puertos, continúe cerrándolos, luego cambie las contraseñas de los usuarios del sistema atacado y verifique si los usuarios creadosson inconsistentes con la empresa para eliminarlos.

- ✓ Para evitar que este tipo de ataque vuelva a ocurrir, las medidas de fortalecimiento que tomaré son las siguientes:
- ✓ Considerando que el lugar al que ingresan para ejecutar el ataque es a través del puerto 80, lo primero que tienen que hacer es cerrar este puerto yotros puertos abiertos que puedan ser usados para futuros ataques.
- ✓ Cambiar la contraseña de acceso guardada por defecto en nuestro sistema.
- ✓ Identificar usuarios que no necesitan ser creados en nuestro sistema y eliminar o bloquear el acceso.
- ✓ Asegúrese de que la PC no tenga un firewall e instálelos.

Establecerá ciertos protocolos de seguridad que los usuarios del sistema o de la red deben seguir, por ejemplo, no instalar programas descargados de páginas de mala reputación.

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

- ✓ CSIRT ofrecen servicios más completos, mientras que el equipo azul trabaja basado en el monitoreo de los sistemas informáticos en busca de de vulnerabilidades y así realizar los planes de mejora verificando el usode diversas aplicativos, los CSIRT además de hacer lo antes mencionadocomola 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.

- ✓ Varios de los análisis de vulnerabilidades que se hacen en los blue team, se realizan n de los estudios que se verifican por los CSIRT, ya que ellos seencargan de verificar un centro de respuesta a incidentes de seguridad de tecnologías de la información donde comparte la información para las auditorias.

COMO UTILIZAR CIS

Los controles CIS se hace como metodología de implementar de buenas prácticas de seguridad informática, ya que este nos brinda lo que debemos seguir en orden dependiendo la vulnerabilidad es decir que nos marcan una ruta estándar en los problemas de seguridad informática más comunes.

ya que los controles CIS son verificados con información encontrada 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 marco legal.

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 totalde la seguridad informática de la empresa, ya que tiene acceso a todos los eventos que ocurren dentro de la empresa lo que le permite actuar de formaeficaz.
- ✓ SIEM es una unión de dos tecnologías SEM y SIM, SEM se encarga de verificar la información y permite analizarla en tiempo real. Y SIM seen cargada del almacenamiento de la información para luego analizarlas.
- ✓ Al contar con almacenamiento de información de amenazas de seguridad nosolo permite controlar las más conocidas si no también las más difíciles de detectar.

Dentro de sus funciones están las siguientes:

- ✓ A través de su alta velocidad y la información histórica a la que tiene accesopermite que la investigación de alertas de seguridad se lleve de forma más eficiente.
- ✓ Proporciona a los ingenieros de seguridad mayor visibilidad y capacidad dedetección 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.

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.

- ✓ Malwarebytes: Otro Herramienta importante para la contención de ataques informáticos son los antimalware, ya que además de protegernos de posibles 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.
- ✓ Cyber Triage Lite, Es una herramienta de respuesta de incidentes, la cual recopila información de nuestros sistemas y permite que el análisis de dichainformación sea efectivo para la detección de intrusos, mostrando la información en línea de tiempo y permite la generación de informes en HTML.

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

Puede ayudar a desarrollar algunos aspectos de la estrategia del equipo rojo y azul. Teniendo en cuenta que estos dos equipos se complementan, es importante promover el trabajo en equipo y existen procesos específicos en la estrategia, por eso, por ejemplo, cuando el equipo azul implementa barreras de seguridad, estas son probadas por el equipo rojo. Mantener una buena comunicación es importante, pues si el equipo rojo logra identificar la vulnerabilidad, se debe comunicar al equipo azul para que puedan establecer actividades de prevención y respuesta ante esta nueva vulnerabilidad, pero para completar su trabajo, deben entender cómo se produce. está Completado. Utilizo esta vulnerabilidad como un aspecto importante para registrar inconsistencias o ataques en los últimos años, y poder analizar y evaluar sus estrategias y cómo mejorarlas para responder a posibles ataques.

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 conocimientossi no a preservar la seguridad de la compañía con mayor eficiencia.[28]

6. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE ORGANIZACIÓN.

Cuando estamos verificando 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 cuidado 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 uno rigen desconocido.

2. Indicarles 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 cómputo 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. Verificar que los equipos de la empresa tengan un buen antimalware y firewall, y que estos siempre estén actualizando su base de datos constantemente.

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 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.

CONCLUSIONES

- Para el Especialista en Seguridad Informática es de vital importancia conocer los diferentes delitos informáticos contemplados en las leyes colombianas, no solo para intentar proteger la red que administra frente aellos, sino también para concienciar a nivel laboral, social y personal a su entorno, de las diferentes amenazas informáticas que pueden presentarsea diario.

- Realizar actividades en las cuales se ponen a prueba los conocimientos informáticos para la búsqueda y hallazgo de posibles vulnerabilidades, asícomo su tratamiento para mitigar y evitar amenazas o ataques

- Entender cómo se presentan los riesgos a la seguridad de la información por medio de vulnerabilidades en un sistema, haciéndolas aptas para su explotación, la identificación y mitigación de amenazas debe ser una tareaen constante desarrollo que no se permite pausas, mantenerse al tanto denuevas vulnerabilidades y formas de aprovecharla así como la manera decontrarrestarlas puede ayudar al especialista en seguridad de la información a estar un paso antes y brindar la seguridad que requiere su sistema.

BIBLIOGRAFÍA

MINTIC. (2009). Ley 1273 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/inicio/3705:Ley-1273- de-2009

COPNIA. (2020). Código de ética | Copnia. https://www.copnia.gov.co/tribunal-deetica/codigo-de-etica

COPNIA (2003). Ley 842 de 2003. | Copnia. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

EL TIEMPO (2015). Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [En línea]. https://www.eltiempo.com/archivo/documento/CMS-15141236

EL ESPECTADOR (2018). Caso Andrómeda y sus interrogantes [En línea]. https://www.elespectador.com/noticias/judicial/casoandromeda-y-sus-interrogantes/

EL ESPECTADOR (2018). Los detalles de Andrómeda, según la Procuraduría. [En línea] https://www.elespectador.com/noticias/judicial/losdetalles-de-andromeda-segun-la-procuraduria/

Villanueva, Lina María Patricia Manrique. (2019) "en Colombia: agencias y complicidades mediáticas. https://www.researchgate.net/profile/Lina-Manrique-Villanueva/publication/336273968_Complicidades_y_agencias_mediaticas/links/5d97e75b458515c1d395778f/Complicidades-y-agencias-mediaticas.pdf

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11(28).

Salazar, J. F. (2011). Situación normativa de la Sociedad de la Información en Colombia. Criterio Jurídico, 9(1).

TINOCO LINARES, Ana, et al. Análisis y clasificación de los ataques y sus exploits: Framework Metasploit como caso de estudio. 2020.

PASTOR RICÓS, Fernando. Pentesting y generación de exploits con Metasploit.2020

NIÑO ORDOÑEZ, José Rafael, et al. Capacidades Tecnicas, Legales y de Gestión para Equipos BlueTeam y RedTeam. 2020.

AVILA GUALDRÓN, Miguel Andrés, et al. Estudio de las mejores prácticas de Ethical Hacking, para generar un nuevo método que facilité la ejecución de análisis de seguridad

DENIS, Matthew; ZENA, Carlos; HAYAJNEH, Thaier. Penetration testing: Concepts,attack methods, and defense strategies. En 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016. p. 1-6.

JASWAL, Nipun. Mastering Metasploit. Packt Publishing Ltd, 2016.

Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287). 2014. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). CVE-2014-6287CVE-111386. 2016. https://www.exploit-db.com/exploits/39161 https://www.exploit-db.com/exploits/34852

Rejetto HFS versions 2.3, 2.3a, and 2.3b are vulnerable to remote commandexecution.2014. https://www.kb.cert.org/vuls/id/251276

Security vulnerabilities of Rejetto Http File Server : List of all related CVE securityvulnerabilities. https://www.cvedetails.com/vulnerability-list/vendor_id-14180/product_id-29196/Rejetto- Http-File-Server.html

LINK VIDEO PRESENTACION

https://www.youtube.com/watch?v=yEvV49sDQYI&ab_channel=RogerUzumaki