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

MIGUEL GIOVAN LEIVA PADILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD – RED TEAM & BLUE TEAM
GRUPO 202337164_6
IBAGUE
2021

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

MIGUEL GIOVAN LEIVA PADILLA

Proyecto de Grado – seminario especializado: equipos estratégicos en ciberseguridad – red team & blue team presentado para optar por el titulo de ESPECIALISTA EN SEGURIDAD INFORMATICA

TUTOR:
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD – RED TEAM & BLUE TEAM
GRUPO 202337164_6
IBAGUE
2021

RESUMEN

En el presente documento se encontrara un informe detallado de las temáticas vistas a lo largo del seminario especializado, Equipos estratégicos de Seguridad Red Team & Blue Team el cual ha sido dividido en 4 fases diferentes cada una enfocada a entender aspectos importantes a la hora de ejercer en campos de ciberseguridad, por ende este informe tratara temáticas relacionadas con las leyes informáticas colombianas que regulan la seguridad informática y los delitos informáticos, análisis de actuaciones éticas según la ley 1273 de 2009, pruebas de vulneración ejecutadas por un equipo Red Team el cual busca identificar por que ha sido vulnerada una organización recreando los posibles hechos de un ciberdelincuente, actuaciones de contención de un equipo Blue Team ante las situaciones presentadas en el ejercicio Red Team, recomendaciones de seguridad y buenas prácticas.

Antes de continuar en el desarrollo del informe es importante tener en cuenta que la ciberseguridad es un factor importante en cualquier organización y que una buena implementación de esta ayudara a las empresas a no presentar fallas de seguridad y mantener sus activos a salvo. Por ello es importante el uso de los equipos Blue Team y Red Team que trabajan de forma conjunta para contribuir con el desarrollo de la seguridad de la empresa, mitigación de riesgos y vulnerabilidades.

CONTENIDO

pág.

TABLA DE ILUSTRACIONES

Pág.

GLOSARIO

AMENAZA: Aprovechamiento de las vulnerabilidades para vulnerar un sistema.

ATAQUE: Utilización de una amenaza para ejecutar un ataque y vulnerar un sistema

BLUE TEAM: Equipo defensivo de ciberseguridad de una organización.

CIBERSEGURIDAD: Es el área encargada de velar por la seguridad de los sistemas informáticos de una organización.

NMAP: Herramienta para realizar análisis de red, esta permite detectar puertos abiertos e incluso conocer detalles a nivel técnico de equipo escaneado.

RED TEAM: Equipo ofensivo de ciberseguridad de una organización.

VULNERABILIDAD: Fallas en los sistemas que pueden ser aprovechados por las amenazas.

INTRODUCCIÓN

Dado el aumento de ataque ciberneticos, ha surgido la necesidad de implementar nuevas estrategias de seguridad por ello se crearon los equipos de ciberseguridad que ayudan a contribuir de forma positiva la seguridad de las organizaciones, estos equipos son conocidos como Blue Team, el cual está encargado del esquema defensivo de la organización, controlando todo tipo de comportamiento inusual, análisis de tráfico, herramientas de escaneo, entre otras. Por otra parte, tenemos el equipo Red Team que se encarga de la seguridad ofensiva de una organización, poniendo a prueba los esquemas de seguridad, controles y aplicaciones es importante entender que este equipo realiza un trabajo complementario con el Blue Team.

En el seminario especializado se puede apreciar el tratamiento de diferentes temáticas que están relacionadas directamente con la seguridad informática, pues para ejercer adecuadamente en este campo se debe tener pleno conocimiento de las leyes y normas vigentes en cada país relacionadas con la seguridad informática, para este caso en particular se basó el estudio y planteamientos con las normas colombianas en seguridad informática, adicional a ello se plantearon campos reales de intrusión a un sistema utilizando herramientas como Nmap y Metasploit ejecutado por un equipo Red Team, por ultimo y para complementar la fase anterior vista se investigan acerca de metodologías que permitan contener los ataques vistos en las fases anteriores papel que llevaría a cabo un equipo Blue Team en una organización.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Documentar los resultados obtenidos a lo largo del seminario especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

1.2 OBJETIVOS ESPECÍFICOS

- Conocer las leyes y normas colombianas que abarcan la seguridad informática.
- Construir el banco de trabajo para el desarrollo de cada fase.
- Identificar los aspectos éticos y legales que pueden estar presentes en un contrato laboral.
- Recrear en un ambiente controlado la vulneración de un sistema por medio del equipo Red Team para detectar como se presentó esta vulneración.
- Establecer métodos de seguridad por parte del equipo Blue Team para evitar posibles fallas futuras relacionadas con la vulneración anterior.

2 DESARROLLO DEL INFORME

2.1 DESARROLLO FASE 1

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.

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

Colombia es un país que en materia de ciberseguridad y delitos relacionados con la informática ha ido implementado leyes y normativas que permitan sancionar y controlar todos estos tipos de incidentes sin embargo en mi criterio personal considero que debe mejorar aún más en este punto pues el aumento de delitos informáticos ha sido considerable en los últimos años.

Las normas, decretos y leyes que existen en Colombia relacionadas con ciber seguridad y delitos informáticos son las siguientes:

Ley 527 de 1999

Fue expedida en Colombia el 18 de agosto del año 1999, allí se definen reglamentos de acceso y el método de uso de los mensajes de datos, comercio electrónico y firmas digitales. También marcan las entidades de certificación entre otras disposiciones. Es importante recalcar que esta ley es aplicable a todo tipo de información encapsulado como mensaje de datos, exceptuando obligaciones contraídas por el Estado Colombiano y las advertencias escritas que por solicitud legal deban ir impresas.

Ley 962 de 2005.

Fue expedida en Colombia el 8 de julio de 2005, allí se establecen disposiciones relacionadas con los tramites y procedimientos administrativos de los organismos y entidades del estado junto con las organizaciones que cooperan con servicios públicos.

Ley 1273 de 2009

Fue expedida en Colombia el 5 de enero de 2009, en esta se modifica el código penal, creando un nuevo bien jurídico dirigido a la protección de la información y de los datos, tipificando los diferentes tipos de delitos informáticos contemplados en la ley, sus sanciones económicas y penales. [1]

Está compuesta por los siguientes artículos:

- Artículo 269A Acceso abusivo a un sistema informático.
- Articulo 269B Obstaculización ilegitima de un sistema informático
- Artículo 269C Interceptación de datos informáticos
- Articulo 269D Daño informático
- Articulo 269E Uso de software malicioso
- Artículo 269F Violación de datos personales.
- Artículo 269G Suplantación de sitios web para capturar datos personales
- Artículo 269H Circunstancias de agravación punitiva
- Articulo 269I Hurto por medios informáticos
- Articulo 269J Transferencia no consentida de activos.

Ley 1341 de 2009

Fue expedida en Colombia el 30 de julio de 2009, se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de información y comunicaciones TIC. [2]

[1] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (enero 5 de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Enero, 2009 Nro. 47.223.p.p. 14-25.

[2] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341 (Julio 30 de 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. En: Diario Oficial. Julio, 2009. Nro. 47.426.

Ley 1581 de octubre 17 de 2012

Fue expedida en Colombia el 17 de octubre de 2012, por la cual se dictan obligaciones generales para la protección de datos personales. Donde su principal objetivo es desarrollar el derecho constitucional que tienen las personas de conocer, actualizar y rectificar la información que se hayan recogido sobre ellas en bases de datos o archivos.

Documento CONPES 3701 de 2011

El CONPES tiene como objetivo presentarle al gobierno nacional, políticas, programas, estrategias y proyectos, enfocados en el desarrollo económico y social del país. El documento 3701 de 2011 expedido por el CONPES habla de los "Lineamientos De Política Para Ciberseguridad Y Ciberdefensa"; el problema se centra en la capacidad actual del Estado para enfrentar las amenazas cibernéticas. Donde se detectan debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. [3]

Ley 842 de octubre 9 de 2003 de COPNIA

Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones.

[3] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Consejo Nacional de Política Económica y Social-CONPES 3701. Bogotá D.C: Departamento Nacional De Planeación, 2011

2.1.2 DEFINIR CADA UNA DE LAS ETAPAS DEL PENTESTING, DENTRO DE LA DEFINICIÓN INCORPORARÁ UN EJEMPLO DE UNA HERRAMIENTA QUE SE UTILICE PARA CADA UNA DE LAS ETAPAS DEL PENTESTING.

Existen tres tipos de pentesting que pueden realizar:

- Pentesting de caja blanca: El pentester o auditor conoce toda la información de la empresa, por tal motivo realiza un análisis completo de la estructura informática identificando los sistemas que pueden ser modificados o mejorados según la infraestructura tecnológica.

- Pentesting de caja negra: Este simula un ambiente real donde el pentester no conoce ningún tipo de información de la empresa y su intención es actuar como un ciberdelincuente para intentar detectar vulnerabilidades y amenazas.

- Pentesting de caja gris: Es una mezcla de las dos fases anteriores, el pentester conoce un mínimo de información de la empresa y desde allí parte para realizar el test.

Para realizar estas fases el pentester debe seguir ciertas etapas que aseguren que el examen realizado cumple con los requerimientos de la organización, estas fases son las siguientes:

- ✓ Recogida de información: Se evalúa la información que tiene de la empresa y el tipo de pentesting a realizar para determinar cómo efectuar el test. Dependiendo del tipo de test, se pueden emplear diferentes herramientas, en el caso de no tener acceso a la información de la empresa existen herramientas como Dig, DnsRecon, Maltego, Pastenum. Para los casos donde se tiene acceso a la información de la empresa existen herramientas como Metasploit y Snmpwalk.

- ✓ Análisis de vulnerabilidades y amenazas: Realizar pruebas para verificar las vulnerabilidades del sistema, posibles fugas de información, amenazas potenciales, todo esto teniendo en cuenta también el factor humano y sus fallos. Para esta fase se pueden utilizar herramientas como Nessus, Burp suite, Nmap.

- ✓ Acceso al sistema: Al analizar la información obtenida, se establecen que tipos de ataque se ejecutaran y el objetivo de los mismos. Para esta fase se utilizan herramientas como Metasploit para aprovechar las vulnerabilidades detectadas.

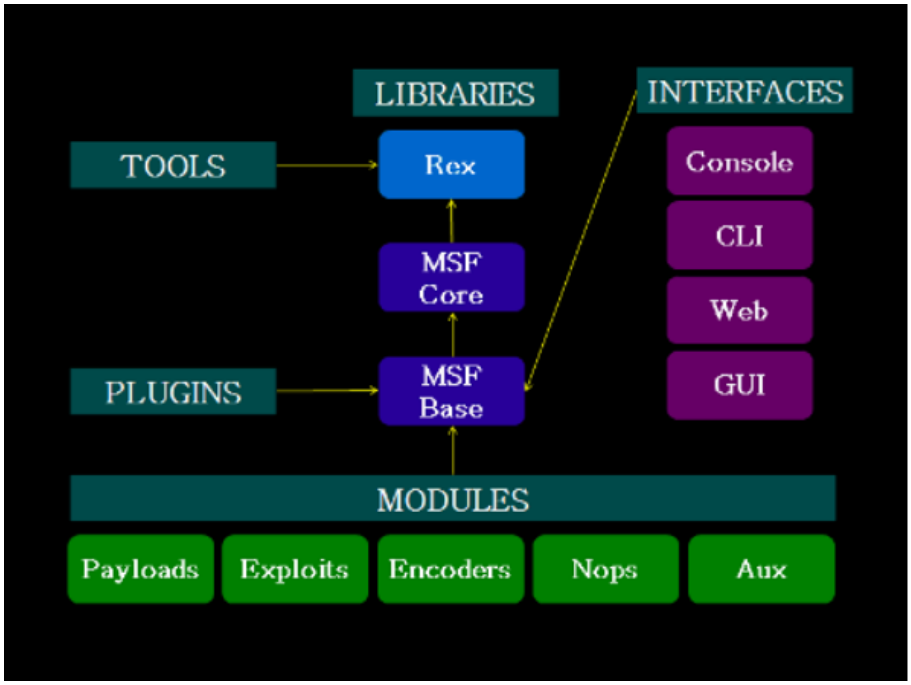
- ✓ Elaboración del informe: Allí se debe evidenciar al alcance de los fallos de seguridad detectados, impacto que podrían tener, por último, debe incluir recomendaciones para mitigar estas fallas y mejoras de medidas de seguridad. Para esta fase existe una herramienta llamada PWNDoc desarrollada en Node.js la cual permite agilizar el desarrollo de los informes.

2.1.3 DEFINIR Y EXPLICAR LAS SIGUIENTES HERRAMIENTAS Y SERVICIOS EN LINEA.

Metasploit

Es una herramienta desarrollada en Perl y Ruby, esta enfocada en auditorias de seguridad, sin embargo, también ha sido utilizada con fines maliciosos por cibercriminales, esta herramienta tiene muchos exploits, los cuales se aprovechan de vulnerabilidades conocidas, con unos módulos conocidos como payloads donde está el código que explota vulnerabilidades. También dispone de otros módulos conocidos como encoders el cual contiene código para evadir un antivirus o sistemas de seguridad. Adicionalmente permite interactuar con otras herramientas externas como son Nmap.

Ilustración 1 Módulos Metasploit



Fuente: https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente/

Nmap

Esta es una herramienta de código abierto para explorar la red y realizar auditorías de seguridad, esta herramienta utiliza paquetes IP para determinar que equipos se encuentran disponibles en una red. Gracias a esta herramienta se puede determinar los servicios como son nombre y versión de la aplicación, sistemas operativos, tipos de cortafuegos que se están ejecutando.

La base de Nmap es el análisis de puertos, pero también cuenta con otras capacidades como:

- Mapeo de red
- Detección de SO
- Descubrimiento de servicios
- Auditorias de seguridad

Ilustración 2 Nmap

Fuente: https://paraisolinux.com/que-es-y-como-usar-nmap/

OpenVas

Es una herramienta de análisis de vulnerabilidades que puede detectar diferentes tipos de problemas ya sean de bajo riesgo para usuarios, como también vulnerabilidades más graves en equipos de red. Esta cuenta con más de 50.000 test y datos de vulnerabilidades conocidas. Esta herramienta surge después de que Nessus cambiara su modelo de código abierto a un modelo de negocio.

Esta herramienta tiene diversas funciones como son:

- Pruebas autenticadas
- Pruebas no autenticadas
- Protocolos industriales y de internet
- Ajustes personalizados
- Desarrollo de un potente lenguaje de programación interno

Ilustración 3 OpenVas

Fuente: https://www.openvas.org/

ExploitDB

Existe un repositorio de Exploit Database en Github donde se encuentra searchsploit, la cual es una herramienta de búsqueda de línea de comandos para realizar Explot DB, esta herramienta también permite realizar búsquedas detalladas fuera de línea.

CVE

Las fallas y puntos de vulnerabilidades comunes, conforman una lista de fallas de seguridad informática estas se encuentran disponible al público, estas fallas cuentan con un número de identificación. Los CVE permiten a los especialistas coordinar estrategias y priorizar soluciones a los puntos vulnerables.
Este sistema funciona por medio de la corporación MITRE que se encarga de supervisar las CVE financiado por la agencia de seguridad de ciberseguridad e infraestructura, del departamento de seguridad nacional de estados unidos.
Para que una falla se califique como CVE debe cumplir los siguientes criterios:

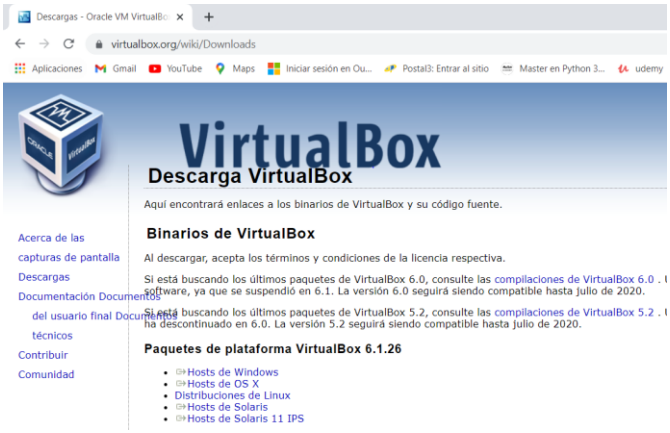
- Se puede solucionar de forma independiente.
- El proveedor afectado las confirma y las documenta.
- Afectan una base del código.

2.1.4 ANALICE Y CONFIGURE “BANCO DE TRABAJO”

Paso A: Descargar virtual Box

Para descargar virtual Box se debe acceder a su página oficial https://www.virtualbox.org/wiki/Downloads y seleccionar el SO correspondiente donde se instalará el programa.

Ilustración 4 VirtualBox

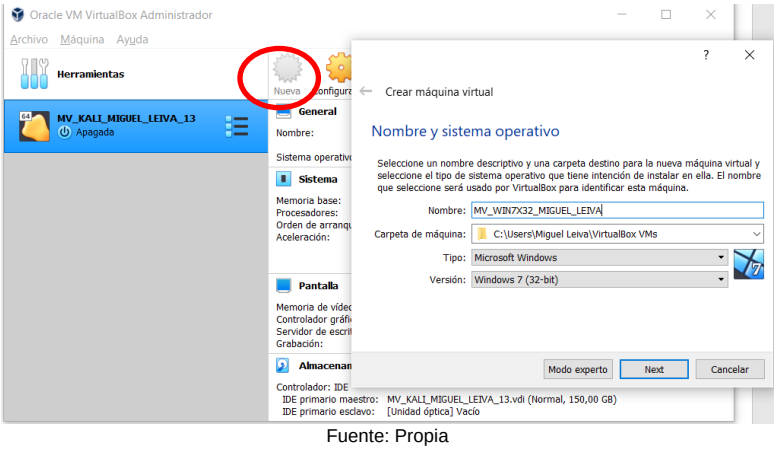


Fuente: Propia

Paso B: Montaje de las maquinas en virtual Box

Se utiliza la máquina virtual Box, donde se crea una nueva máquina, se asigna el nombre y el sistema operativo.

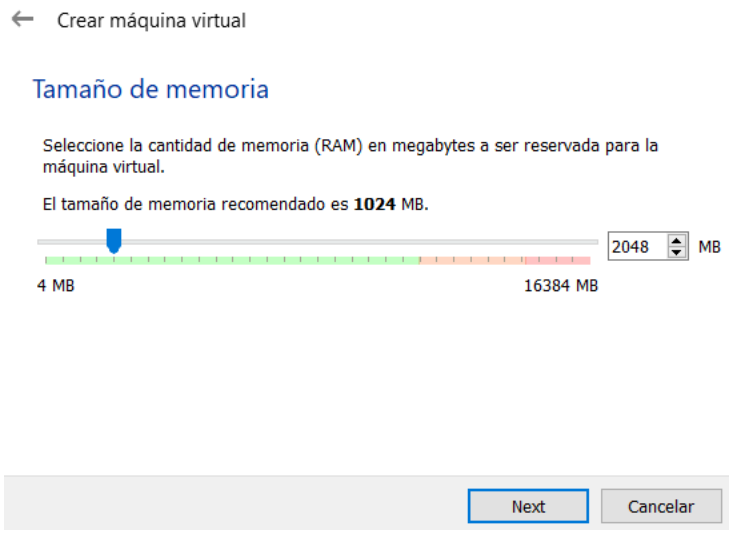
Ilustración 5 Nueva Máquina VistualBox



Fuente: Propia

Se asigna el tamaño en memoria que para todas las maquinas será igual 2048 MB

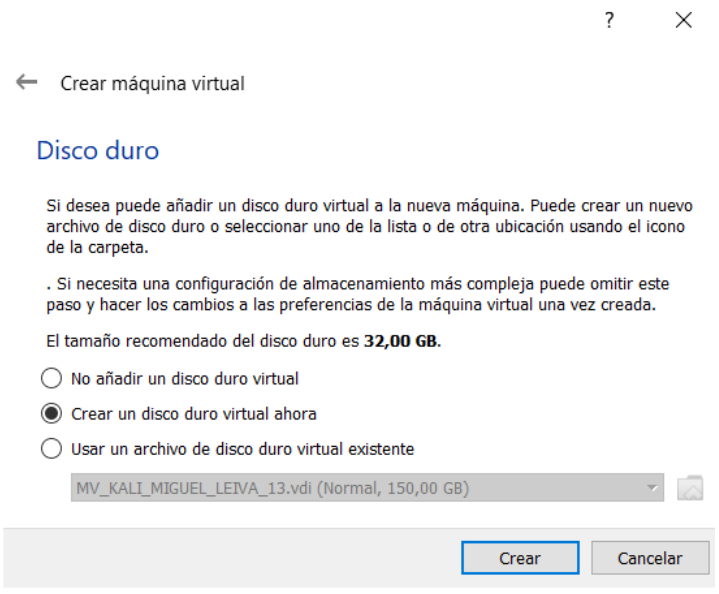
Ilustración 6 Tamaño de memoria VirtualBox



Fuente: Propia

Se crea un disco virtual

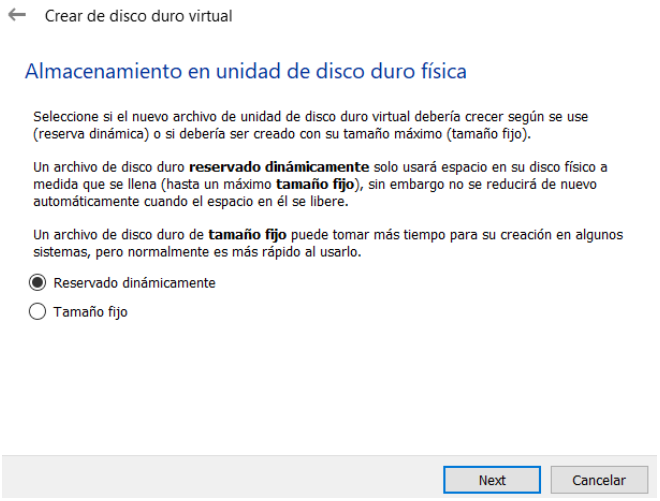
Ilustración 7 Disco Virtual



Fuente: Propia

Se reserva el tamaño del disco dinámicamente.

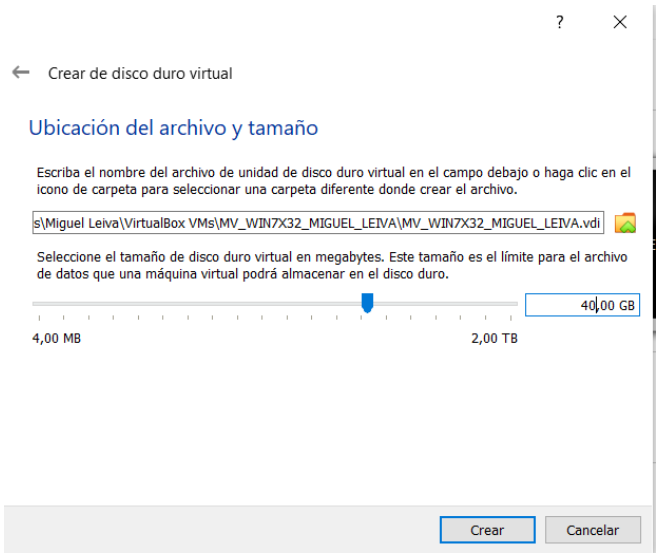
Ilustración 8 Tamaño de Disco



Fuente: Propia

Se selecciona el tamaño del disco.

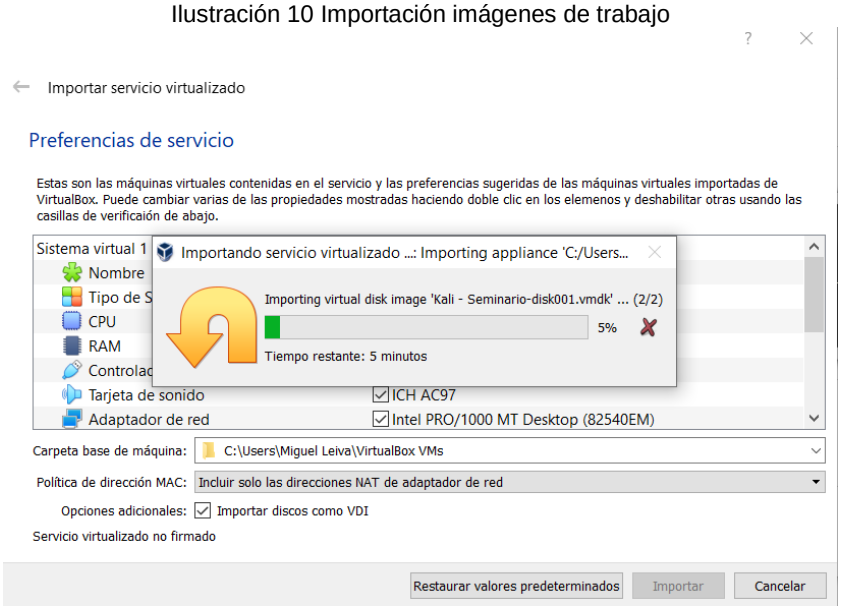
Ilustración 9 Memoria del disco



Fuente: Propia

Dado que se generaron los servicios de virtualización de los 3 sistemas operativos, solo se deben importar dichos sistemas.

Ilustración 10 Importación imágenes de trabajo

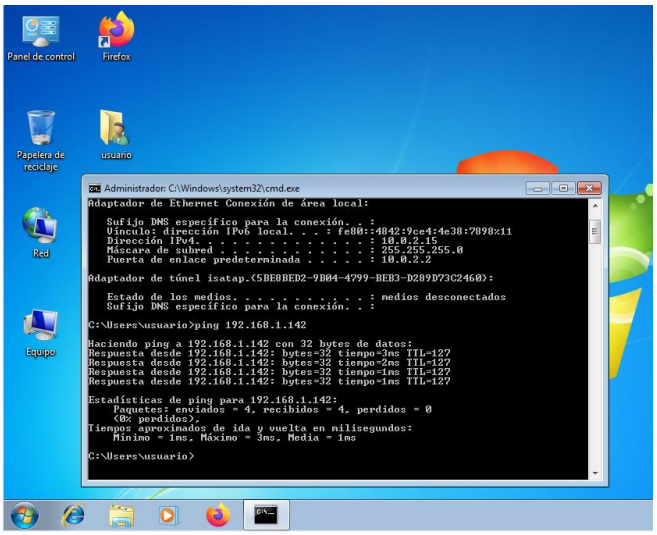


Fuente: Propia

2.1.5 Paso C: Validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux.

Ping de la maquina Windowsx64 a la maquina Windowsx32

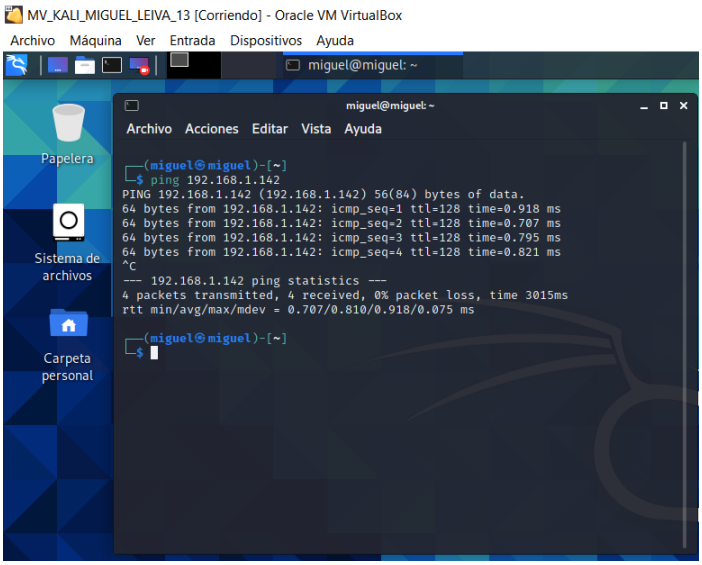
Ilustración 11 Ping WIN x64 a x32



Fuente: Propia

Ping de maquina con Kali Linux a máquina Windowsx32

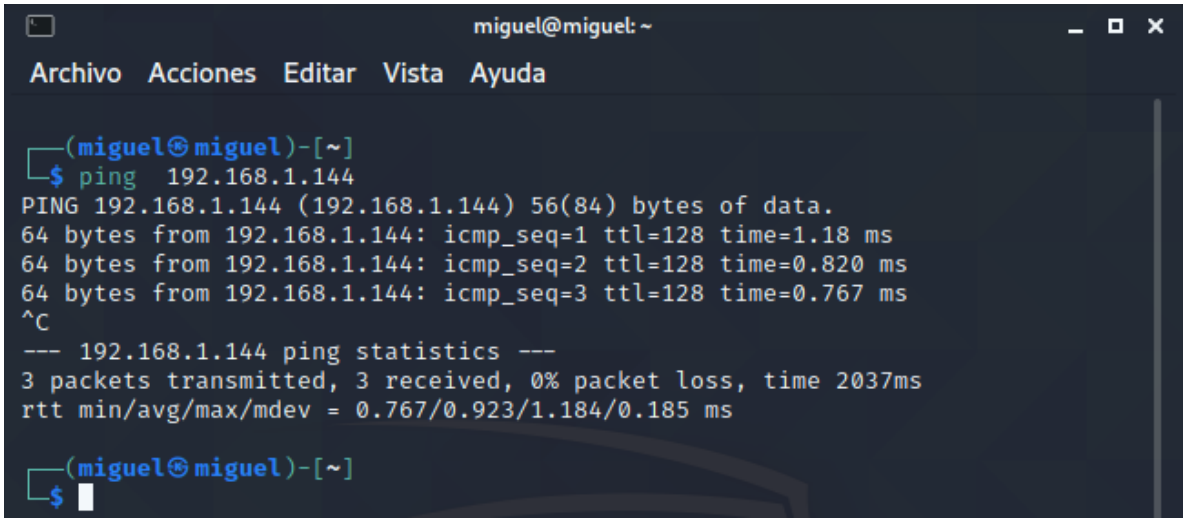
Ilustración 12 Ping Kali a Winx32



Fuente: Propia

Ping de maquina con Kali Linux a máquina Windowsx64

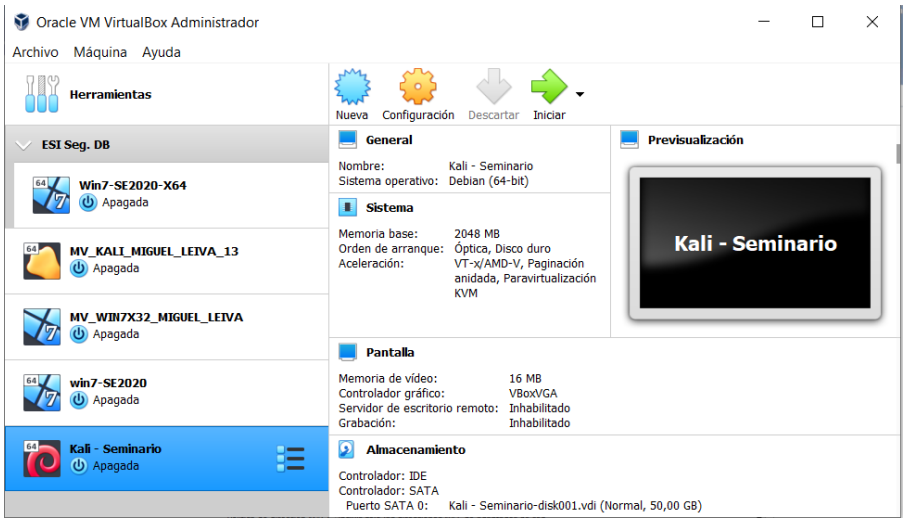
Ilustración 13 Ping Kali a Winx64



Fuente: Propia

2.1.6 Paso D: Evidenciar con printscreen el montaje del banco de trabajo

Ilustración 14 Banco de Trabajo



Fuente: Propia

2.2 DESARROLLO FASE 2

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 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. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

2.2.1 ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo?

Se logra evidenciar en el acuerdo cláusulas que están fuera del marco de ley. En varios apartados de estas cláusulas se menciona que el receptor en este caso el estudiante está en la obligación de mantener confidencialidad con la información tratada incluso si esta proviene de procesos ilegales como lo son chuzadas, interceptación de información y accesos abusivos a un sistema informático, teniendo en cuenta esto el estudiante estaría infringiendo la ley ser consciente de la forma ilegal en la que se obtiene la información y de mantener el silencio de lo mismo, en el código penal de Colombia se menciona este comportamiento como un delito de encubrimiento según el artículo 446 del código penal colombiano. Adicionalmente también se evidencia como en las cláusulas la empresa busca limitar su responsabilidad y obliga al receptor a aceptar la culpa en caso de que se le encuentre algún tipo de información ilícita por parte de las autoridades competentes.

En resumen, estas cláusulas comprometen negativamente al estudiante, que decida participar en esta organización.

Como acuerdos ilegales se encontraron las siguientes clausulas:

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

Segunda. Definición de información confidencial

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

Cuarta. Obligaciones de la parte receptora:

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

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

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

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

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

Quinta. Obligaciones de la parte reveladora:

Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.

Que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

La ley 1273 de 2009 contempla la protección de la información y de los datos, para así tipificar los delitos informáticos, sus sanciones y condenas penales. Según el acuerdo a firmar y la ley colombiana se considera que este acuerdo vulnera los siguientes artículos de la ley 1273 de 2009:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.

Los artículos 269ª, 269C y 269E se pueden considerar como violentados en el acuerdo pues en este habla que la información confidencial puede ser obtenida de diferentes formas entre ellas está el uso de métodos ilegales como lo son el acceso

abusivo a un sistema informático, interceptación de datos informáticos y el uso de software malicioso para acceder a los sistemas y extraer la información, al cumplirse la violación de uno de los artículos anteriormente mencionados inmediatamente se está violentando el articulo 269F pues se está accediendo a información personal por medio de métodos ilegales que violan sus derechos.

2.2.2 ¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? usted como experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio.

Como experto de ciberseguridad no aceptaría este trabajo, puesto que el acuerdo infringe las leyes colombianas como se menciona en los anteriores puntos viola diferentes artículos de la ley 1273 de 2009 y adicionalmente se sale del marco de los acuerdos de ética para el ejercicio de la ingeniería en Colombia ley 842 de 2003, donde el incumplimiento a alguno de estos artículos puede conllevar en sanciones como amonestación escrita, suspensión de la matricula profesional y cancelación de la matricula profesional. En este acuerdo en el articulo 31 se habla de los deberes generales de los profesionales donde se menciona que se deben denunciar los delitos, contravenciones y faltas al código como lo seria en el caso del acuerdo establecido con la empresa WhiteHouse. También se encuentran en el articulo 32 las prohibiciones para los profesionales donde no es permitido tolerar o facilitar el ejercicio ilegal de alguna actividad, como se puede apreciar el código de ética COPNIA regula el comportamiento que debe de seguir un profesional en el marco de la ingeniería y este comportamiento se vería afectado por el planteamiento ilegal en los acuerdos ofrecidos por la empresa.

2.2.3 Deberá buscar la noticia del caso “OPERACIÓN ANDROMEDA BUGGLY” en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.

La operación Andrómeda buggly que al parecer fue creada con fines legales para obtener información de procesos de ciberseguridad, perdió su rumbo pues según testigos esta operación desvió sus principales objetivos para la extracción de información de forma irregular utilizando esta información extraída con fines de lucro. Aun que el ejército argumento que esto fue ejecutado por los civiles que asistían allí y que su falla radicaba en no poder controlar lo que estas personas realizaban en los laboratorios que se llevaban a cabo en estas instalaciones, no obstante, existen testimonios y pruebas que demuestran lo contrario y revelan una participación del personal militar en estas actividades ilícitas.

Teniendo en cuenta lo anterior se puede hablar de una violación a los siguientes artículos de la ley 1273 de 2009:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269E: Uso de software malicioso
- Artículo 269F: Violación de datos personales.

Según la información obtenida en la investigación, parece ser que esta fachada realizo interceptación de datos informáticos violando así los datos personales de varias personas donde se encuentran objetivos como el ELN y la guerrilla, esto se presenta por medio del uso de software malicioso el cual capturaba la información que se digitaba en los equipos, tomaba capturas de pantalla y registraba el tráfico de red para posteriormente enviar esta información al mismo sitio donde se alojaba la Web de buggly.

2.3 DESARROLLO FASE 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 v2.3. 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.

2.3.1 Describa las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

Las herramientas utilizadas para el desarrollo de la actividad fueron Nmap y Metasploit a continuación se dará una explicación de la utilidad que tienen estas herramientas.

Nmap – fase de Análisis de vulnerabilidades y amenazas

Esta es una herramienta de código abierto para explorar la red y realizar auditorías de seguridad, esta herramienta utiliza paquetes IP para determinar que equipos se encuentran disponibles en una red. Gracias a esta herramienta se puede determinar los servicios como son nombre y versión de la aplicación, sistemas operativos, tipos de cortafuegos que se están ejecutando.

La base de Nmap es el análisis de puertos, pero también cuenta con otras capacidades como:

- Mapeo de red
- Detección de SO
- Descubrimiento de servicios

- Auditorias de seguridad

Ilustración 15 Nmap

Fuente: https://paraisolinux.com/que-es-y-como-usar-nmap/

Metasploit – FASE DE Acceso al sistema

Es una herramienta desarrollada en Perl y Ruby, está enfocada en auditorias de seguridad, esta herramienta tiene muchos exploits, los cuales se aprovechan de vulnerabilidades conocidas, con unos módulos conocidos como payloads donde está el código que explota vulnerabilidades. También dispone de otros módulos conocidos como encoders el cual contiene código para evadir un antivirus o sistemas de seguridad. Adicionalmente permite interactuar con otras herramientas externas como son Nmap.

Ilustración 16 Metasploit

Fuente: https://jesusfernandeztoledo.com/instalacion-de-metasploit-en-kali-linux/

2.3.2 Liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 7 X64.

En el anexo 4 se explica de forma detallada los sucesos acontecidos en la organización, los cuales fueron clasificados de la siguiente forma:

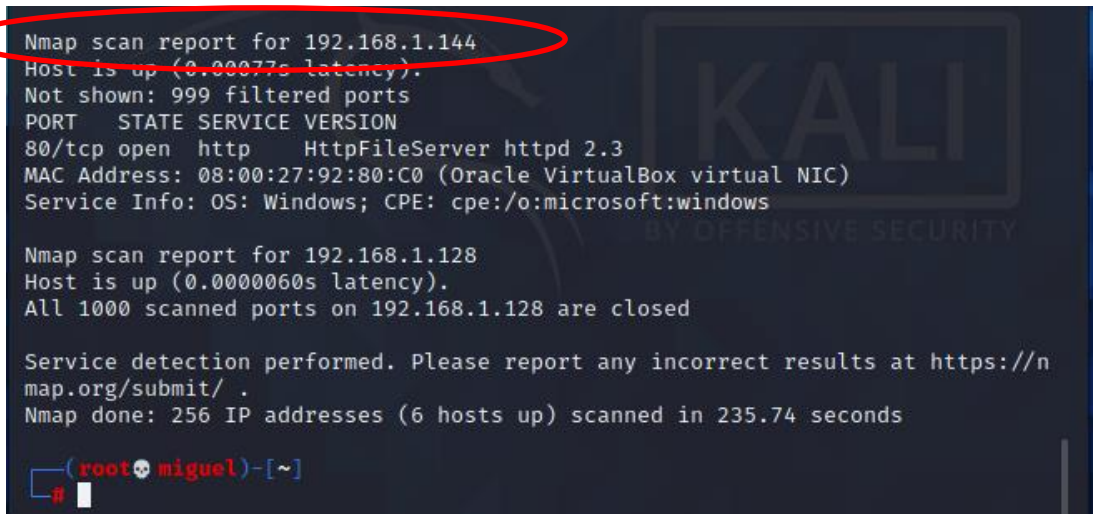
- Sistema operativo Windows 7 x 64
- Aplicación rejetto v 2.3
- Fuga de información
- Shell reversa y sesión abierta de meterpreter
- Escalamiento de privilegios

2.3.3 ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 7"? ¿Qué puerto abre la aplicación específica en el anexo?

Para identificar los fallos de seguridad de la maquina Windows, se utilizo el sistema operativo Kali Linux, dentro de allí se utilizó la aplicación Nmap el cual permite explorar la red y detectar los servicios activos que tiene la aplicación en este caso en específico se utilizó el siguiente comando:

Nmap -sV 192.168.1.0/24 el cual nos permite saber los servicios y versiones que están en la red, según los resultados se puede apreciar que la aplicación abre el puerto 80 y que la versión de esta es la 2.3

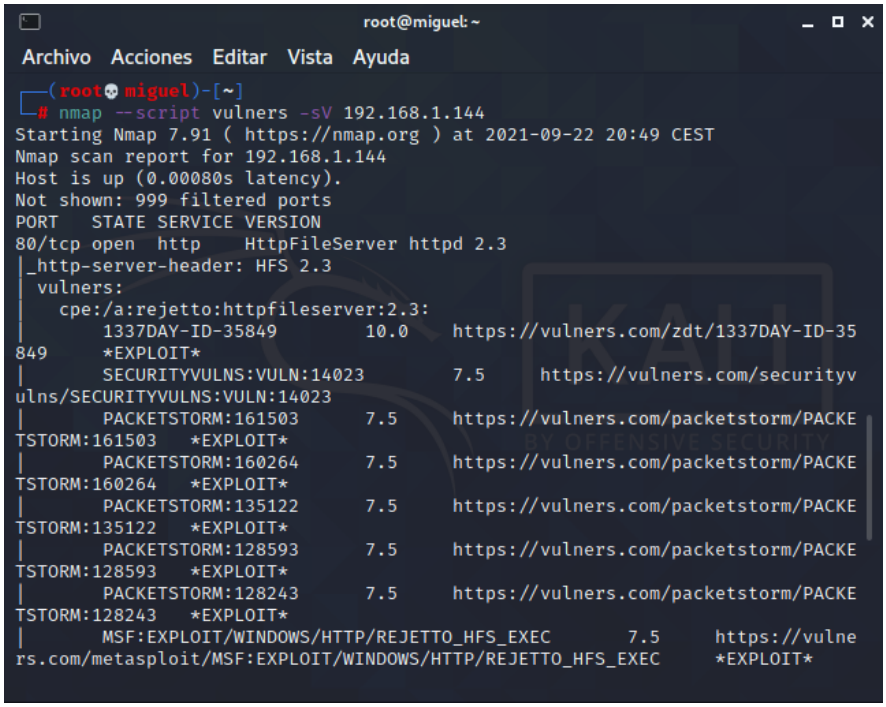
Ilustración 17 Puertos Abiertos



Fuente: Propia

Conociendo esta información se ejecuta el siguiente comando para detectar las vulnerabilidades de la aplicación: nmap –script vulners -sV 192.168.1.144

Ilustración 18 Vulnerabilidades nmap



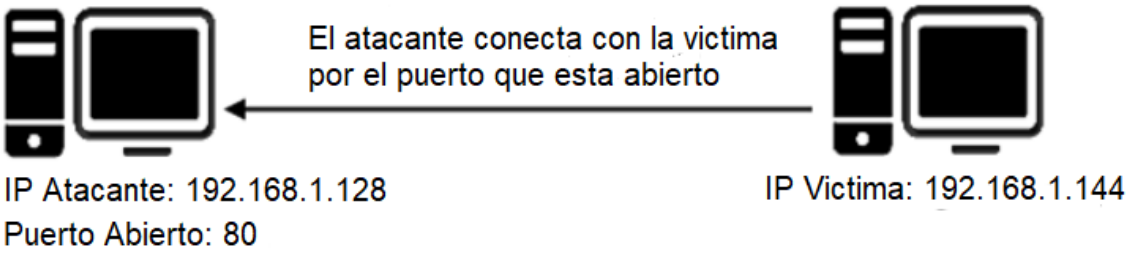
Fuente: Propia

Como se aprecia en la ilustración nmap por medio del script conecta con una Api de la página www.vulners.com la cual es una página que recolecta información de vulnerabilidades.

2.3.4 Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.

Una Shell reversa se da cuando la maquina host en este caso la víctima, se comunica hacia el atacante por medio del puerto que está abierto, en este caso el puerto 80 que está utilizando la aplicación rejetto V 2.3, al obtener esta comunicación permite a la maquina atacante acceder a la maquina victima con una Shell y ejecutar cualquier tipo de comando, en el caso de la empresa se ve que por medio de la creación de un usuario con privilegios se extrajo la información del equipo, sin embargo al tener acceso a la maquina esta es vulnerable a cualquier tipo de ataque que se quiera realizar en la máquina.

Ilustración 19 Shell Reversa



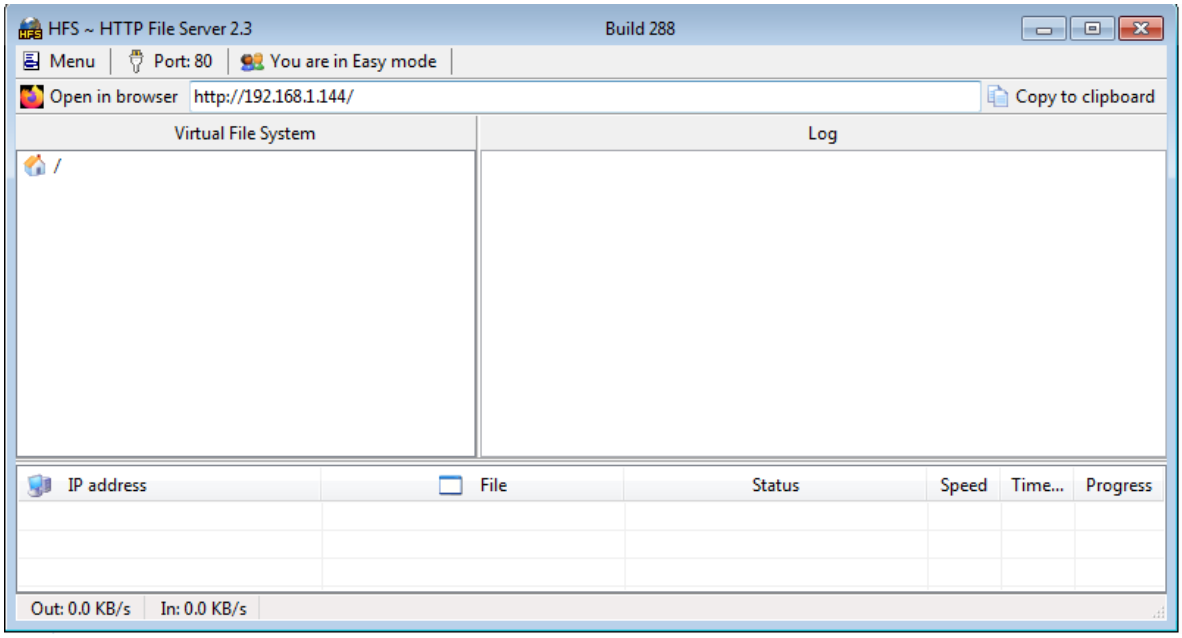
Fuente: Propia

2.3.5 Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Los pasos para el desarrollo de la actividad son los siguientes:

Visualización del aplicativo rejetto instalado en la maquina Windows 7 x 6

Ilustración 20 Aplicación rejetto



Fuente: Propia

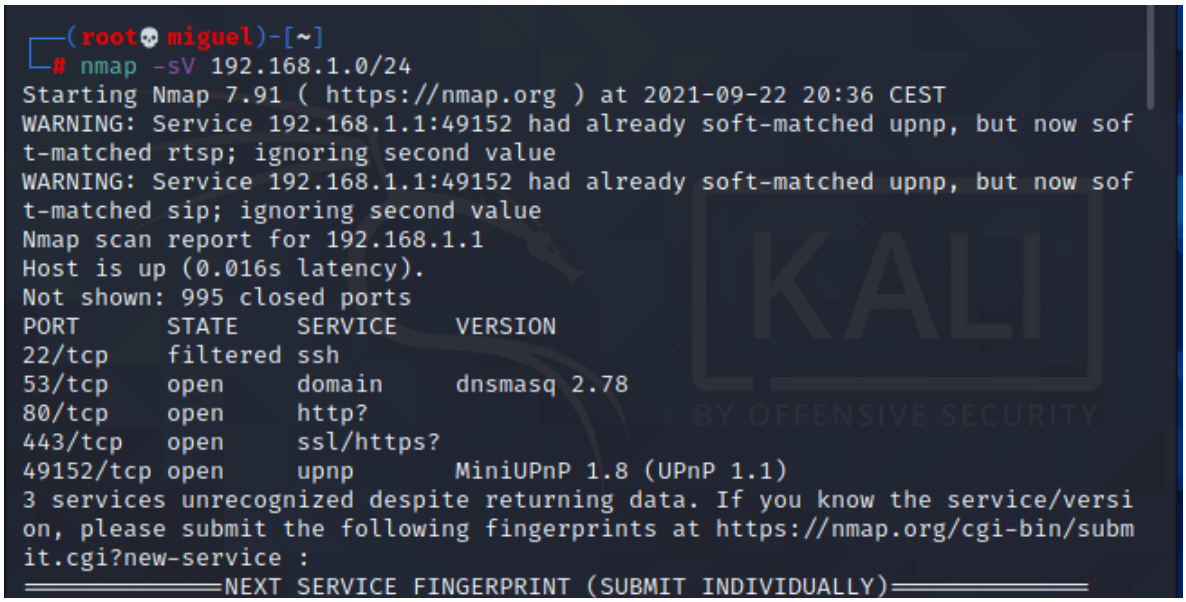
2.3.6 FASE DE RECOLECCION DE INFORMACION.

Como su nombre lo indica en esta fase se debe recolectar la información del equipo y por donde se esta vulnerando dicho sistema, al analizar el Anexo 4 se evidencia que existe un software instalado en el sistema llamado rejetto V 2.3 el cual tiene ciertas vulnerabilidades que pueden ser aprovechadas por un atacante, este software es utilizado para compartir documentos con otros dispositivos. Por lo cual se procede a documentar por Google las vulnerabilidades que tiene este software.

2.3.7 ANALISIS DE VULNERABILIDADES Y AMENAZAS

En esta fase se realiza en análisis de vulnerabilidades y amenazas del sistema operativo. Para detectar las vulnerabilidades de la maquina victima utilizamos la herramienta nmap en primer lugar para descubrir que sistemas y versiones están conectados en la red se utiliza el comando nmap -sV 192.168.1.0/24 como se ve en la imagen.

Ilustración 21 Detección de los pc en la red local



Fuente: Propia

```
Nmap scan report for 192.168.1.144
Host is up (0.00077s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.128
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.1.128 are closed

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 235.74 seconds

┌──(root💀 miguel)-[~]
└─#
```

Fuente: Propia

Por medio del comando nmap -A 192.168.1.144 se puede obtener una exploración más a fondo de la víctima.

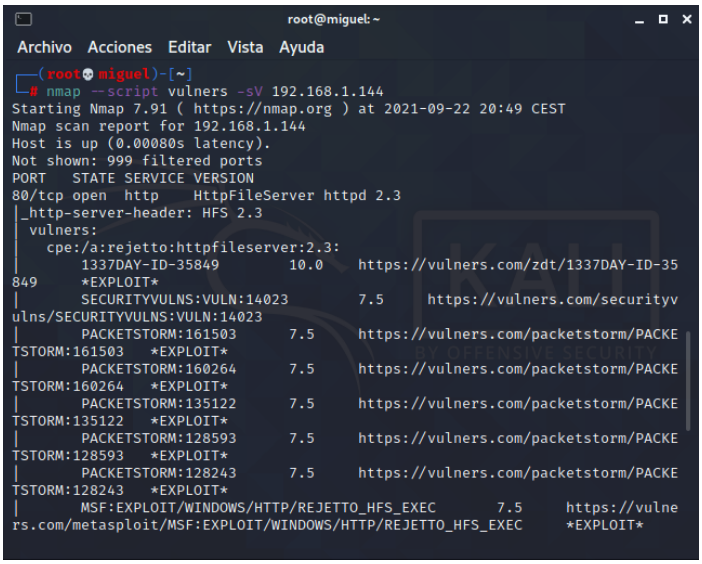
Ilustración 22 Exploración agresiva

```
root@miguel: ~
Archivo  Acciones  Editar  Vista  Ayuda

┌──(root💀 miguel)-[~]
└─# nmap -A 192.168.1.144
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-22 20:43 CEST
Nmap scan report for 192.168.1.144
Host is up (0.00068s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_
vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Window
s Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows
Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vi
sta SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
```

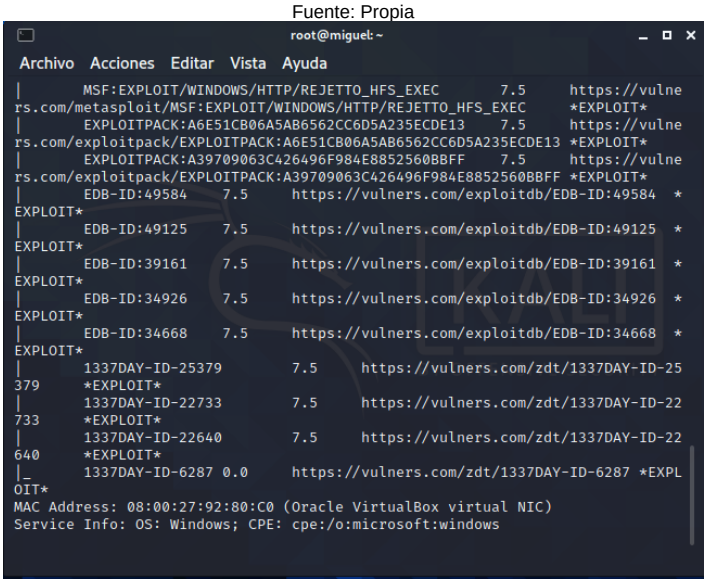
Fuente: Propia

Escaneo de vulnerabilidades con script, realiza una petición a un servidor remoto una API de www.vulners.com para detectar si existen vulnerabilidades conocidas para el equipo.

Ilustración 23 Escaneo de vulnerabilidades



Fuente: Propia

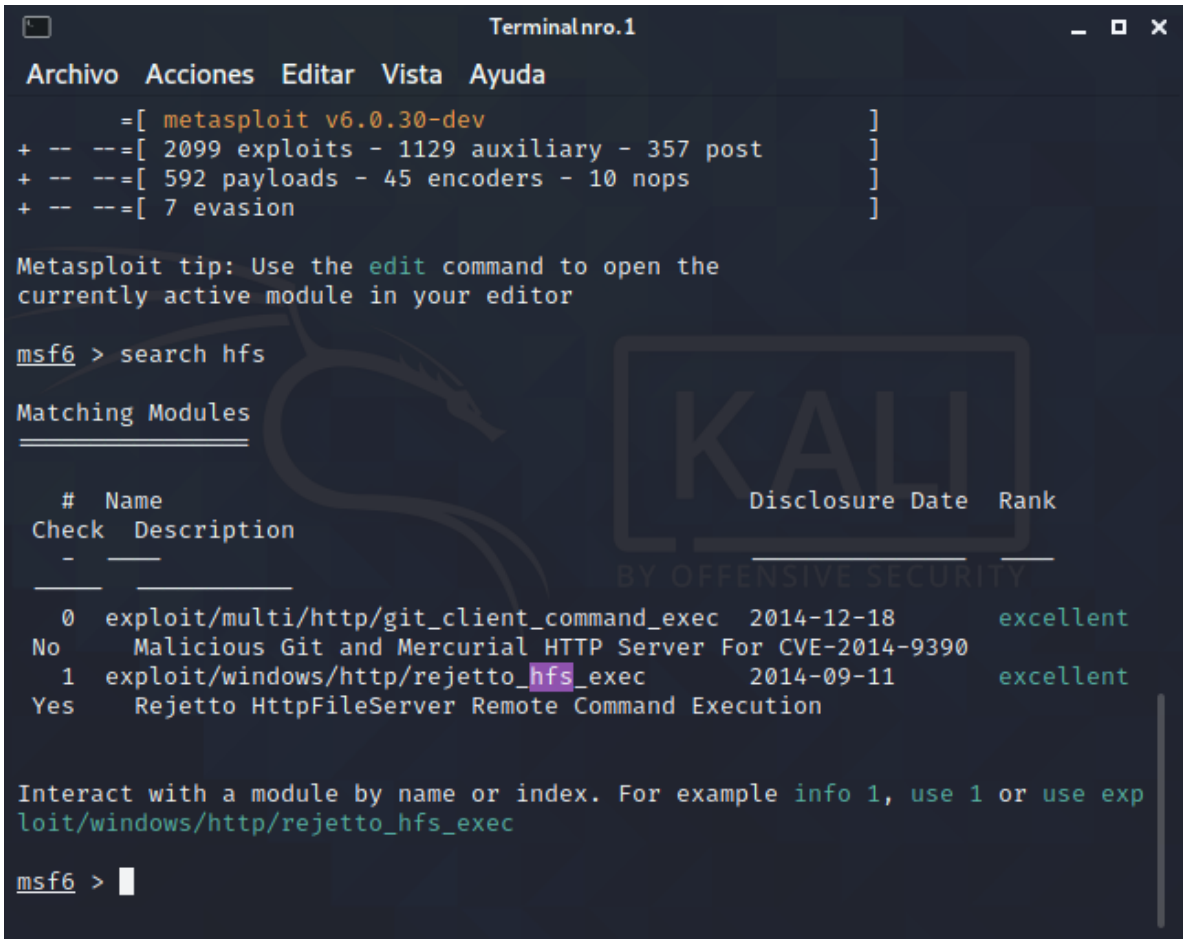


Fuente: Propia

2.3.8 FASE DE ACCESO AL SISTEMA

Al analizar la información obtenida, se establecen que tipos de ataque se ejecutaran y el objetivo de los mismos. Para esta fase se utiliza la herramienta Metasploit, se usa el comando search hfs.

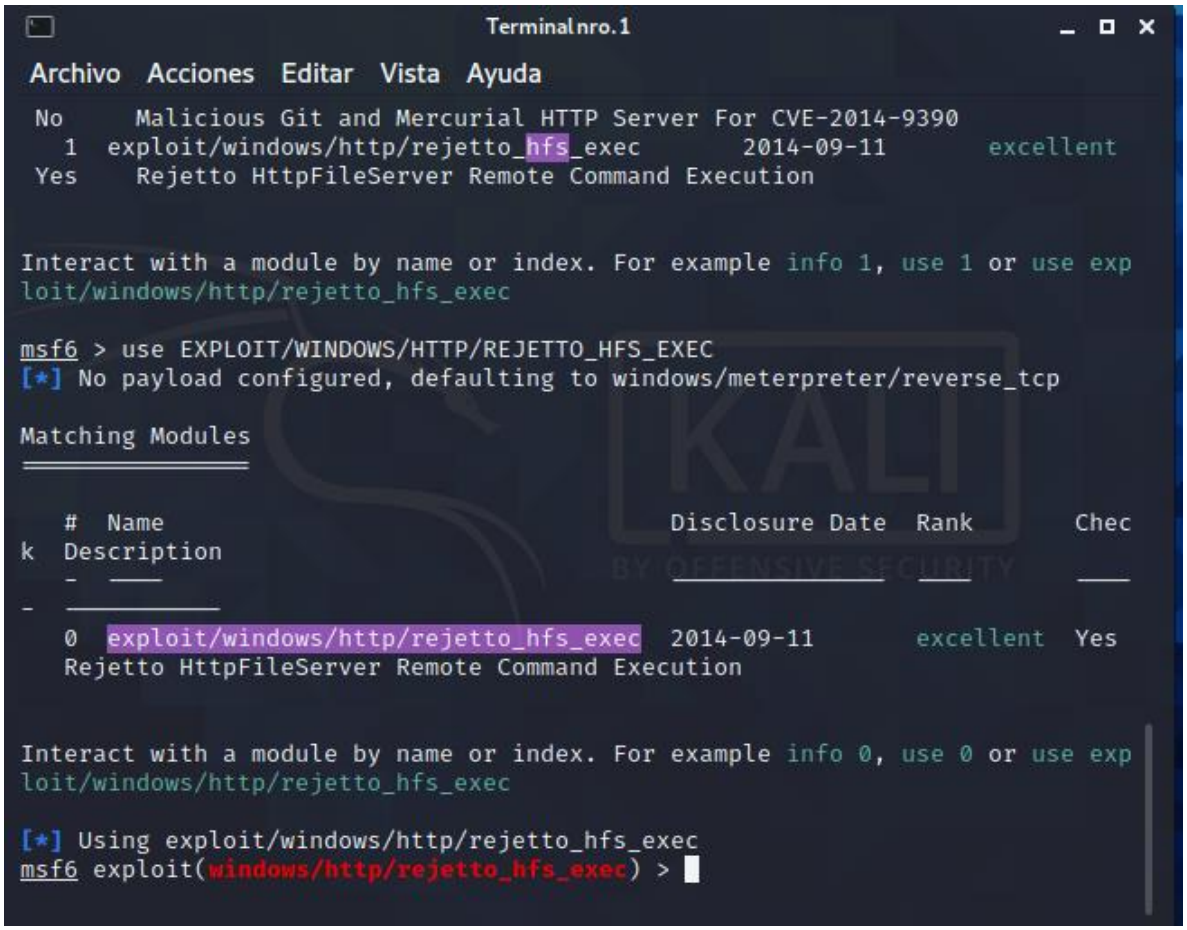
Ilustración 24 Buscando vulnerabilidades con metasploit



Fuente: Propia

Según los exploits detectados por Nmap y Metasploit se ejecuta el comando use exploit/Windows/http/rejetto_hfs_exec

Ilustración 25 Ejecutando los exploits



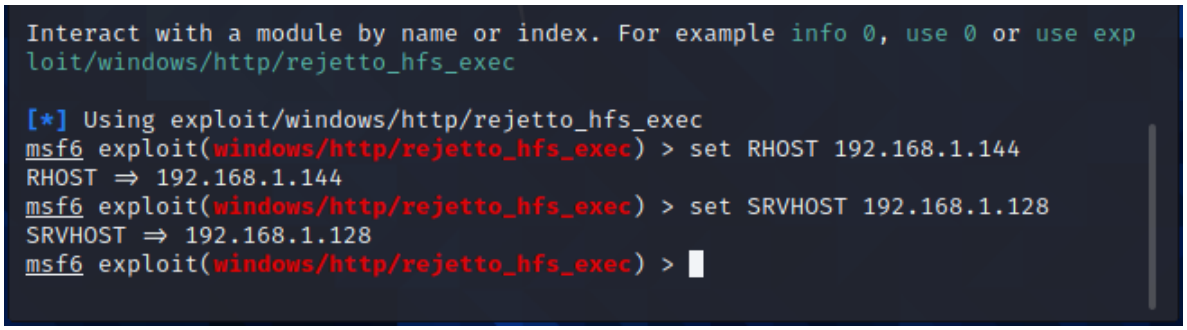
Fuente: Propia

Posterior a ejecutar este comando es necesario configurar el exploit para eso vamos a utiliza el comando SET que permite establecer las variables, en este caso es necesario configurar la IP de la máquina que vamos atacar y la IP de la maquina donde tenemos instalad Kali Linux

Con set RHOST establecemos la IP de la máquina que vamos atacar

Con set SRVHOST establecemos la IP de la maquina con Kali

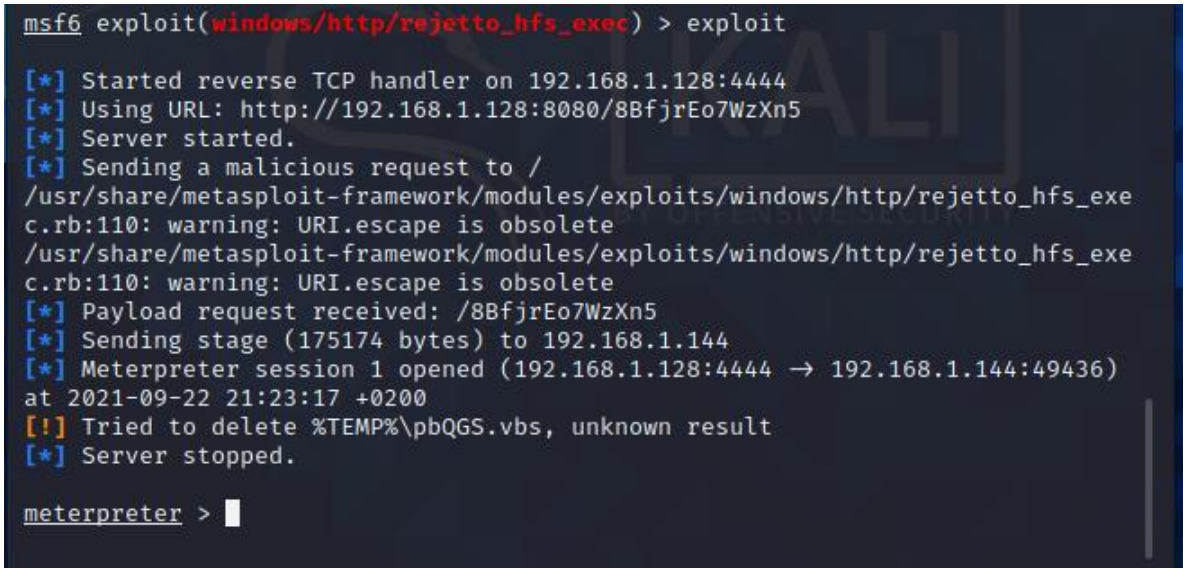
Ilustración 26 Configuración exploit



Fuente: Propia

Luego de tener configurado el exploit se ejecuta el comando exploit para inicial el programa.

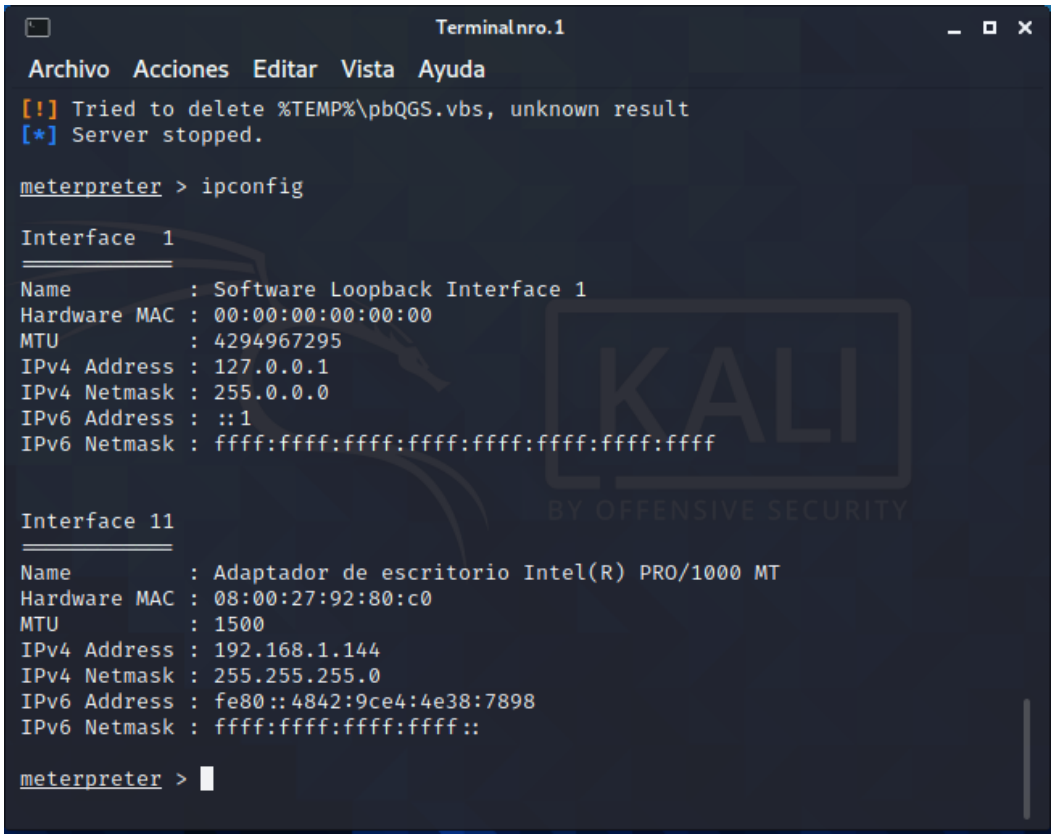
Ilustración 27 Ejecutando el exploit



Fuente: Propia

Para comprobar el acceso a la maquina victima ejecutamos un ipconfig para ver si desde la maquina atacante podemos ejecutar este comando.

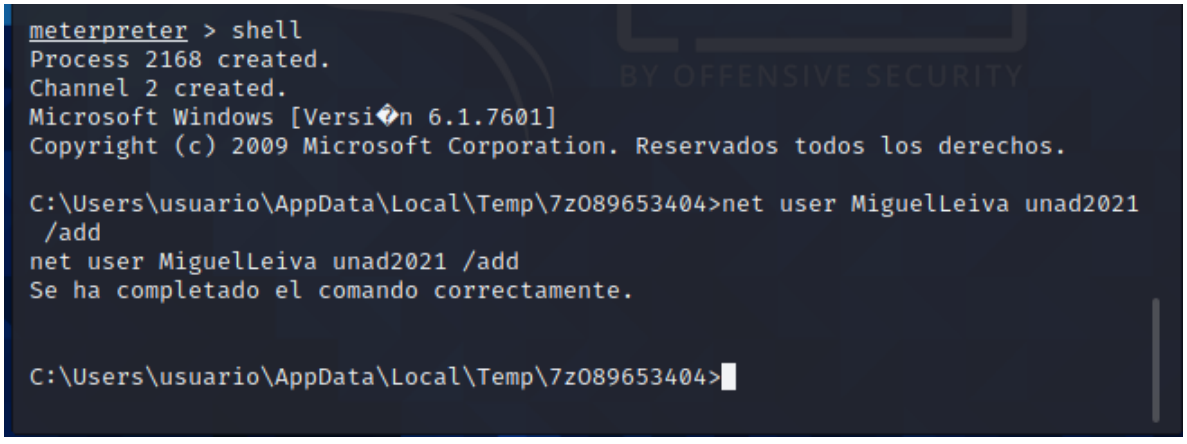
Ilustración 28 ipconfig victima



Fuente: Propia

Ahora accederemos al equipo mediante Shell reversa y crearemos el usuario con el comando net user MiguelLeiva con clave unad2021 /add

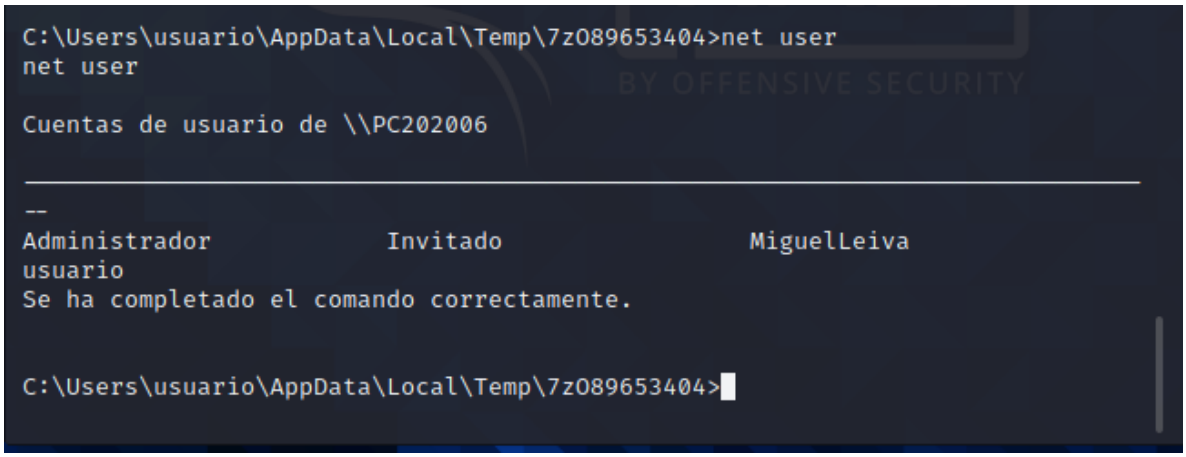
Ilustración 29 Shell reversa y usuario



Fuente: Propia

Verificamos el usuario creado con net user

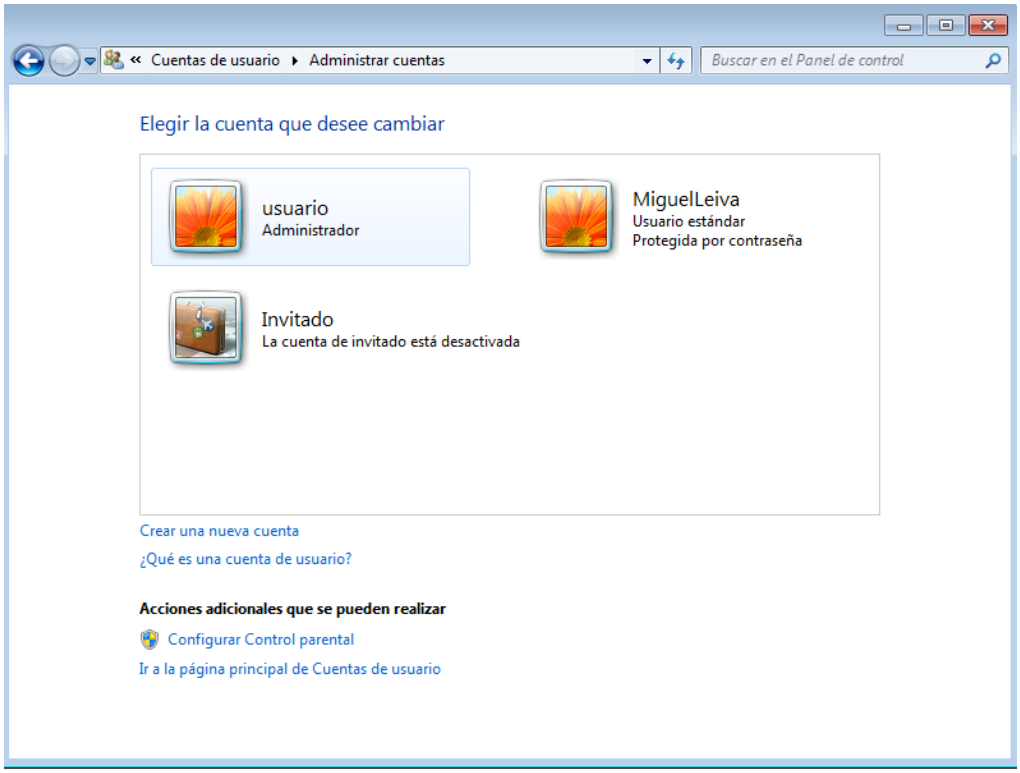
Ilustración 30 usuario



Fuente: Propia

Adicionalmente accedemos al panel de control desde la maquina víctima, cuentas de usuario, administrar cuentas y se evidencia la creación del usuario MiguelLeiva.

Ilustración 31 Comprobación de usuario



Fuente: Propia

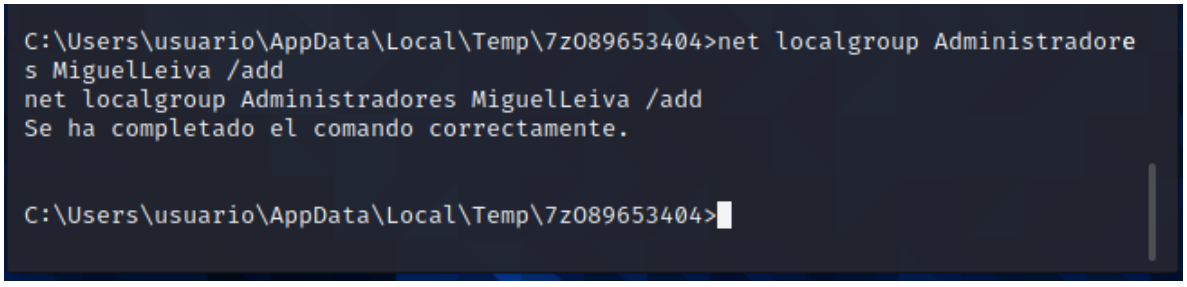
Ahora ejecutamos el comando net localgroup, para ver la carpeta donde trasladar al usuario creado y darle permiso de administrador en este caso se llama “Administradores”

Ilustración 32 net localgroup

Fuente: Propia

Pasamos el usuario a administradores con el comando net localgroup Administradores MiguelLeiva /add

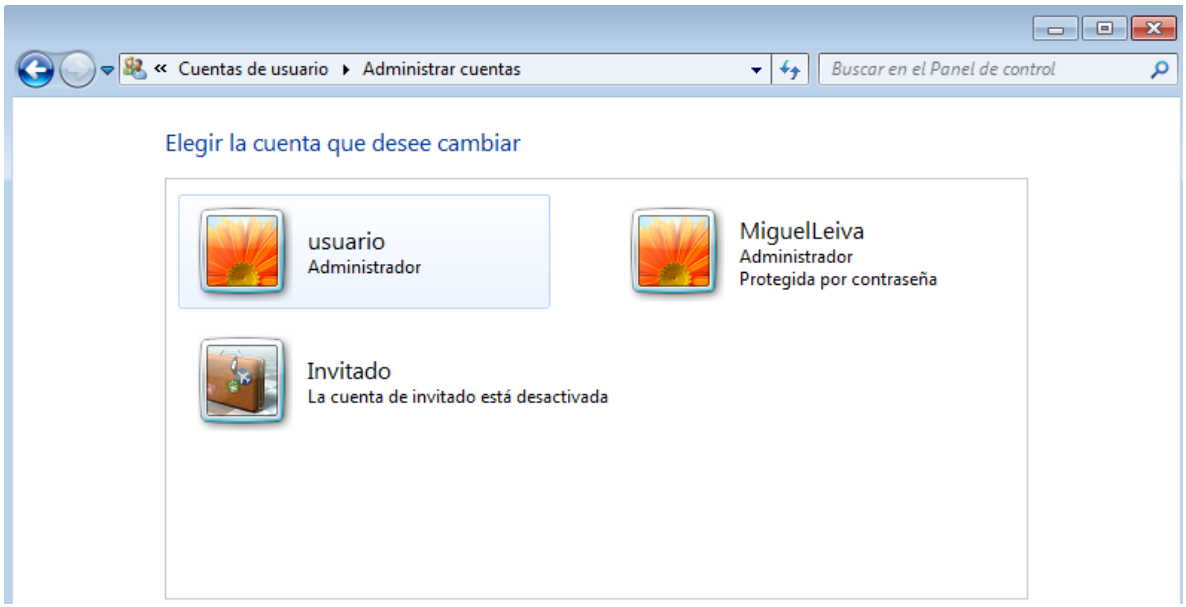
Ilustración 33 usuario administrador



Fuente: Propia

Verificamos nuevamente al Usuario MiguelLeiva como Administrador, según la ruta anterior por el panel de control.

Ilustración 34 Comprobación usuario



Fuente: Propia

2.4 DESARROLLO FASE 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.

2.4.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Para actuar de forma correcta ante un ataque en tiempo real es importante tener en cuenta los siguientes pasos:

Evaluar el incidente: Cuando se detecta un ataque informático se recomienda revisar los sistemas de seguridad con los que cuenta la organización como lo son los logs, IDS, cortafuegos, etc. Posterior a ello se debe identificar que tipo de ataque está afectando la organización pues no todos los ataques funcionan de la misma manera y puede variar el método de contención dependiendo de un ataque a otro. También es importante detectar que sistemas, equipos e información han podido verse comprometidos con este ataque, con esto se logra identificar los activos afectados para posteriormente tomar las medidas necesarias.

Luego de esto se debe determinar el origen del ataque, si este fue efectuado por medio de correo, USB, puertos abiertos, etc. Determinar si este ataque es dirigido intencionalmente a la organización o es un ataque aleatorio, por último, pero lo más importante será registrar y documentar toda la información obtenida en esta fase pues esto servirá para tomar medidas de prevención en el futuro y para contener el ataque de forma adecuada.

Informar el incidente: El trabajo en equipo es parte fundamental de una buena seguridad, sin embargo, a la hora de manejar este tipo de incidentes las únicas personas que deben conocer esta información son aquellas que puedan ser de ayuda a la solución de este, es de vital importancia evitar fugas de información que afecten a la organización aún más.

Contención de daños y minimizar los riesgos: Al detectar un ataque en tiempo real lo mejor es actuar rápidamente para prevenir que el ataque afecte mas sistemas y evitar que el ataque se convierta en un problema cada vez mas grande. Por ello es importante aislar los equipos afectados de la red de la organización para evitar que se siga expandiendo el ataque, clonar los discos afectados o sustituirlos por unos discos nuevos, cambiar las credenciales de todos los usuarios pues están pueden estar comprometidas en el ataque.

Al tener aislado el equipo este debe ser analizado por un experto en seguridad, utilizando herramientas forenses que le permitan analizar detalladamente la información del sistema, de los datos afectados y el objetivo del atacante.

2.4.2 ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

El ataque evidenciado en el ejercicio de Red Team corresponde al aprovechamiento de una aplicación vulnerable llamada Rejetto 2.3 la cual habilitaba el puerto 80 que facilitaba al atacante vulnerar el sistema por esta razón dado que la finalidad del Hardening es endurecer los sistemas para reducir las posibles amenazas se proponen las siguientes medidas:

- Actualización del sistema operativo, activación del firewall y definir reglas de entrada y salida.
- Cierre de puertos innecesarios.
- Endurecimiento de contraseñas para los usuarios.
- Evaluar si es necesario el acceso remoto a la máquina de ser necesario restringir el acceso a un número limitado de usuarios.
- Configuración de los protocolos de red.
- Configurar un sistema de respaldo de archivos.
- Programar copias de seguridad periódicas.
- Monitoreo constante de los equipos.

2.4.3 ¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Un equipo de respuestas a incidentes informáticos también conocido como CSIRT por sus siglas en ingles es aquel que recibe, analiza y responde ante incidentes de seguridad informática, esta labor se realiza cuando el ataque ya ha sido ejecutado, por lo que las acciones que realiza este equipo de respuestas es análisis de malware, investigación de como se produjo el ataque, ayudar a recuperar los sistemas caídos y gestionar las vulnerabilidades detectadas.

Por otra parte el Blue Team analiza cual es la conducta normal de la empresa verificando que esta misma se cumpla, sin descuidar cualquier comportamiento inusual en la organización, su capacidad de procesamiento les permite abarcar grandes volúmenes de información y cubrir en su totalidad todas las áreas con sistemas informáticos de la empresa, también utilizan herramientas tecnológicas a las cuales se les asignan una reglas de análisis para detectar cualquier movimiento inusual estas herramientas son conocidas como sistemas de detección de intrusos.

Entendiendo estos conceptos su principal diferencia radica en que el equipo Blue Team está en revisión constante de los sistemas para evitar cualquier tipo de amenaza que se pueda presentar mientras que el equipo de respuesta de incidentes

de seguridad actúa únicamente cuando el ataque ya ha tenido éxito y el sistema ha sido vulnerado.

2.4.4 ¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

CIS es una organización que desarrolla diversas políticas y controles relacionados con un conjunto de buenas prácticas en seguridad informática, prueba de ello es que sus CIS Controls y sus CIS Benchmarks son consideradas como el estándar mundial y las mejores prácticas para proteger un sistema en ciberseguridad. Esta organización también actúa como el centro de análisis e información lo que lo convierte en el recurso de referencia para la prevención, protección y respuesta frente a amenazas en ciberseguridad de los Estados Unidos.
´

Todos los controles y mejores prácticas que considera CIS son un factor complementario al trabajo de un equipo Blue Team, por tal motivo utilizar estas normas y la información que posee CIS acerca de las amenazas y ataques en ciberseguridad permiten tener un sistema mas seguro, blindado con las ultimas actualizaciones en tendencias de ciberseguridad.

2.4.5 Explique y redacte las funciones y características principales de lo que es un SIEM.

SIEM es un software diseñado para la gestión de eventos e información de seguridad. Su finalidad es dar información útil a las organizaciones acerca de potenciales amenazas de seguridad que puedan afectar a la línea de negocio de la organización, esto se realiza mediante un análisis de datos de seguridad los cuales se obtienen de diversos sistemas como son antivirus, firewalls, sistemas de detección de intrusos, entre otros.

SIEM abarca tres capacidades detecciones de amenazas, investigación y tiempo de respuesta, por lo que las funciones principales de este son:

- Monitorización de seguridad.
- Detección de amenazas.
- Centralizar la vista de amenazas
- Análisis forense y respuesta a los incidentes.
- Recopilar los logs
- Alertas y notificaciones
- Documentación de todos los eventos detectados y sus tratamientos.

En la actualidad las empresas que desarrollan este tipo de software y que cuentan con una gran acogida por las organizaciones son:

- IBM Qradar
- Arc Sight
- Alien Vault
- Symantec
- McAfee SIEM
- Fortisiem

2.4.6 Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Cisco FireSIGHT

Este es un software que analiza la actividad en la red dentro de la organización en busca de código malicioso o que esté prohibido según las políticas de seguridad de la empresa, también monitorea las conexiones de los usuarios para prevenir que estos accedan a dominios sospechosos. Cuando se es detectada una actividad inusual por parte del programa este avisa al motor de servicios de identidad, el cual alerta a las herramientas de seguridad de la red donde entra en juego cisco TrustSec que aísla los dispositivos afectados.

OpenNac

Es un software que permite efectuar escaneos de red, en busca de comportamiento a normal y en caso de detectar algo inusual aislar el dispositivo afectado y responde ante los incidentes que se puedan presentar por la vulneración. Esta herramienta también automatiza las auditorias de seguridad, segmenta la red corporativa automáticamente determinando el tramo de red al que será asignado cada dispositivo.

Cynet

Esta es una herramienta que permite a las organizaciones contar con un nivel de seguridad en sus redes a través de la configuración de la misma, esta herramienta ejecuta análisis en busca de software malicioso y cuenta con la capacidad de aislar los dispositivos afectados en caso de detectar algo inusual.

3 CONCLUSIONES

- Colombia cuenta con diferentes leyes y normativas que ayudan a regular los delitos informáticos en el país, sin embargo, es importante seguir adaptando estas leyes para endurecer las penas ante delitos informáticos.

- La ciberseguridad en un factor importante en cada organización, tener la capacidad de diferenciar los problemas éticos que se evidencian en el entorno laboral le permite al especialista actuar de forma correcta ante cualquier situación.

- La ejecución de pruebas de penetración por parte del equipo Red Team permite a la organización conocer como actuó el ciberdelincuente que vulnero la empresa.

- El equipo Blue Team esta encargado de diseñar, analizar y explorar los sistemas previendo cualquier tipo de anomalía que este relacionada con una falla de seguridad.

- Existen diferentes herramientas de seguridad que permiten a los equipos Red Team y Blue Team ejecutar sus respectivos análisis adecuadamente.

4 RECOMENDACIONES

La ciberseguridad es un campo que mantiene en cambio constante, pues con el pasar de los años la forma en que los ciberdelincuentes actuaban ha ido evolucionando, es por ello que los especialistas en seguridad informática deben estar al tanto de las nuevas amenazas y tendencias tecnológicas que van surgiendo, así mismo tener conocimientos de las leyes que existen en el país donde laboran relacionadas con el cibercrimen y la ciberseguridad.

Sin duda alguna contar con los equipos Blue Team y Red Team facilitan a una organización estructurar una seguridad mas robusta, pues al independizar su esquema de seguridad del departamento de sistemas, le permite tener un mejor control en cuanto seguridad informática, estos dos equipos como se menciona anteriormente son un complemento mutuo pues el Blue Team se encarga de establecer la seguridad de la organización, por medio de análisis, monitoreo, herramientas, creación de reglas, entre otras y cuando este considera que su esquema de seguridad es solido entra en juego el equipo Red Team que pone a prueba dicha seguridad.

5 BIBLIOGRAFÍA

(2021, 12 mayo). Tutorial y listado de comandos más útiles para Nmap. Recuperado 22 de septiembre de 2021, de https://protegermipc.net/2018/11/07/tutorial-y-listado-de-comandos-mas-utiles-para-nmap/

A. (2019a, abril 30). ¿Qué es Nmap? Por qué necesitas este mapeador de red. Recuperado 1 de septiembre de 2021, de https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/

C. (2021, 13 mayo). Como actuar ante un ataque informático | Arditec. Recuperado 5 de octubre de 2021, de https://arditec.es/como-actuar-ante-un-ataque-informatico/

CIS (Center for Internet Security). (2021, 24 julio). About us. Recuperado 5 de octubre de 2021, de https://www.cisecurity.org/about-us/

CIRCULAR EXTERNA 052 DE 2007 modificada por la CE 22/10 y CE 026/11 PROYECTO DE MODIFICACIÓN - PDF Descargar libre. (2021). Certicamara. https://docplayer.es/42071447-Circular-externa-052-de-2007-modificada-por-la-ce-22-10-y-ce-026-11-proyecto-de-modificacion.html

COPNIA. (2003). COPNIA (pág. 3 – 18). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Copnia. (2021). Ley 842 de 2003 | Copnia. Recuperado 13 de septiembre de 2021, de https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

D. (2019, 25 febrero). Cisco Seguridad: Detección de amenazas en las organizaciones. Recuperado 5 de octubre de 2021, de https://datacom.global/cisco-seguridad-deteccion-de-amenazas-en-las-organizaciones/

de Adastra, V. T. L. E. (2021, 28 enero). Conceptos Basicos de Meterpreter – MetaSploit Framework. Recuperado 22 de septiembre de 2021, de https://thehackerway.com/2011/04/26/conceptos-basicos-de-meterpreter-metasploit-framework/

de Ceupe, B. (2020, 17 abril). Todo lo que debes saber del pentesting. Recuperado 1 de septiembre de 2021, de https://www.ceupe.com/blog/todo-lo-que-debes-saber-del-pentesting.html

(2020, 5 agosto). Las 8 herramientas imprescindibles de pentesting. Recuperado 1 de septiembre de 2021, de https://www.viewnext.com/8-herramientas-imprescindibles-pentesting/

Gómez, P. (2021, 18 febrero). La tecnología SIEM para la seguridad informática. Recuperado 5 de octubre de 2021, de https://www.icm.es/2020/08/18/tecnologia-siem/

Gomez, V. (2021). Análisis de Vulnerabilidades con Flan Scan – DOJOConf Panamá 2021. Recuperado 22 de septiembre de 2021, de https://dojoconfpa.org/analisis-de-vulnerabilidades-flan-scan/

Hernández, N. Q. (2021, 29 abril). De Andrómeda a los «hackers». Recuperado 13 de septiembre de 2021, de https://www.elespectador.com/investigacion/de-andromeda-a-los-hackers-article-492933/

Navarro, J. L. (2021, 29 julio). El CSIRT y el trabajo de un BlueTeam. Recuperado 5 de octubre de 2021, de https://codespaceacademy.com/blog/csirt-trabajo-blueteam/

Normatividad sobre delitos informáticos. Policía Nacional de Colombia. (2021). Recuperado 15 June 2021, de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos.

OSSEC: El mundo del IDS (Intrusion Detection System) y del HIDS (Host IDS). (2021). Recuperado 5 de octubre de 2021, de https://www.elladodelmal.com/2020/11/ossec-el-mundo-del-ids-intrusion.html

P. (2019, 24 marzo). ¿Qué es Metasploit y cómo utilizarlo correctamente? Recuperado 1 de septiembre de 2021, de https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente/

Pasos a seguir ante un ataque informático. (2016, 26 octubre). Recuperado 5 de octubre de 2021, de https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

Peñarredonda, J. L. (2015, 9 diciembre). Detrás de Buggly: la historia de la fachada Andrómeda •. Recuperado 12 de septiembre de 2021, de https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Policia Nacional. (2020, 1 julio). Normatividad sobre delitos informáticos. Recuperado 13 de septiembre de 2021, de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Polanco, C. (2020, 7 abril). ¿Qué es un sistema SIEM? | ¿Cómo funciona y cuáles son los mejores? Recuperado 5 de octubre de 2021, de https://sofecom.com/que-es-un-siem/

Smartekh, G. (2021). ¿QUÉ ES HARDENING? Recuperado 5 de octubre de 2021, de https://blog.smartekh.com/que-es-hardening

Uso y comandos importantes de Meterpreter - programador clic. (2021). Recuperado 22 de septiembre de 2021, de https://programmerclick.com/article/39021426263/

User, S. (2021). Cynet, la verdadera plataforma de seguridad - Tecnek Ciberseguridad. Recuperado 5 de octubre de 2021, de https://www.tecnek.com/noticias-ciberseguridad/45-cynet.html

Vera, R. A. (2021, 18 agosto). Qué es OpenVAS. Recuperado 1 de septiembre de 2021, de https://openwebinars.net/blog/que-es-openvas/

Vulners - Vulnerability Data Base. (2021). Recuperado 22 de septiembre de 2021, de https://vulners.com/

vulners NSE Script. (2021). Recuperado 22 de septiembre de 2021, de https://nmap.org/nsedoc/scripts/vulners.html

You are being redirected. . . (2021). Recuperado 5 de octubre de 2021, de https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

Zúniga, C. (2018, 1 diciembre). Net User ¿Cómo crear usuarios en Windows? Recuperado 22 de septiembre de 2021, de https://www.proyectobyte.com/windows/como-crear-usuarios-en-windows-10-8-y-7-desde-cmd-con-net-user/

6 ANEXOS

Link de la Presentación: https://youtu.be/uCvmBP2JI9I

Mis entregas

Sección 1 | Sección 2 | Sección 3 | Sección 4 | Sección 5

Titulo	Fecha de inicio	Fecha límite de entrega	Fecha de publicación	Correcci
ECBTI - Draftbank 1 - Sección 2	13 jul 2021 - 00:00	20 dic 2021 - 23:59	31 dic 2021 - 23:59	

Resumen:

En este espacio puede realizar el envío de los documentos a los que desea verificar el nivel de autenticidad antes de realizar la presentación forma que puede subir archivos en formato **Word**, **PDF**, **PowerPoint** y el tamaño del archivo es máximo **50Mb**.

Cuenta con **cinco** secciones y por cada una puede enviar **un** documento para su revisión de forma independiente. Una vez reciba la revisión, pued documento diferente o el mismo para realizar una nueva revisión

	Titulo de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud	Calificación	Nota general
Ver recibo digital	Seminario Especializado	1670403877	10/10/2021 19:15	27%	N/A	--