Capacidades Tecnicas, Legales y de Gestion Para Equipos Blue Team y Red Team

Walter Camilo Virviescas Rua

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Basicas, Tecnologia e Iingenieria - ECBTI

Seminario Especializado: Equipos Estrategicos en Ciberseguridad: Red Team & Blue Team

(202337164A_1715)

2024

Resumen

El siguiente informe técnico tiene como fin el dar a conocer de manera practica, las actividades mas relevantes que realizan los equipos Red Team y Blue Team, teniendo en cuenta la normatividad Colombiana referente a la ciberseguridad y manejo de datos, junto con la presentación de metodologias aplicables a pruebas de penetracion o pentesting y recomendaciones para la hardenizacion de sistemas de información que den mayor protección a los activos de diferentes tipos de compañias.

***Palabras clave*:** Red Team, Blue Team, Hardenizacion, Ciberseguridad, Normatividad.

Contenido

Lista de Tablas

Lista de Figuras

Glosario

BLUETEAM: Equipos diseñados para la prevención y defensa de ataques cibernéticos

CIBERDELINCUENTE: Persona que utiliza sus conocimientos para cometer delitos informáticos.

CIS: Centro de seguridad de internet

CVE: Identificador único asignado a las vulnerabilidades.

EXPLOIT: Software que aprovecha los fallos que se encuentran en los sistemas informáticos.

REDTEAM: Equipos diseñados para realizar pruebas de ataques cibernéticos controlados.

SIEM: Gestión de información y eventos de seguridad

VULNERABILIDADES: Debilidades que existen en los sistemas y que pueden ser utilizada por atacantes o ciberdelincuentes.

Introducción

Dia a dia se aumenta el trafico de datos por medio de los canales de conexión existentes y esto a generado que se intensifique el accionar de los ciberdelincuentes, que buscan violentar la seguridad de los sistemas y tomar de manera ilegal, información de vital importancia para usuarios y compañias en general. Con esta problemática en aumento, los equipos de Red Team y Blue Team juegan un papel importante dentro de la protección y fortalecimiento de las políticas de seguridad aplicadas por los usuarios a sus sistemas de información , conformando barreras casi impenetrables y a su vez realizando pruebas constantes para identificar cualquier tipo de vulnerabilidad que ponga en peligro sus activos.

Dentro de las pruebas relizadas por los equipos Red Team y Blue Team, se debe resaltar la importancia del cumplimiento de las normas legales y codigos de ética que garanticen la correcta ejecución del accionar y arrojando resultados que ayuden a las compañias y usuarios a resguardar de la mejor manera la información generada por sus sistemas.

Objetivos

Objetivo General

Presentar informe detallado sobre las practicas mas relevantes en equipos Red Team y Blue Team, junto al seguimiento de normativas legales y modelos aplicables a la ciberseguridad.

Objetivos Específicos

- Identificar la normativa legal colombiana sobre delitos informáticos.
- Conocer sobre pruebas de penetracion y herramientas mas utilizadas.
- Realizar ejercicio practico de Red Team.
- Conocer la política legal aplicable a ejercicios de Red Team.
- Conocer sobre las herramientas utilizadas por los equipos Blue Team.
- Realizar recomendaciones para la mejora de ejercicios Blue Team y Blue Team.

Desarrollo del Informe

Dentro de las actividades realizadas en el seminario, se desarrollaron ejercicios propios de los equipos Red Team y Blue Team, para ello se analizo el marco legal Colombiano, etapas de pentesting, algunas de las herramientas mas utilizadas y se configuro ambiente controlado para pruebas logrando la identificación de vulnerabilidades y planes de mejoras y recomendaciones para mitigarlas.

Marco Legal Colombiano

En la legislación colombiana se encuentra enmarcadas diferentes leyes y artículos relacionados con la protección de datos y delitos informáticos. Dentro de ellos se pueden encontrar:

- **Ley 1273 de 2009**. Que se denomina de “la protección de la información y de los datos” Esta ley permite tener bases jurídicas con referencia a la información suministrada y recaudada por cualquier sistema y las consecuencias legales sobre su mal uso, protección y acceso de manera abusiva y sin autorización.

Algunos artículos:

- **Articulo 269A**. Acceso de manera abusiva a un sistema de información.
- **Artículo 269B** Obstaculizar un sistema informático o de red de comunicaciones impidiendo su funcionamiento.
- **Artículo 269C** Interceptar datos informáticos desde su origen, destino o en el interior de un sistema de información
- **Artículo 269F** Acceso, manejo o divulgación de información de carácter personal de manera fraudulenta y sin autorización.

- **Artículo 269H** Las penas se agravan si se comete estos delitos dentro de sistemas de comunicación o redes de carácter estatal o financiero, si se realiza sobre servidor público, revelación de información con fines lucrativos o personales, si es el responsable del manejo de dicho sistema.

LEY 1581 DE 2012 Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

Etapas de Pentesting y Metodologia

Para la realización de pruebas de penetración o Pentesting, es importante contar con un equipo y herramientas adecuadas que den seguridad en los procedimientos realizados y aplicados a cada sistema a evaluar.

Los auditores en ciberseguridad deben cumplir con pasos que den claridad y tranquilidad en los procedimientos realizados y lograr así el objetivo especifico que es la identificación de vulnerabilidades y fallas en el sistema para así generar protección y corrección de este. Algunos pasos a seguir son:

- Determinar los Objetivos.
- Recopilar información
- Acceder al sistema
- Elaboración de informes

Estos pasos son recopilados y ajustados por la metodología **PTES** que da claridad sobre los puntos descritos de una manera más detallada.

Metodología que se aplica por proveedores de servicios de seguridad y que da un marco de referencia para realizar pruebas de penetración, Esta consta de 7 fases:

1. **Interacción previa:** Se concertar los objetivos y acuerdos previos a realizar. Se establecen acuerdos y los procedimientos a realizar.
2. **Recolección de información:** Teniendo en cuenta las necesidades de la organización, se realiza la recolección de la información necesaria para la realización de las pruebas.
3. **Modelado de amenazas:** Con la información recolectada se identifican los activos (Tecnológicos o humanos) más vulnerables y que podrían ser objetivo de ataques.
4. **Análisis de vulnerabilidades:** Se identifican las vulnerabilidades presentes en los activos y que pueden llegar a ser explotables.
5. **Explotación:** Se realiza la explotación de forma silenciosa y de manera ágil, buscando ingresar lo más profundo en el sistema.
6. **Post explotación:** Se realiza el análisis del equipo o sistema explotado, rutas, acceso e impacto, todo de manera controlada y sin afectar al sistema. Se debe garantizar el retorno del equipo a su estado inicial previo a la explotación.
7. **Presentación de reportes:** Se debe presentar el informe completo de las pruebas realizadas, vulnerabilidades encontradas, así como la manera en se debe dar corrección a estas.

Herramientas de Pentesting y Servicios en Linea

MetaSploit

Metasploit es un software de código abierto o también llamado open source que viene preinstalado en los sistemas Kali Linux y que contiene gran cantidad de exploit, más de 900. Es de las herramientas que se mas se utilizan por los equipos Rojos en el hacking ético.

Por medio de Metasploit se pueden poner a prueba las diferentes vulnerabilidades que pueden tener los sistemas informáticos ya que con esta herramienta se pueden ejecutar las siguientes acciones:

- **Escaneo y recopilación de información:** Metasploit utiliza herramientas como nmap para realizar el escaneo de puertos e identificación de puertas de entrada a los sistemas
- **Identificación y explotación de vulnerabilidades:** Identifica que vulnerabilidades están presentes en un sistema y que están publicadas en CVE, de esta menara identifica como explotar dicha vulnerabilidad.
- **Escalada de privilegios:** Cuenta con software que permite la elevación de privilegios como administrador en diferentes sistemas operativos tales como Linux y Windows.
- **Instalación de puertas traseras:** Basado en códigos maliciosos o payloads, instala puertas traseras o backdoors en el equipo víctima, para poder robar información confidencial.
- **Fuzzing:** Automatiza el ingreso de valores aleatorios que pueden ser inesperados o erróneos en la entrada de los sistemas con el fin de identificar fallos que permitan el ingreso a un dispositivo o red.

- **Evasión de sistemas antivirus:** Metasploit contiene herramientas que permite la ofuscación de código o escribir código malicioso que no le permite al sistema de defensa ser detectado.
- **Eliminación de registros de rastros:** Con sus herramientas permite la eliminación de registros o rastros en los logs de los sistemas operativos impactados.

Nmap

Herramienta de auditoría de seguridad y exploración de red de código abierto. Mediante el uso de paquetes IP en su forma original permite identificar qué equipo están disponibles en la red, los servicios y sus versiones presentes, sistemas operativos y sus versiones, cortafuegos y filtros de paquetes, escaneo de vulnerabilidades y diversas características.

Entre los resultados obtenidos podemos encontrar listas de puertos y protocolos con sus servicios y estados con las versiones de cada uno de ellos. De igual forma, llega a mostrar nombres de DNS, direcciones de MAC y tipos de dispositivos.

- Nmap permite especificar objetivos como escanear un IP específica, parte de una red, segmentos o la red completa mediante el método CIDR y el uso de diversos comandos.
- Nmap permite analizar 65535 puertos, entre los que encontramos más de 1660 puertos TCP y cada uno de sus 6 estados, permitiendo obtener información confiable y precisa de su estado.
- Nmap permite a los atacantes identificar las vulnerabilidades de los puertos y servicios presentes en cada uno de los equipos activos en la red gracias a su capacidad de detección de versiones y detalle en cada equipo.

- Nmap analiza más de 1500 huellas resguardadas en sus bases de datos para identificar los sistemas operativos, las cuales son comparadas con los resultados arrojados de paquetes TCP y UDP en el escaneo.

Por otra parte, mediante el uso avanzado y la experiencia en Nmap, es posible evadir cortafuegos e IDS, ya que los usos básicos ya están filtrados o bloqueados por algunos sistemas, haciendo más difícil realizar el análisis de la red

Openvas

Es un potente escáner que permite identificar vulnerabilidades en sistemas de red de pequeño y gran tamaño y que es de código abierto. Cuenta con mas de 50.000 test y registros de vulnerabilidades que a diario son alimentadas por la comunidad y a su vez cuenta con una interfaz grafica que permite su uso de manera más dinámica y agradable.

Por medio de Openvas se puede realizar seguimiento continuo a los sistemas, logrando identificar fallas de diseño y posibles vulnerabilidades tales como la inyección de código SQL.

Openvan viene incluido en el paquete de Kali Linux, aunque es necesaria la configuración de este para que funcione correctamente.

ExploitBD

Es una base de datos publica y en línea que fue desarrollada por la compañía Offensive Security, quien también creo a Kali Linux. Esta Base de datos contiene información sobre vulnerabilidades, exploits y que a su vez contiene los códigos de prueba.

Todas las vulnerabilidades y exploits registrados en esta base de datos, son alimentadas y actualizadas por la comunidad de seguridad y contienen detalles importantes como los sistemas

que pueden llegar a ser afectados, datos importantes y técnicos sobre los sistemas y los códigos más relevantes.

Con estas bases de datos, los profesionales de seguridad cuentan con mas fuentes que les permite identificar los Exploits de diferentes vulnerabilidades detectadas.

CVE

Es un sistema público y en línea que cataloga las vulnerabilidades de seguridad de hardware y sofware y que permite a los fabricantes y expertos en seguridad, identificar las vulnerabilidades y gestionar de maneras más eficiente sus sistemas.

CVE asigna un código único de identificación, a cada vulnerabilidad encontrada y suministra información de la vulnerabilidad, la afectación sobre el sistema y la posible solución a la misma.

Con el uso de CVE los profesionales de seguridad, pueden gestionar mejor los parches y actualizaciones necesaria para los sistemas.

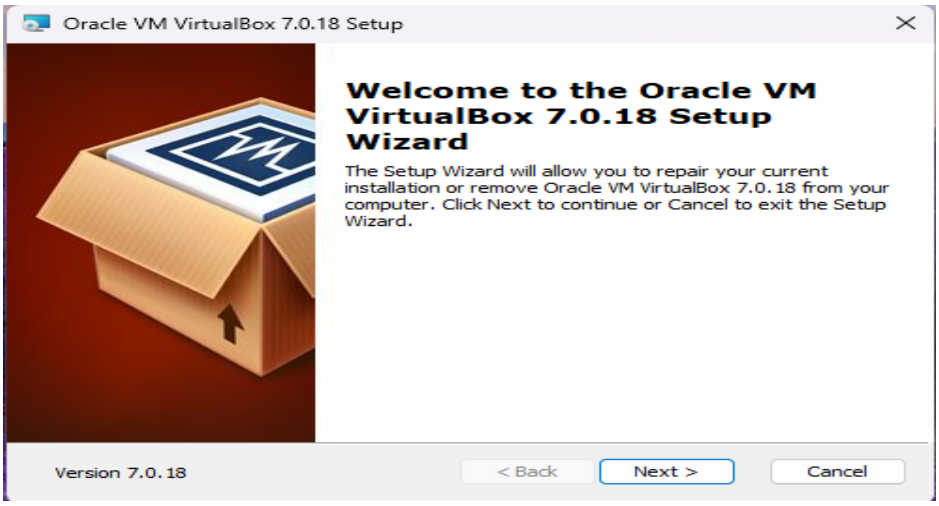
Configuracion de Ambiente Controlado de Pruebas

Para las pruebas en ambientes controlados, se utilizan herramientas tales como VirtualBox, Maquina virtual Windows 7 y Kali Linux.

A continuación se detalla la configuración realizada para el caso ejemplo.

1. Se realiza el descargue de VirtualBox desde la pagina oficial y se procede con la instalación.

Ilustración 1 Instalacion Virtual Box



Fuente Propia

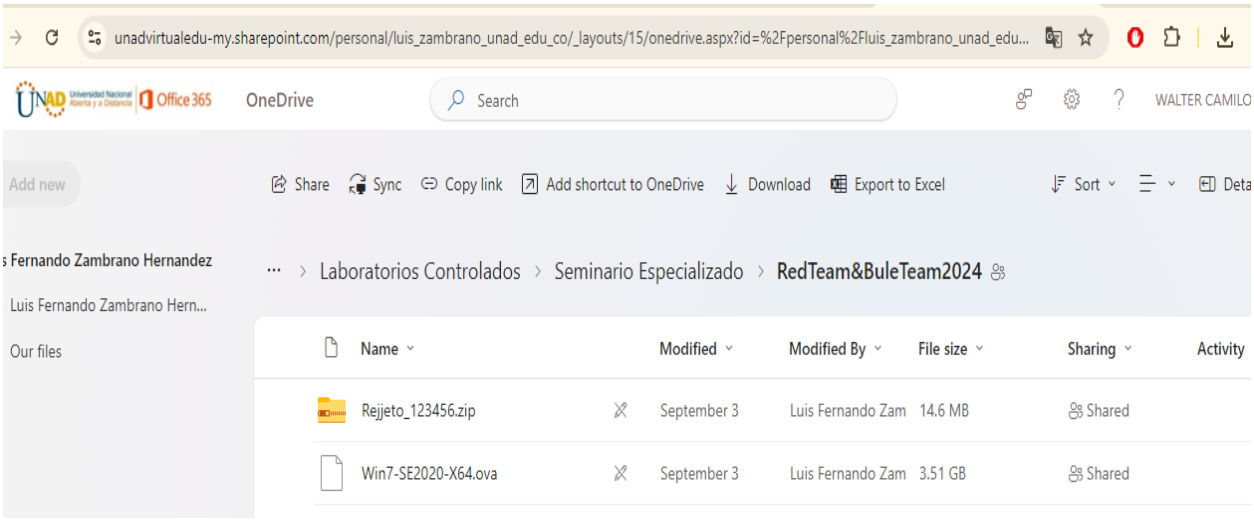
Ilustración 2 VIrtualBox Iniciado

Fuente propia

Configuracion de Ova y Kali Linux

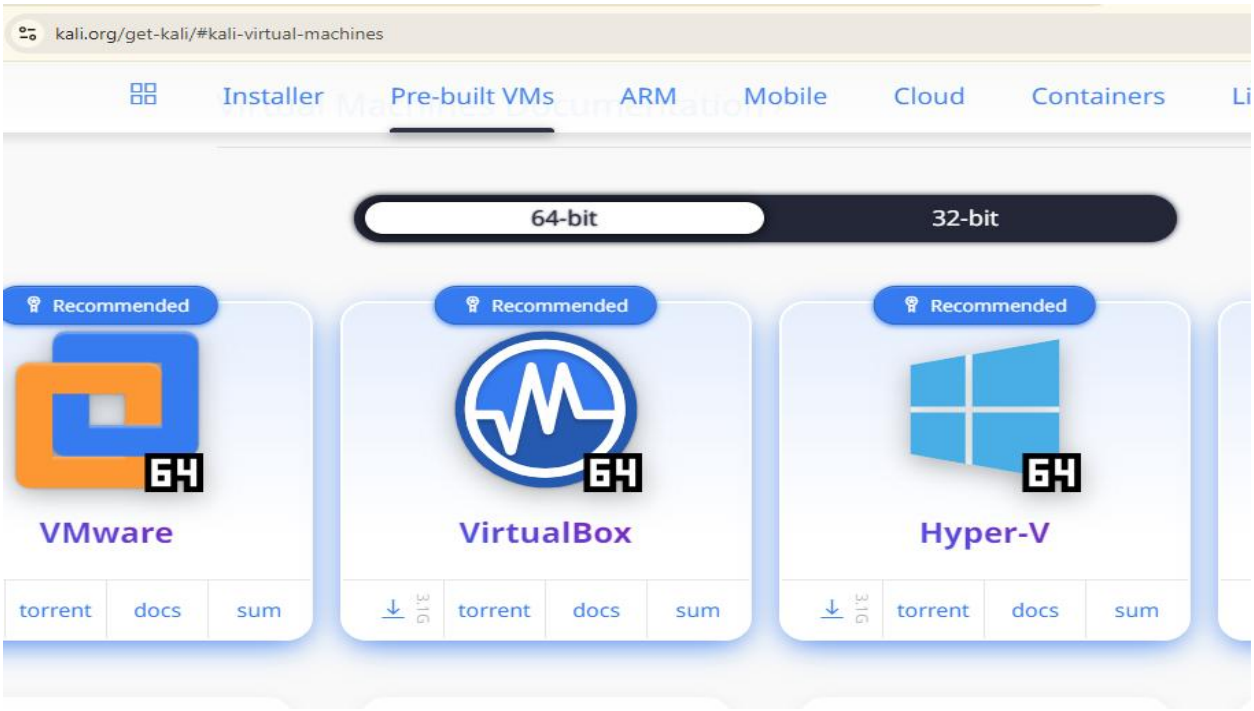
Se descarga Ova de Windows 7 desde la ruta suministrada por la UNAD y el Kali Linux desde la página oficial.

Ilustración 3 Descarga de OVA



Fuente propia

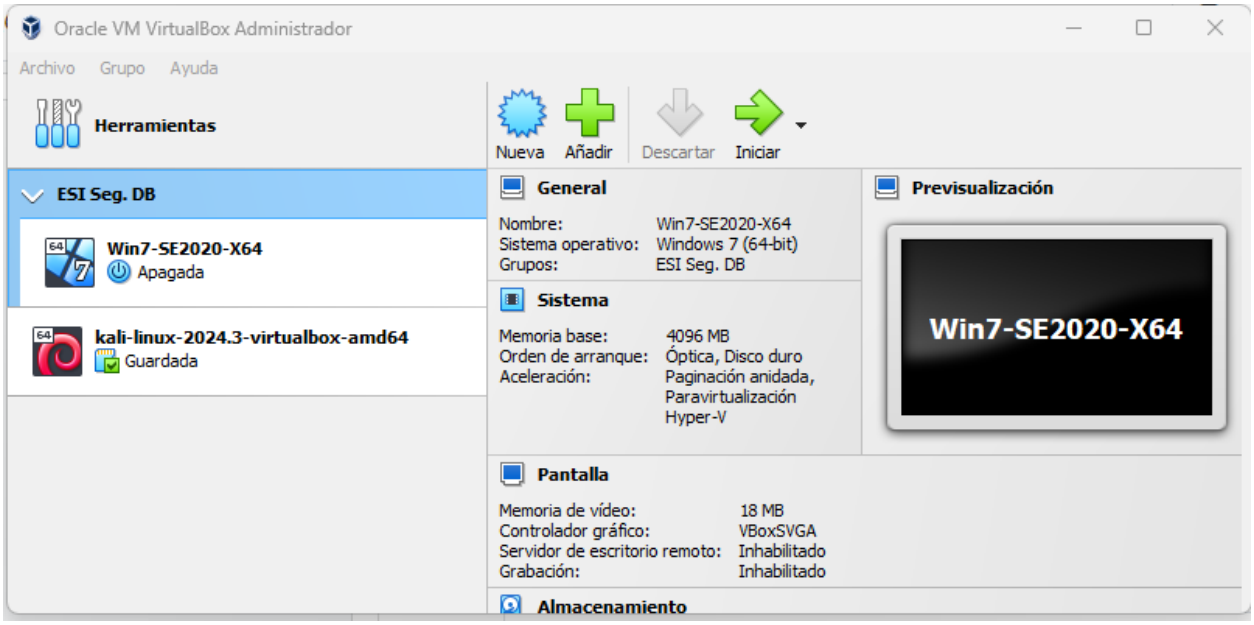
Ilustración 4 Descarga Kali Linux



Fuente Propia

Las descargas son instaladas en VirtualBox

Ilustración 5 Configuracion Maquinas Virtuales

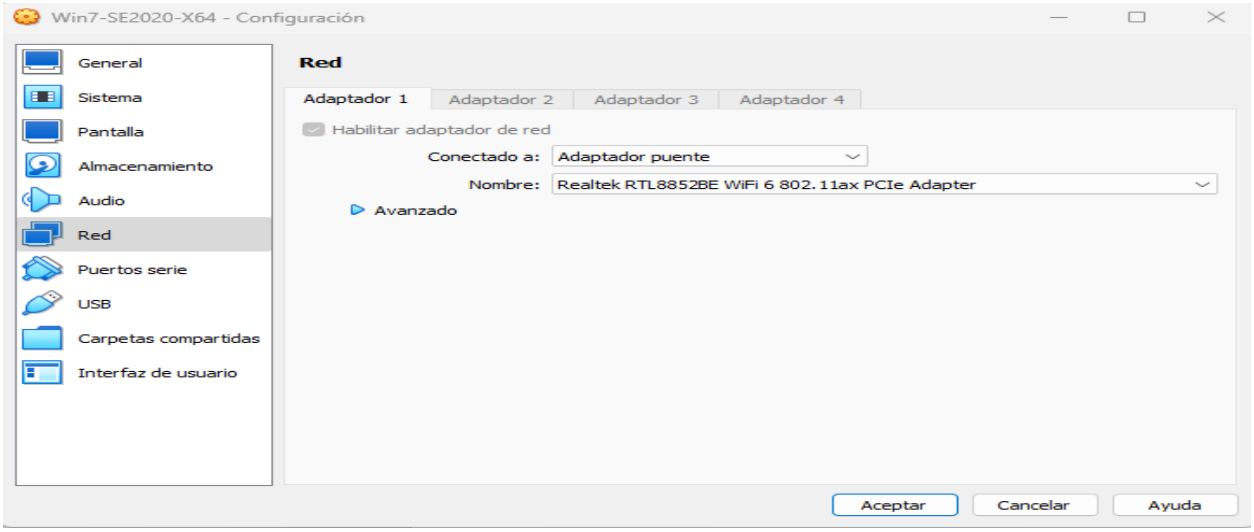


Fuente Propia

Configuracion para la Comunicación Entre las Maquinas.

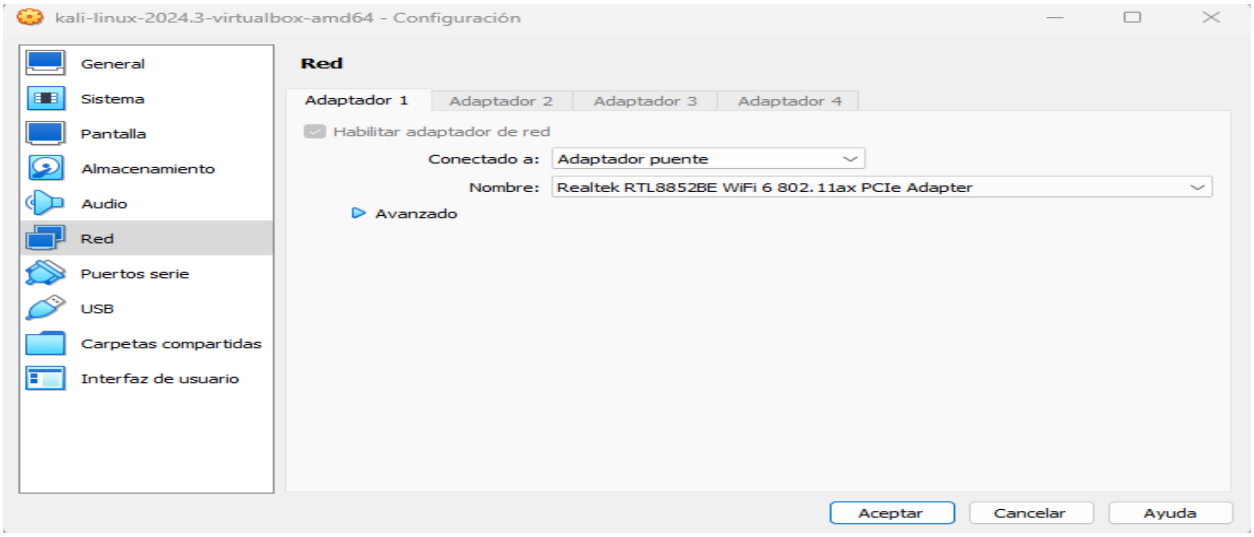
Se realiza configuración de red en adaptador puente en ambas maquinas.

Ilustración 6 WIn 7 Configuracion



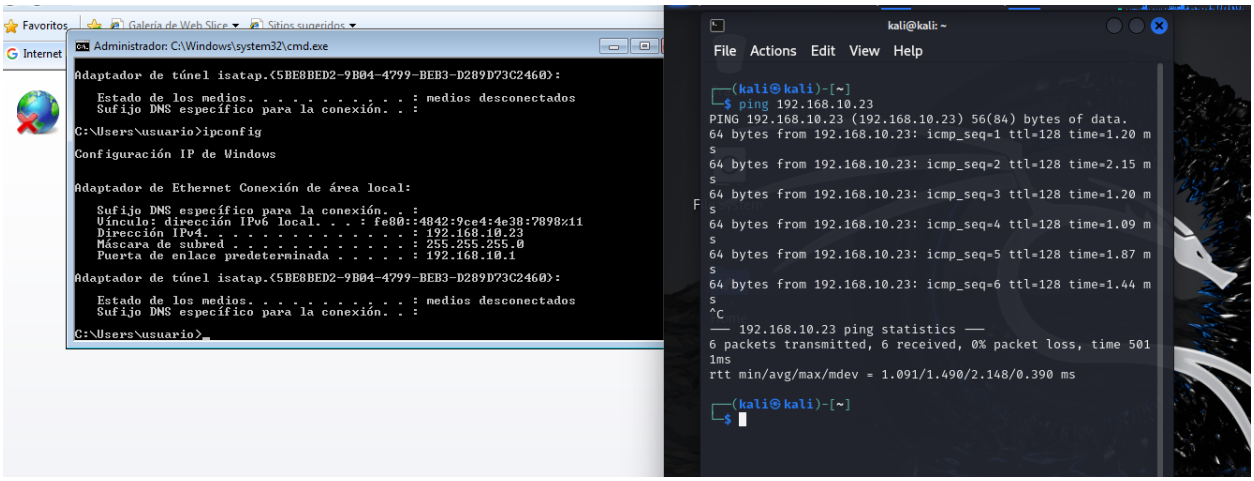
Fuente Propia

Ilustración 7 Config Kali Linux



Fuente Propia

Ilustración 8 Prueba de conectividad



Fuente Propia

Procesos Eticos y Legales en Escenarios No Eticos.

En escenarios en los cuales se presentan procesos no éticos con respecto a temas relacionados con Red Team y Blue Team, se recomienda el seguimiento del marco legal Colombiano y el Codigo de ética del COPNIA.

Como primera medida se encuentra el revisar los contratos por medio de los cuales se realiza el proceso de reclutamiento del personal para los Red Teams y Blue Teams. La premura de contratación y puesta en marcha de proyectos, dan mucho de que hablar sobre la ética y procesos legales en los acuerdos de confidencialidad firmados.

Para el acuerdo de confidencialidad se puede evidenciar varios procesos que acarrean problemas legales y éticos para los firmantes de estos:

- El no permite el reporte ante las autoridades competentes, sobre procesos ilícitos que se logren identificar por objeto del contrato.
- Identificar la falta al código de ética en el ocultamiento o sustracción de información.
- Tener presente que que no se viole el código de ética de COPNIA al no permitir la denuncia ante hechos delictivos.
- Comprender la responsabilidad sobre el uso indebido de información por parte de los representantes.
- La solución de controversias, se debe llevar acabo de manera responsable entre las partes y no recargando la responsabilidad sobre una de las partes.

Violación ley 1273

Tener claridad sobre la ley 1273 de 2009 en los siguientes artículos:

Articulo 269A: Acceso abusivo a un sistema informático.

Articulo 269F: Violación de los datos personales.

Articulo 269H la conducta se agrava si se presentan situaciones como las descritas:

- Aprovechar la confianza depositada por el poseedor.
- Obtener provecho para si o para terceros.

En los procesos de contratación de equipos Red Team y Blue Team, surgen las siguientes interrogantes:

Interrogante 1

Ilustración 9 Interrogante 1

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Fuente Guia de actividades y rubrica de evaluación – Etapa 2 Actuacion ética y legal

Respuesta: En los procesos de auditoria de seguridad, es inevitable que se acceda a información de vital importancia para los clientes, esto debido al grado de penetración que se realice por parte de los equipos red teams y blue teams. No en todos los casos se logrará acceder a información sensible, pero si a procedimientos que permite acceder a esta, es por ello que los procesos de intrusión se deben proteger con contratos claros y concretos sobre la extracción y uso de esta, generando acuerdos de confidencialidad y acuerdos de confianza.

El personal que realizara las auditorias de seguridad, deben ser idóneos y con ética profesional clara y aplicada, adicional se debe proteger los contratos con acuerdos ligados a la ley y al código de ética profesional del COPNIA.

Interrogante 2

Ilustración 10 Interrogante 2

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Fuente Guia de actividades y rubrica de evaluación – Etapa 2 Actuacion ética y legal

Respuesta: Para ello de sebe realizar un análisis concienzudo de los contratos del personal opcionado, la contratación se debe realizar bajo los mas altos estándares de validación y escogencia, esto se debe complementar con contratos claros y ligados a la ley 1273 y basados en los códigos de ética de COPNIA, que permitan el actuar legal frente a lo posible violación de las políticas y contratos.

La aplicación de acuerdos de confidencialidad y claridad frente a las implicaciones legales derivadas de malas prácticas o ética cuestionable, debe ser suficiente para evitar que las empresas de ciberseguridad caigan en las malas practicas o en implicaciones legales con sus clientes.

Interrogante 3

Ilustración 11 Interrogante 3

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente

Fuente Guia de actividades y rubrica de evaluación – Etapa 2 Actuacion ética y legal

Respuesta: Los gobiernos y organizaciones deben prestar especial cuidado a las empresas de ciberseguridad que se vean inmiscuidas en malas practicas o actos de ciber espionaje y más si estos se presentan de manera constante. Aunque a diario en el país, los ataques cibernéticos se presentan con mayor frecuencia y grado de impacto, esto no debe influenciar en la normativa aplicable para las empresas que se dedican a las auditorias de seguridad, es ahí en donde se deben aplicar medidas que permitan la restauración de la confianza con los clientes, y esto es la aplicación eficaz de la ley 1273 y el código de ética de COPNIA, si no hay mano dura y firme legalmente, la confianza se pierde y los procesos se dañan.

Aunque no se puede garantizar que los incidentes ocurran nuevamente, si dan luz a las autoridades para poder actuar concreta y eficazmente frente a los infractores.

Ejercicio Practico Controlado Red Team.

Con la claridad sobre los marcos legales y éticos frente a la realización de pentesting con red Team y Blue Team, se muestra un ejercicio practico de Red Team en ambiente controlado y configurado anteriormente.

Para la realización del informe, se tendrá en cuenta la metodología PTES que expone 7 pasos para realizar pruebas de penetración, adicional se utiliza la herramienta Kali Linux, nmap y metasploit para identificar y explotar vulnerabilidades en el sistema Windows 7.

1. Interacción previa: El objetivo principal es la identificación de vulnerabilidades que permitieron la explotación y posterior ataque sobre el sistema Windows. Se acuerda la utilización de la metodología PTES como guía y modelo de pentesting.
2. Recolección de información: Se suministra por parte del equipo forense, la copia del servidor, para posterior análisis.
3. Modelado de amenazas: Se identifica maquina con sistema operativo Windows 7 con aplicativo hsf instalado. Maquina vulnerada.
4. Análisis de vulnerabilidades: Se realiza identificación de puertos abiertos en la maquina Windows 7, por medio de la maquina Kali Linux y Nmap utilizando los comandos:

Sudo nmap -sV 192.168.10.23 Permite identificar la versión de los puertos listados abiertos, se identifica el puerto 80 del servicio http versión 2.3

Se identifica la vulnerabilidad cve-2014-6287 desde la página de CVE.

5. Explotación: Con el código CVE se realiza explotación por medio de la herramienta MetaSploit desde Kali Linux.

Se utiliza el comando search cve-2014-6287 arrojando el exploit/Windows/http/rejetto_hfs_exec que es explotado con metasploit.

Se apertura una sesión y se crea usuario con privilegios de administrador con incognito con el comando add_user “waltervirviescas” “Colombia123” y se agrega al grupo Administradores por medio del comando add_localgroup_user “Administradores” “waltervirviescas”

Se logra ingresar con privilegios de administrador y la creación de usuario con permisos de administrador, teniendo así el control total del equipo Windows.

6. Post explotación: Se identifica maquina Windows 7 con puerto 80 abierto y servicio httpd versión 2.3 desactualizada que permite la explotación de la vulnerabilidad cve-2014-6287. Esta vulnerabilidad permite el ejecutar programas de manera arbitraria y por medio de esta vulnerabilidad se explota el equipo y se logra la creación de usuario con privilegios de administrador.
7. Presentación de reportes: Se presenta informe del proceso de ataque realizado y se identifica que la vulnerabilidad se presenta por la falta de actualización del servicio httpd.

Herramientas Utilizadas

Para la identificación del fallo que presenta la maquina Windows 7, se utilizaron las siguientes herramientas:

- Kali Linux
- Nmap
- Metasploit

- CVE
- exploit/Windows/http/rejetto_hfs_exec

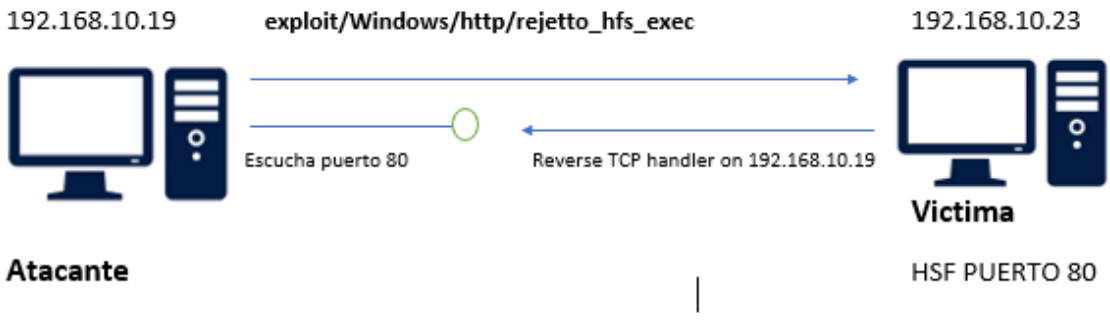
Con estas herramientas se logra identificar que la aplicación HFS de la maquina Windows, utiliza el puerto 80 servicio http y maneja una versión 2.3 que esta desactualizada y permite la explotación de la vulnerabilidad encontrada.

Analisis del Ataque Realizado

Este ataque realizado sobre la maquina Windows, la afecta de manera significativa, ya que da control total a esta, y de manera sigilosa.

La apertura el puerto 80 al momento de utilizar la aplicación HSF, permite la ejecución de manera remota y arbitraria de aplicaciones que permiten el acceso a usuario con privilegios y tener control total sobre el sistema operativo. De esta manera se puede crear cuentas adicionales, extracción de información o instalación de puertas traseras que permitan el acceso continuo y silencioso al equipo y al sistema.

Ilustración 12 Grafico ataque



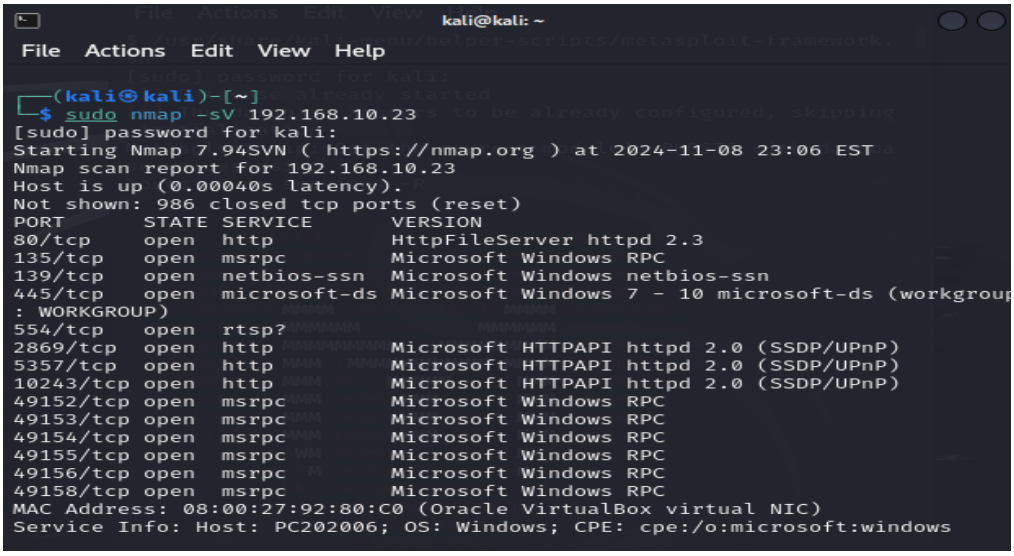
Fuente Propia

Informe de Explotacion

Se realiza identificación de puertos abiertos en la maquina Windows 7, por medio de Kali Linux y Nmap utilizando los comandos:

Sudo nmap -sV 192.168.10.23 Permite identificar la versión de los puertos listados abiertos.

Ilustración 13 Puertos Abiertos

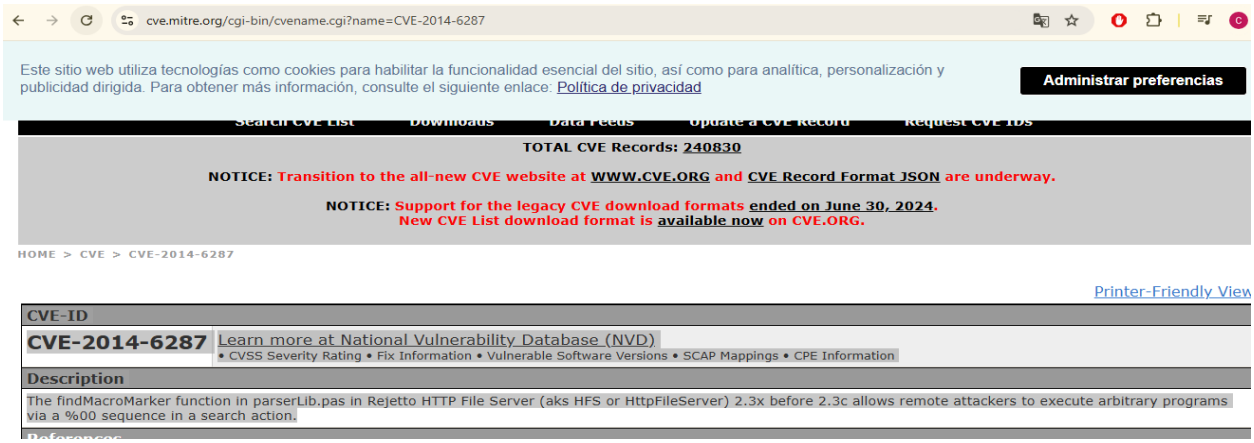


Fuente Propia

Se identifica un HttpFileServer httpd 2.3.

Se identifica los CVE para el httpd 2.3. CVE-2014-6287

Ilustración 14 CVE

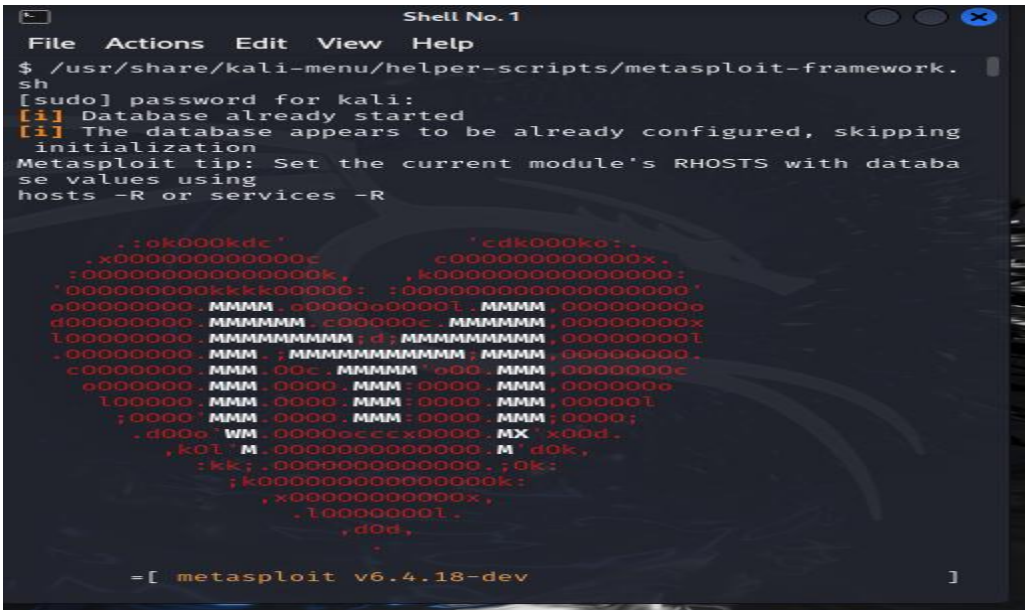


Fuente Propia

Con este CVE se puede ejecutar programas arbitrarios de manera remota.

Con el código CVE se realiza explotación por medio de la herramienta MetaSploit desde Kali Linux.

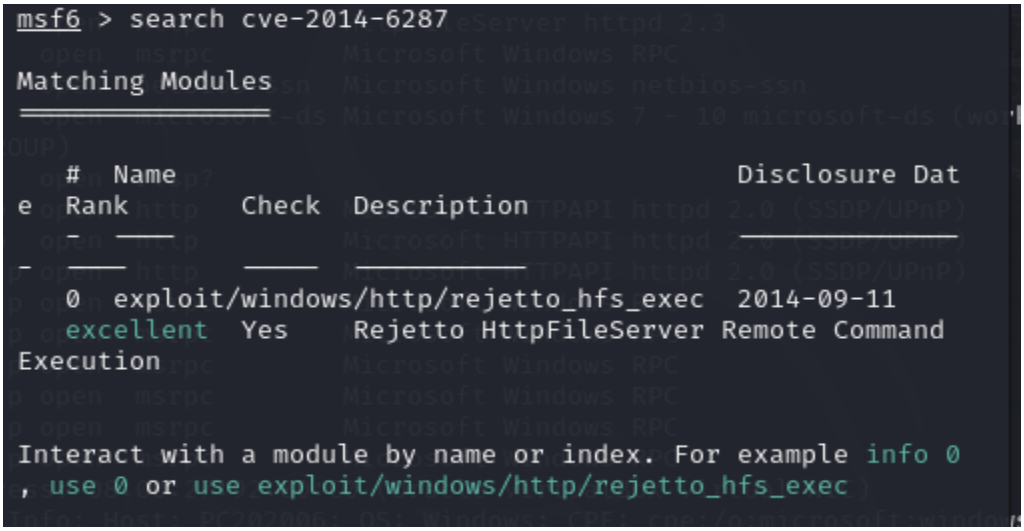
Ilustración 15 Metasploit



Fuente propia

Con el comando search cve-2014-6287 se puede identificar el exploit a utilizar para explotar la vulnerabilidad encontrada en la versión del httpd.

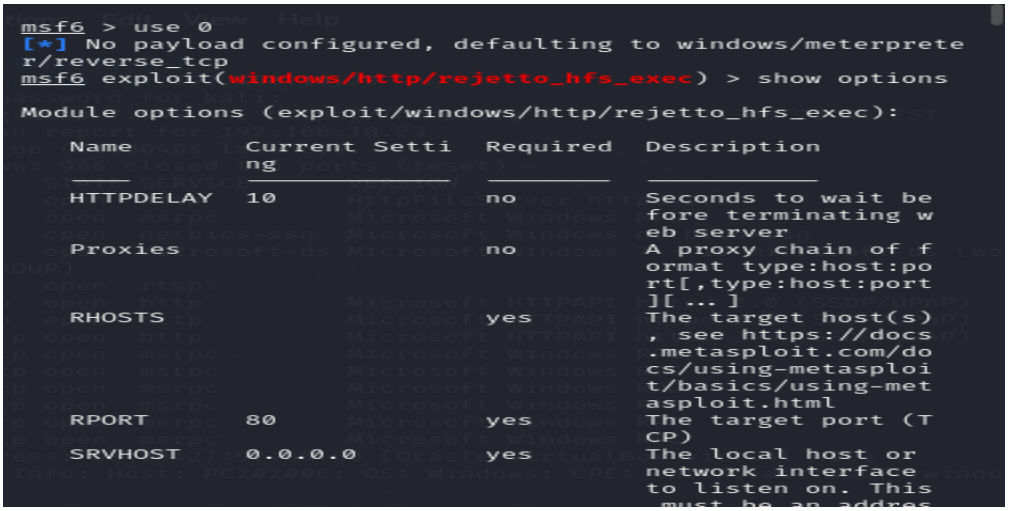
Ilustración 16 Escaneo CVE



Fuente Propia

Se utiliza el exploit 0 exploit/Windows/http/rejetto_hfs_exec y se identifica el RHOSTS a configurar con el comando show options

Ilustración 17 Exploit



Fuente Propia

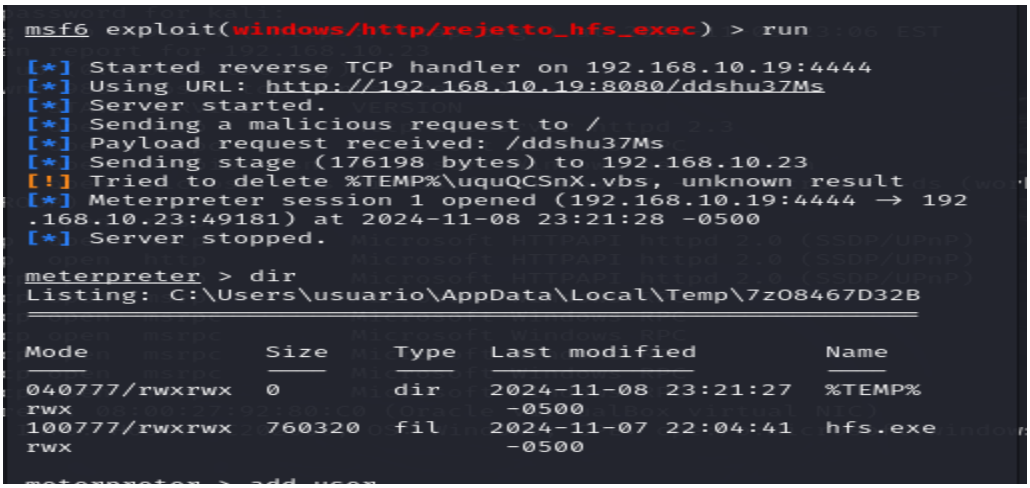
Se configura el RHOSTS con el comando set rhosts 192.168.10.23 y se confirma con el comando show options.

Ilustración 18 Configuracion RHOST

Fuente Propia

Se ejecuta el exploit por medio del comando run y se identifica una sesión abierta con meterpreter y con el comando dir, se puede confirmar que se encuentra en el directorio de la maquina Windows.

Ilustración 19 Explotacion

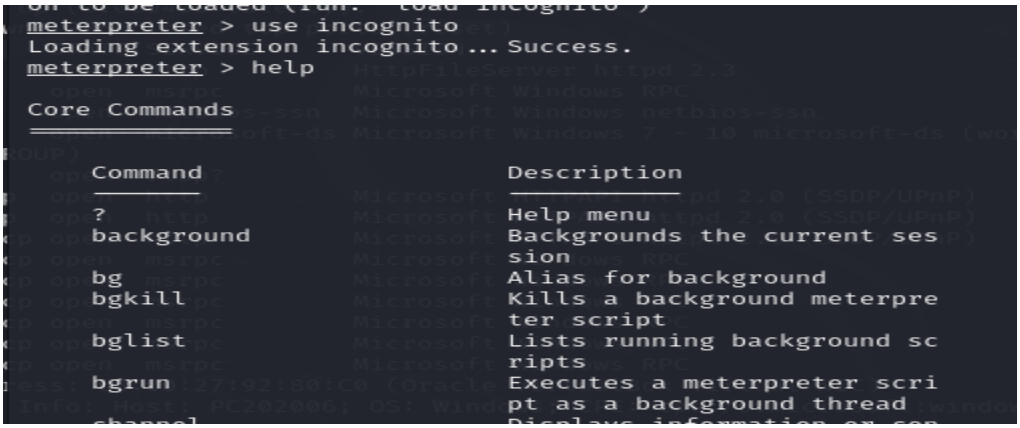


Fuente Propia

Una vez dentro de la maquina impactada, se realiza la creación de un usuario administrador que se denominará “waltervirviescas” y que estará en el grupo de “Administradores”

Se ejecuta el comando use incognito para ingresar de manera sigilosa y help para identificar los comandos a utilizar.

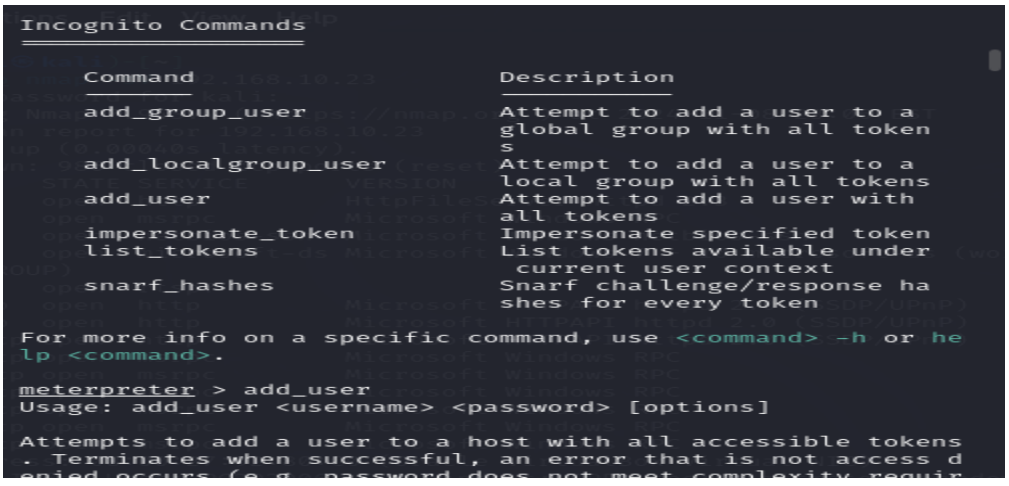
Ilustración 20 Incognito



Fuente Propia

Se utiliza el comando ***add_user*** de los comandos de ***incognito commands***. Esto para la creación del usuario en la maquina impactada.

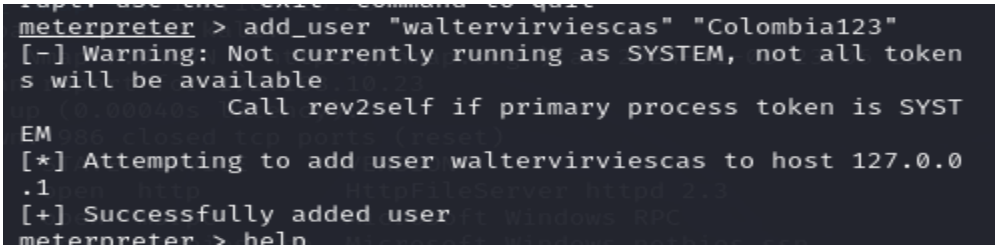
Ilustración 21 Incognito User



Fuente Propia

Se crea el usuario y la contraseña con el comando add_user “waltervirviescas” “Colombia123”.

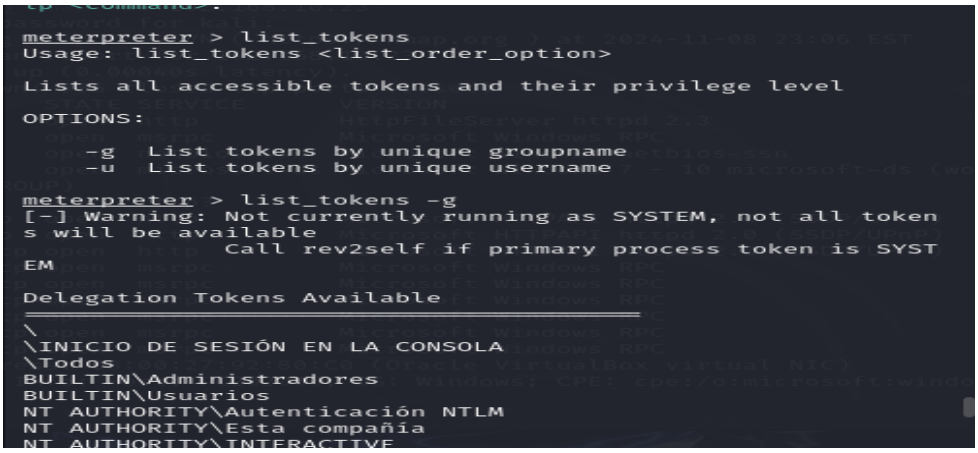
Ilustración 22 Crear Usuario



Fuente Propia

Se ejecuta el comando list_tokens -g para lograr identificar como se llama el grupo administradores BUILTIN\Administradores.

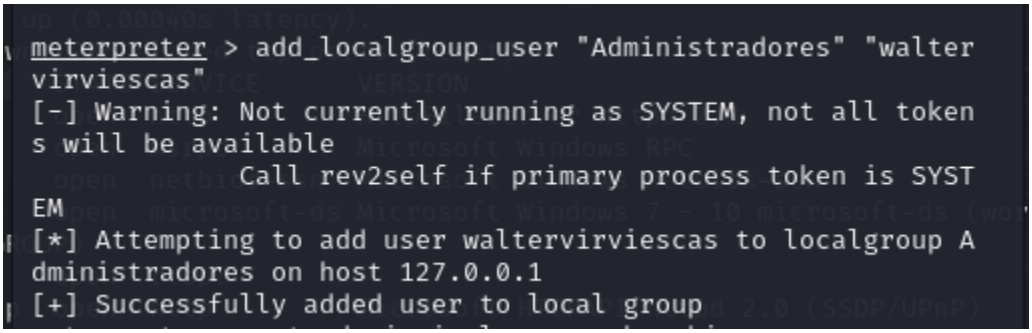
Ilustración 23 Privilegios



Fuente Propia

Se ejecuta el comando add_localgroup_user “Administradores” “waltervirviescas” para agregar el usuario creado al grupo de administradores.

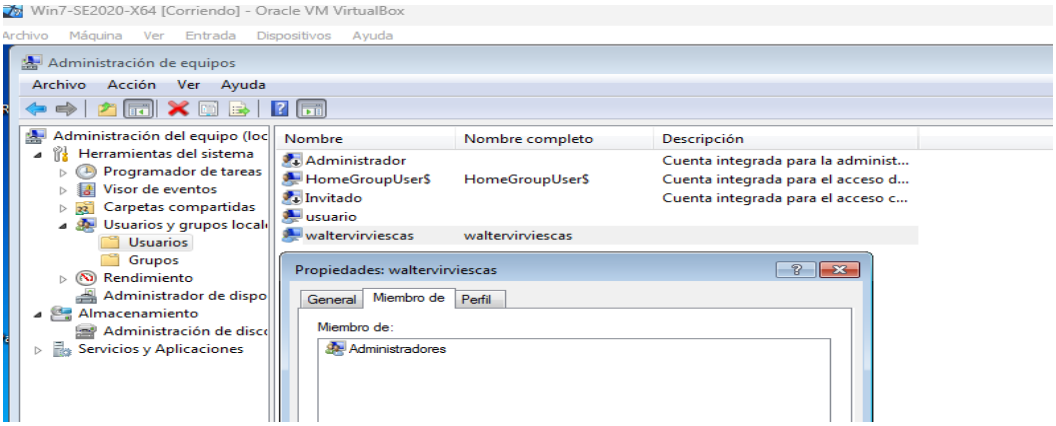
Ilustración 24 Administrador



Fuente Propia

Se confirma en la maquina impactada, la creación del usuario y su vinculación al grupo de administradores.

Ilustración 25 Usuario Creado



Fuente Propia

Ejercicio equipos Blue Team

Dentro de las labores de los equipos Blue Team es importante comenzar a contrarrestar el ataque identificado, es por ello que se deben seguir los siguientes pasos:

Teniendo en cuenta que se presenta un ataque sobre una maquina con sistema operativo windows 7, comienza a realizar aseguramiento de la zona y del equipo que reporta vulnerabilidad explotada.

A continuacion de detallan los pasos a seguir para lograr realizar el aseguramiento del equipo.

1. **Desconectar el equipo de la red y aseguramiento**: Al identificar que una de las máquinas de la compañía está siendo atacada por medio de una de sus vulnerabilidades y con el fin de evitar que se propague este ataque, se procede con la desconexión del equipo de la red, ya sea de internet o de la LAN. La propagación de diferentes malware, ransomware, phishing y más, por medio de la red, es algo que debe preocupar en gran manera, de ahí a la importancia de la desconexión inmediata del equipo vulnerado y lograr su aseguramiento, evitando así, que se siga propagando el ataque, ya sea con intención o por desconocimiento del aseguramiento del equipo.
2. **Evaluar el incidente presentado:** Una vez realizada la desconexión del equipo de la red y teniendo un aseguramiento efectivo de esta, se procede con la evaluación del incidente, buscando identificar la gravedad del ataque, que otros sistemas infectos y que grado de impacto tuvo sobre el sistema. Es importante contar con herramientas que permitan la identificación de esto, estas pueden ser las herramientas de monitoreo o SOC con los que cuenta la compañía, el registro que toma el antivirus y la revisión

de logs del propio equipo impactado junto con el visor de eventos de Windows o la actividad sobre la red.

3. **Registro de evidencias y copias de seguridad:** Es importante contar con evidencias concretas sobre el incidente presentado, es por ello por lo que se debe documentar todos los registros y pasos realizados en la identificación del ataque, junto con el registro se debe realizar copia de seguridad de la máquina y continuar con el análisis forense con más seguridad. Se debe evitar el manipular directamente el equipo infectado, todas estas revisiones y pruebas se deben realizar sobre la copia realizada, evitando alterar la escena del ataque.
4. **Ejecutar medidas de contención:** Dentro de los primeros pasos a seguir una vez identificado un ataque al sistema, se debe revisar las políticas de seguridad y como estas están siendo ejecutadas sobre el equipo impactado, se identificarse falencias, se deben aplicar de manera inmediata. Dentro de las medidas a revisar se encuentran:

- **Revisión de antivirus:** junto con la revisión se debe dar la actualización y aplicación de este, para lograr identificar y eliminar cualquier tipo de malware que pudo haber sido impactado.
- **Actualización del sistema:** Un alto grado de ataques se encuentran en las vulnerabilidades que están presentes en sistemas desactualizados, es por ello por lo que se debe aplicar y ejecutar las actualizaciones necesarias para contener y mitigar el impacto que tiene el ataque sobre la máquina, estas actualizaciones se deben aplicar sobre el sistema operativo y demás aplicaciones que use.

Es importante saber que Windows 7 ya no tiene soporte, por tal razón se recomienda la actualización a Windows 10 u 11.

- Revisión de políticas de seguridad de la compañía: Identificar si dentro de las políticas se identifica alguna vulnerabilidad que pueda dar cabida a un ataque informático.
- Bloqueo de cuentas: al identificar cuentas que estén comprometidas en el ataque, se debe hacer un bloqueo inmediato, esto con el fin de proteger el sistema y evitar la propagación del ataque.

Medidas de Hardenizacion

Con el ejercicio realizado en el momento anterior, se logra identificar falencias en los sistemas de protección con los que cuenta el equipo Windows 7 impactado y vulnerado, de ahí a la importancia de realizar y aplicar medidas de hardenizacion que logren mitigar el grado de impacto y vulnerabilidades existentes. Aunque no se puede garantizar que un ataque de ese tipo se repita, si se pueden aplicar medidas que mitiguen el riesgo, dentro de ellas están las siguientes:

Para el sistema local.

- **Aplicación de actualizaciones:** una de las medidas más eficientes es la de mantener los sistemas siempre actualizados, esto mitiga las vulnerabilidades posibles cobre los sistemas operativos y así mismo lograr gestionar las actualizaciones de las aplicaciones utilizadas. Para ello se recomienda la activación de actualizaciones automáticas de Windows, o el agente de Windows update, con ello se logra mantener al día, las actualizaciones del sistema operativo y aplicaciones. De igual manera se puede activar las actualizaciones automáticas en Microsoft store.

Es importante mencionar que Windows 7, ya no posee soporte por parte de Microsoft y es por ello que se recomienda en alto grado, el realizar la migración a sistemas operativos Windows 10 o Windows 11.

- **Configuración del Firewall de Windows:** Endurecer las reglas aplicadas en el firewall, con ello se logra controlar gran parte del tráfico entrante y saliente, dando acceso a la red únicamente a las aplicaciones que así lo requieren. Es importante que el firewall este activo para redes públicas y privadas y configurar reglas personalizadas sobre aplicaciones específicas para evitar que aquellas que no requieren acceso a la red, sean blanco de ataques. Las reglas del firewall se deben revisar de manera regular y actualizar de acuerdo con las necesidades propias del servicio o sistema.

- **Configuración de antivirus:** Es importante contar con un sistema de protección antivirus confiable y actualizada que permite el escaneo y que este habilitado la protección en tiempo real. Dentro de la protección antivirus, se recomienda la activación de Windows defender, que protege contra malware, protección en tiempo real y algunas funciones de seguridad esenciales tales como análisis programados, actualizaciones de manera automática, control de aplicaciones y navegación, protección contra ransomware, reporte de amenazas y a su vez no consume muchos recursos del equipo, siendo muy eficiente. Aunque es una buena herramienta de protección, se recomienda que se complemente con otros antivirus GPL tales como

Avast Free, AVG antivirus, Panda, Bitdefender entre otros, que dan una protección extra y de manera gratuita.

- **Aplicación de cifrado de datos BitLocker:** Aunque esta es una herramienta de cifrado para el disco duro y discos extraíbles, esta es importante para la protección de los datos que se encuentran almacenados allí e impide que personas no autorizadas ingresen de manera indebida a ella.

Bitlocket se integra con TPM o módulo de plataforma segura y da un grado mayor de protección al ir dirigida directamente al hardware y ayuda con la protección contra software malicioso, ya que verifica la integridad del sistema antes de realizar el cargue del sistema operativo utilizado facilitando el Secure boot para evitar el arranque con software malicioso.

- **Ajustar el control de cuentas de usuario o UAC:** Contar con alertas o notificaciones cuando se realicen cambios en el sistema, que requieren que se eleven los privilegios a administrador del sistema, permite identificar en tiempo real un posible ataque de elevación de privilegios, es por ello que, en control de cuentas de usuarios, se deben ajustar a los niveles máximos

- **Aplicación de política de contraseñas:** El contar con un buen control y política de manejo de contraseñas, aumenta la seguridad en cuanto a los accesos y frente a vulnerabilidades que se relacionen con ataques de fuerza bruta o de contraseñas, es

por ello que se recomienda que las políticas de contraseñas estén bien configuradas y tenga mínimos estándares.

La configuración local se puede realizar desde la política de seguridad local, aunque se recomienda que se pueda realizar por medio de un directorio activo.

Algunas políticas locales y de directorio activo serian:

- Longitud de la contraseña con un mínimo de caracteres, estos pueden estar alrededor de los 12, que contengan, números, letras y símbolos.
- Caducidad de por lo menos 30 días.
- Evitar el uso de contraseñas repetidas.
- Activar el bloqueo de cuentas si se excede el número de intentos de inicio de sesión incorrectos.

Diferencia Entre Blue Team y Equipo de Respuesta a Incidentes

Dentro de la ciberseguridad los equipos blueteam y de respuesta a incidentes juegan un papel crucial en la protección de los sistemas de información, y aunque en un sentido amplio se podrían catalogar como similares, en el fondo son dos equipos que tienen labores distintas y con un propósito un tanto diferente pero que se complementan entre sí.

Estas son algunas de las diferencias:

Tabla 1 Blueteam Vs CSIRT

	Blueteam	**CSIRT**
Enfoque	Defensa proactiva que busca prevenir los posibles ataques informáticos al sistema.	Defensa reactiva frente a los ataques informáticos que se están ejecutando.

Actividades	Previene, detecta y analiza las posibles vulnerabilidades del sistema, mediante la vigilancia continua.	Contención, erradicación e investigación forense, frente a los ataques informáticos detectados y en tiempo real.
Objetivo	Busca fortalecer las defensas del sistema mediante la aplicación de políticas efectivas y el uso correcto de herramientas tales como los IDS e IPS entre otros.	Busca minimizar el grado de impacto de los incidentes presentados, evitando en menor daño posible sobre el sistema.

Mientras los equipos de blueteam se enfocan en la defensa proactiva, siempre realizando un análisis constante al sistema, buscando mejorar las políticas y herramientas de protección frente a ataques de ciberseguridad, los equipos de respuesta a incidentes, son mas reactivos frente a ataques en curso y busca minimizar el grado de impacto del ataque, protegiendo al sistema de manera inmediata y directa.

Recomendaciones para el Ejercicio de Blue Team

Para fortalecer los ejercicios de Blue Team, se recomienda el uso de modelos y buenas practicas de controles de seguridad que cumplan con los estandares mas altos en ciberseguridad.

Uso de CIS

El CIS o centro de seguridad de internet, son buenas practicas y controles de seguridad que se pueden aplicar a todo tipo de compañías ya sean privadas o publicas y que busca apoyar a los expertos en ciberseguridad a aplicar las mejores practicas frente a las políticas de seguridad que mitiguen el riesgo de ataques e incidentes en los sistemas.

El CIS contiene varios controles de mejores practicas de ciberseguridad que ayudan a mitigar las posibles amenazas en los sistemas. Estos controles fueron diseñados especialmente para ayudar a los expertos en ciberseguridad a fortalecer la defensa de las organizaciones al tener como punto de referencia las experiencias de otras organizaciones.

Dentro del equipo de Blueteam se utilizaría CIS para:

- **Control sobre inventario:** esto para lograr obtener la identificación de todos los activos informáticos junto con sus características, evitando perder del radar, algunos activos que puedan llegar a presentar vulnerabilidades explotables.

Las buenas prácticas probadas del CIS dan línea directa sobre cómo manejar correctamente los activos de la organización.

- **Control de gestión de cuentas:** Las buenas prácticas en la gestión de cuentas permite que se minimicen las vulnerabilidades por ataques de elevación de privilegios.

Cuando se maneja las cuentas de manera estándar como en el ejemplo y estas no se gestionan correctamente, son blanco fácil para los ciberdelincuentes, que logran acceder al equipo con elevación de privilegios de manera más ágil y fácil. El buen control y gestión de

cuentas, ayuda para poder cerrar el acceso de manera más efectiva y en tiempo real, al tener control total sobre los usuarios activos en el equipo y en el sistema.

- **Control de configuración segura para hardware y software:** Esto para poder configurar correctamente y bajos los estándares de CIS, los sistemas de información, minimizando así las vulnerabilidades referentes a configuraciones erróneas al estar monitoreada y generando alertas.
- **Limitación y control de puertos de red:** Permite supervisar y controlar la actividad sobre los puertos de red, al gestionar y configurar las aplicaciones y su acceso a la red. Evitando así que aplicaciones sin la necesidad de acceso a red permitan vulnerabilidades. En ocasiones se permite en el firewall, la configuración por defecto, que ocasiona apertura de puertos de red que dan entrada a atacantes, con el control de puertos, se busca cerrar esa puerta.
- **Cumplimiento con regulaciones:** El CIS y el cumplimiento de sus controles, facilitan el cumplimiento de las diferentes regulaciones en seguridad y así las compañías pueden enfocar sus esfuerzo y recursos de manera más eficiente.

Todos estos controles implementados del CIS buscan el fortalecimiento de las configuraciones iniciales en los sistemas de seguridad de las compañías y se enfoca en fortalecer los puntos más críticos y relevantes, sin dejar de lado los pequeños detalles. Todo esto hace que la implementación de CIS, sea un punto a favor en el fortalecimiento de la seguridad de las compañías por medio de la utilización de equipo blueteam.

SIEM

Un SIEM por sus siglas en ingles Security Information and event management o Gestión de información y eventos de seguridad, es un sistema de seguridad o solución de software que es capaz de centralizar la información o datos que provienen de diferentes soluciones de seguridad y registros de los sistemas informáticos, para ayudar a detectar cualquier tipo de amenaza en tiempo real, al analizar patrones sospechosos en el tráfico y acceso a la red.

Los sistemas SIEM son la evolución de la gestión de eventos de seguridad SEM, que detecta los patrones de acceso a los sistemas que no son comunes y los detecta en tiempo real y la gestión de información de seguridad SIM, que centraliza todos los registros que se originan del monitoreo de seguridad y que busca dar respuesta inmediata y en tiempo real a los eventos de seguridad.

Funciones: como funciones principales se encuentra el

- Recopilación de información: Recopila todos los registros que llegan de las diferentes herramientas de seguridad, estos pueden ser, Logs, dispositivos de red, aplicaciones y más.
- Unifica la información: La información recopilada proviene de diferentes fuentes y SIEM unifica la información para una mejor y fácil interpretación y análisis.
- Identificación de patrones: Al analizar la información recopilada, por medio de algoritmos avanzados, busca patrones incorrectos en el funcionamiento y uso de los sistemas que sean sospechosos.
- Detección de amenazas: Los análisis realizados y la identificación de patrones incorrectos o anormales dentro del sistema, permite la identificación en tiempo real

de amenazas y la generación de alertas ante posibles ataques. No solo permite la detectar las amenazas, sino que las cataloga según su grado de impacto.

- Generación de informes: Genera informes detallados de las amenazas detectadas, posibles soluciones y acciones tomadas en tiempo real.

SIEM cuenta con diferentes características importantes para la protección de los sistemas, estas serian las mas relevantes:

- Permite el manejo de grandes volúmenes de información y de diferentes fuentes
- Unifica dicha información para mejor manejo y análisis
- Es automatizado generando eficiencia en los análisis.
- Flexible, ya que se integra con diferentes herramientas.
- Detecta amenazas al identificar diferentes patrones incorrectos en los sistemas.
- Permite dar respuesta mas oportuna a los incidentes generados por su monitoreo en tiempo real.
- Ayuda con el cumplimiento de normas y legislaciones vigentes relacionadas con la política de seguridad de la información.

Existen varias herramientas que se basan en SIEM aquí algunas de ellas.

- IBM Security QRadar, de los sistemas SIEM más completos del mercado.
- McAfee Enterprise Security Manager, de la prestigiosa y confiable compañía de seguridad.
- LogRhythm, está orientada a pequeñas empresas.

Herramientas de Contencion de Ataques

Las herramientas de contención de ataques ayudan a eliminar el impacto sobre los sistemas una vez ha ocurrido, estas herramientas pueden ser de hardware o software. Aquí algunas de ellas.

- **Firewalls:** los firewalls son herramientas de hardware que permiten resguardar la red al permitir o bloquear el tráfico que se pueda generar, todo esto por medio de las reglas definidas en él. Al tener control del tráfico de red, permite contener ataques al bloquear el tráfico malicioso, impidiendo su propagación.

Una de las herramientas más utilizadas son los Fortinet Fortigate, que previene y bloquea el tráfico incluso antes de que el atacante ingrese a la red.

Otra de las herramientas más utilizadas y GPL es Pfsense, que permite el filtrado de Ip/puertos, y equilibrio de carga Nat y VPN.

- **Suricata:** aunque se utiliza para detección de intrusos, esta herramienta GPL permite en su configuración, ser una herramienta de contención de ataques informáticos al analizar el tráfico de red y bloquearlo según se identifique una amenaza en tiempo real.
- **Antivirus:** los antivirus, aunque se utilizan en su mayor grado en la detección de eliminación de software malicioso, también es capaz de contener ataques al poner en cuarentena a los archivos infectados y de esta manera evitar su propagación. Algunos antivirus o antimalware pueden ser ClamWin Free Antivirus, ClamAV

- **Sandboxing:** esta caja de arena que está diseñada para el malware, permite ejecutar aplicaciones potencialmente peligrosas dentro de entornos controlados, evitando la propagación del malware en la red.

Algunos de los sandboxing más utilizados se encuentran, cuckoo sandbox, QEMU e inclusive Virtualbox.

Conclusiones

Con los conocimientos de las herramientas y procedimientos establecidos para la realización de pruebas de penetración o pentesting, se puede abordar los sistemas de información de manera más ágil y segura, siempre bajo el marco y legislación colombiana referente a la política de delitos informáticos.

El conocimiento de la ley 1273 de 2009 proporciona bases y sustento legal a las compañías que realizan pruebas de penetración, tales como los red teams y los blue teams, brindando claridad y tranquilidad a las compañías contratantes respecto a la idoneidad del personal contratado para efectuar las auditorías de seguridad. Estas buenas prácticas deben complementarse con la aplicación del código de ética de COPNIA, que establece una línea ética para los profesionales que realizan las auditorías y permite la claridad frente a las medidas aplicables legalmente ante acciones indebidas.

Es de vital importancia para las compañías contar con pruebas de penetración controladas por equipos Red Team, que proporcionen claridad sobre los ataques recibidos y permitan ajustar o corregir los fallos encontrados. Con las pruebas realizadas, es posible comprender la metodología utilizada por los ciberdelincuentes y realizar un aseguramiento más robusto de los sistemas, mediante acciones simples como actualizaciones de las herramientas utilizadas en los sistemas.

El fortalecimiento de las políticas y metodologias aplicadas a los controles de seguridad en la ejecución de acciones provenientes de equipos Blue Team, permiten fortalecer y robustecer los sistemas de información dando mas tranquilidad a los usuarios y valor agregado a las compañias que los aplican.

Recomendaciones

Para la aplicación y ejecución de equipos Red Team y Blue Team, se recomienda tener presente los siguientes aspectos:

- Tener claridad y conocimiento sobre la normativa legal vigente sobre delitos informáticos, esto permitirá contar con acuerdos y contratos ligados a la legalidad.
- Tener objetivos claros y determinar el alcance de las pruebas a realizar.
- Contar con una planificación detallada de los ejercicios a realizar dentro de los sistemas para evitar violación de la normativa legal y codigos de ética de COPNIA.
- Realizar pruebas en ambientes controlados que sean lo mas realistas posibles, esto dará mayor claridad sobre el alcance y afectación posible en los sistemas.
- Aplicar correctamente los controles establecidos según el modelo a seguir para la planificación y puesta en marcha de la seguridad del sistema.
- Realizar monitoreo continuo sobre los sistemas, esto dará mayor información sobre el método utilizado por los ciberdelincuentes.
- Tener comunicación abierta entre los dos equipos, ayudara a generar informes mas detallados que fortalezcan la seguridad del sistema.

Referencias Bibliográficas

Copnia, Codigo de ética, [Online]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Funcion publica, Ley 1273 de 2009, [Online]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Policía Nacional, Normatividad sobre delitos informáticos [Online], Disponible en https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos#:~:text=Art%C3%ADculo%20269A%3A%20Acceso%20abusivo%20a,el%20leg%C3%ADtimo%20derecho%20a%20excluirlo

Ciberseguridad club. Que es OpenVas. [Oline]. [Publicado el 8, febrero, 2024]. Disponible en: https://ciberseguridad.club/que-es-openvas/

HolmSecurity base de conocimiento. ¿Qué es la base de datos Exploit-BD? [Online]. [consultado el 13, octubre, 2024]. Disponible en: https://support.holmsecurity.com/knowledge/what-is-exploit-db-database

OpenWebinars. Que es OpenVas. [Oline]. [Publicado el 11, Noviembre, 2020]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

Policía Nacional, Normatividad sobre delitos informáticos [Online], Disponible en https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos#:~:text=Art%C3%ADculo%20269A%3A%20Acceso%20abusivo%20a,el%20leg%C3%ADtimo%20derecho%20a%20excluirlo.

Tarlogic. ¿Qué es CVE? [Online]. [2024]. Disponible en: https://www.tarlogic.com/es/glosario-ciberseguridad/cve/

CVE, CVE-2014-6287, [Online], Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

Openwebinars, Nmap, uso básico para rastreo de puertos, [Online], Disponible en: https://openwebinars.net/blog/nmap-uso-basico-para-rastreo-de-puertos/

Security ar work, escalada de privilegios con incognito, [Online], Disponible en: https://www.securityartwork.es/2014/01/14/escala-de-privilegios-con-incognito/

Ambit ¿Qué significa SIEM y cómo funciona?, [Online], Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

AWS, ¿En qué consisten los puntos de referencia del CIS?, [Online], Disponible en: https://aws.amazon.com/es/what-is/cis-benchmarks/

Cibernos grupo, Pasos a seguir ante un ataque informático, [Online], Disponible en: https://www.grupocibernos.com/blog/pasos-a-seguir-ante-un-ataque-informatico

Cyber zaintza, Equipo de respuesta ante incidentes, [Online], Disponible en: https://www.ciberseguridad.eus/ciberglosario/equipo-de-respuesta-ante-incidentes#:~:text=Un%20Equipo%20de%20Respuesta%20frente,o%20un%20grupo%20ad%20hoc.

Hackmetrix, que hacer en las primeras horas y días luego de un ciberataque, ? [Online], Disponible en: https://blog.hackmetrix.com/que-hacer-en-las-primeras-horas-y-dias-luego-de-un-ciberataque/

Microsoft learn challenge, Actualizar el agente de Windows update a la versión mas reciente, [Online], Disponible en: https://learn.microsoft.com/es-es/troubleshoot/windows-client/installing-updates-features-roles/update-windows-update-agent

Zona ia Samsung, ¿Cómo saber si hay intrusos en el ordenador? [Online], Disponible en: https://www.adslzone.net/reportajes/seguridad/detectar-intrusos-pc/

Anexos

https://youtu.be/X5Ryq58POdc