Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Arnovis Mendoza

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2024

Resumen

Se reconoce el margen legal sobre las distintas leyes y decretos que hacen parte del ordenamiento jurídico colombiano para regular la protección de datos ya sean personales o de organizaciones y los delitos sobre estos, también se revisan las fases del pentesting y la importancia de este, se exponen los conceptos de las principales herramientas de software especializado para la ciberseguridad y por último se instala el banco de trabajo utilizando la herramienta Virtual Box y los sistemas operativos de Kali Linux y Windows 7.

En esta actividad se enfoca en poder resolver la situación presentada en el anexo 4 escenario 3 que se debe buscar una máquina que tiene una aplicación vulnerable desde la cual está sucediendo fugas de información, se debe detectar el problema y realizar una prueba de concepto que básicamente sería una comprobación a los altos directivos, es importante tener en cuenta las afectaciones de un ataque a través del pentesting el cual como metodología ayuda a saber el nivel de vulnerabilidad en que se encuentra la organización.

Palabras clave: *blue team, red team, ciberseguridad, margen legal de la seguridad en Colombia.*

Abstract

The legal framework on the different laws and decrees that are part of the Colombian legal system to regulate the protection of data, whether personal or organizational, and crimes against these are recognized, the phases of pentesting and the importance of this are also reviewed, the concepts of the main specialized software tools for cybersecurity are exposed and finally the workbench is installed using the Virtual Box tool and the Kali Linux and Windows 7 operating systems.

This activity focuses on being able to solve the situation presented in annex 4 scenario 3, which should look for a machine that has a vulnerable application from which information leaks are happening, the problem should be detected and perform a proof of concept that basically would be a check to senior management, it is important to consider the effects of an attack through the pentesting which as a methodology helps to know the level of vulnerability in which the organization is.

Keywords: blue team, red team, cybersecurity, legal margin of security in Colombia.

Tabla de contenido

Glosario

Blue team: equipo responsable de proteger los activos de información de una organización para que no sea víctima de un ciberataque.

CMD: es una consola de línea de comando que viene en el sistema operativo Windows para ejecutar instrucciones a través de palabras claves que ejecutan acciones.

Comando: es una instrucción para realizar una acción, un comando se escribe o se indica a través de una consola que proporciona el sistema operativo.

CSIRT: equipo especializado que se activa cuando ha ocurrido un incidente de ciberseguridad.

Exploit: es un script que contiene instrucciones y comandos con una serie de pasos para poder ejecutar código en una maquina remota con el objetivo de poder aprovechar sus vulnerabilidades.

Framework: es un marco de trabajo que proporciona herramientas para desarrollar una actividad especifica.

Hardenización: significa fortalecer o endurecer algo, en este caso los controles aplicados para el mejoramiento de la ciberseguridad.

IP: es un protocolo que permite identificar los disipativos a través de un número, en este caso se usan direcciones IP de 32 bits, por ejemplo 192.168.216.1.

Red team: expertos que buscan simular ataques a una organización para examinar su defensa.

Lista de Tablas

Lista de Figuras

Introducción

El marco legal sobre la seguridad informática abarca el alcance y la guía para siempre actuar de manera responsable y dentro de la ley, es de vital importancia saber las brechas de seguridad de los sistemas a través de la metodología de pentesting que es la misma que puede utilizar un hacker, de esta manera se le comunican los resultados al equipo blue team desarrollado por el equipo red team.

Los equipos de red team deben de actuar en una organización ya sea de manera proactiva o reactiva, se evalúa un caso de fuga de información y donde se tienen información básica sobre una aplicación que puede ser utilizada para filtrar información de manera externa de la organización.

Por lo anterior se llevará a cabo un proceso de pentesting el cual servirá de guía para desarrollar la actividad y responder las preguntas de los directivos acerca de sus sospechas.

Los equipos de blue Team y CSIRT deben de actuar en una organización, el primero de una manera proactiva y el segundo de manera reactiva, se evalúa un caso de fuga de información y donde se tienen información básica sobre una aplicación que puede ser utilizada para filtrar información de manera externa de la organización, con base esto se da respuesta a la pregunta de la actividad.

Justificación

Cada día se vienen registrándose aumentos considerables de nuevas amenazas y ataques, entender cómo proteger esta tecnología es de vital importancia para las organizaciones, por lo tanto, se debe saber cómo realizar pruebas de pentesting en un laboratorio controlado utilizando la herramienta VirtualBox, NMAP y Windows 7 para posteriormente comunicar los resultados.

Los equipos de red team deben de ser capaces en poder dar respuestas a situaciones que se presentan en las organizaciones públicas y/o privadas de manera certera, de esta manera se debe llegar por medios de una investigación soportada mediante la metodología del pentesting para desarrollar la prueba de concepto que de tranquilidad a los directivos de la compañía sobre el origen de la fuga de información que se viene presentando.

Se debe tener una claridad sobre la función y diferencia de cada uno de los equipos de blue team y CSIRT para una organización, basados en el anexo 5 – escenario 4 se da respuesta a las necesidades de la organización CyberFort Technologies, quienes solicitan la contención y sacar adelante el ataque que están sufriendo en tiempo real.

Objetivos

Objetivo General

Analizar el impacto de la implementación de los equipos red y blue team en la ciberseguridad de las organizaciones para la protección de los datos e infraestructura tecnológica.

Objetivos Específicos

Identificar y aplicar las principales herramientas para la realización de los ejercicios de red y blue team tenieno en cuenta.

Aplicar la dinámica en un laboratorio virtual controlado del equipo de red team para el ejercicio de blue team y fortalecimiento de los controles.

Evaluar los beneficios de implementar estrategias que ayuden a aumentar la ciberseguridad en las organizaciones.

Sobre el marco legal colombiano para la ciberseguridad

El estado colombiano viene fortaleciendo su política para combatir los delitos informáticos que vienen en aumento, entre las leyes tenemos las siguientes:

Ley 1955 de 2019. “Por la cual se expide el Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, pacto por la equidad”. (“LEY 1955 DE 2019 - SUIN –JURISCOL”).

Ley 1978 de 2019. “Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones.” (“ley consulta.docx - LEY No. 1978 25 JUL 2019”).

Manual de Gobierno Digital – 2018. Donde es implementada la Política de Gobierno Digital con cuatro características importantes que son conocer, planear, ejecutar y medir la política donde cada uno de ellos incorpora las acciones que permitirán desarrollar la Política en las entidades públicas de nivel nacional y territorial.” (“PLAN ESTRATÉGICO DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES - PETI ...”).

Decreto 1008 – 2018. “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.

Documento CONPES 3920 – 2018. Política Nacional De Explotación De Datos (BIG DATA).

Decreto 1413-2017. “Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del

título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales".

Documento CONPES 3854-2016. POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.

Decreto 1083 -2015. "Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014 que establece los lineamientos generales de la Estrategia de Gobierno en Línea (Hoy Gobierno Digital)" ("Plan Estratégico De Seguridad De La Información")

Ley 1712 de 2014. "Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos (NTC-ISO/IEC Colombiana 27001:20013).

Ley 527 de 1999. "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones." ("Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso ...").

Ley 962 de 2005. "Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos." ("Ley 962 de 2005 - Gestor Normativo - Función Pública").

Decreto 1747 de 2000. Donde se reglamenta la Ley 527 de 1999, en lo relacionado con: "Las entidades de certificación, los certificados y las firmas digitales". ("Firma Electrónica - Inicio | Archivo General de la Nación").

Ley 1273 de 2009. También llamada ley de delitos informáticos, donde es denominado en el código penal “la protección de la información y de los datos” donde se protegen de manera completa los sistemas que den uso de la tecnología de la información y las comunicaciones.

Ley 1341 de 2009. Donde son definidas las principales leyes y orden de la sociedad de la información que también abarca un nuevo orden a las TIC. (“LEY 1341 DE 2009 - SUIN – JURISCOL”)

Plan para la implementación TI en Colombia.

Circular 17 de 2011. Donde se reglamenta y se le da orden a la verificación del uso legal de software en las organizaciones públicas de orden nacional.

Decreto 1377 de 2013. Reglamentar parcialmente la Ley, 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Directiva presidencial 002 de 2002. “Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software)” (“1. INFORME DERECHOS DE AUTOR”)

Decreto 886 de 2014. “El presente decreto tiene como objeto reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos” (“DECRETO 886 DE 2014 - SUIN – JURISCOL”)

Decreto 090 de 2018. Donde se deben reportar en el Registro Nacional de Bases de Datos, todas las bases de datos que tengan información personal automático o manual de cualquier organización sin ánimo de lucro con personería jurídica. (“Decreto 90 de 2018 - Gestor Normativo - Función Pública”).

Decreto 1078 de 2015. Donde se debe definir principios y conceptos para 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 (“LEY 1341 DE 2009 - SUIN – JURISCOL”)

Decreto 2194-2017. Modifica el artículo 2.2.2.4.1 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015.

Ley 1266 de 2008 (Ley de Habeas Data): Regula el uso de las bases de datos de entidades financieras, comerciales y de servicios, ley de Habeas Data.

Ley 1581 de 2012 (Ley General de Protección de Datos Personales): Sobre el tratamiento de los datos personales de los ciudadanos en Colombia regulando la recolección, almacenamiento, protección y uso de los datos por parte de las organizaciones.

Prueba De Penetración o Pentesting.

El pestenting es una metodología usada para poner a prueba los sistemas informáticos de una organización, es poder simular un ataque de un hacker quien buscaría buscas las vulnerabilidades y luego explotarlas para lograr su objetivo.

Por medio de los resultados del pentesting se pueden tomar medidas para mejorar y mitigar las vulnerabilidades encontradas de acuerdo con las prioridades de la organización, el pentesting tiene 6 fases y son las siguientes:

Reconocimiento

En esta primera fase se busca recoger toda la información pública acerca del objetivo, esta información ayudará en las siguientes fases para tomar decisiones en cómo desarrollar el escaneo, existen 2 tipos de reconocimiento, el primero es el activo, donde hay una interacción directa con el objetivo y donde se dejan rastros digitales del análisis realizado, en muchos casos se requiere autorización para realizar este tipo de reconocimiento, el segundo es el pasivo, es

donde no se deja ningún rastro o evidencia de la recolección de la información, se reúnen todos los datos sobre un sistema sin tener un contacto directamente con el objetivo.

Escaneo

Posterior a la fase de reconocimiento y con la información pública obtenida es perfilar el objetivo para realizar una exploración de vulnerabilidades completo, en esta etapa del pentesting se identifican toda vulnerabilidades para luego tomar la decisión y alistar para la siguiente fase, la herramienta para realizar esta fase por ejemplo puede ser NMAP.

Obtención de Acceso

Teniendo un listado de vulnerabilidades se debe validar que exploits se pueden utilizar para lograr el acceso a los sistemas, de esta manera se hacker puede sacar provecho a las vulnerabilidades y activar las acciones maliciosas en cumplimiento del objetivo propuesto, la herramienta para realizar esta fase por ejemplo es Exploit que ya viene instalada en NMAP.

Mantenimiento del Acceso

En esta fase del pentesting debe de asegurar la persistencia del acceso al sistema y es donde se busca escalar los privilegios del sistema, esta fase también es conocida como postexplotación.

Borrado de Huellas

En esta fase que es posterior a la simulación del ataque se debe eliminar todas las huellas que puedan delatar a quien hizo el ataque debido a que le pueden servir a un hacker en caso real y pueda aprovechar esta información de manera maliciosa.

Elaboración del reporte

En esta última fase se deben de elaborar los informes pertinentes donde los profesionales en seguridad de la información comunican y describen las vulnerabilidades encontradas para que

el equipo blue team pueda tomar las acciones para mitigar estas brechas de seguridad encontradas por el equipo red team.

Herramientas Principales para el Desarrollo del Pentesting.

Metasploit

Es un framework líder en el área de la ciberseguridad, es de código abierto que permite realizar pruebas de penetración, desarrollar scripts propios y ejecutar exploits. Esta herramienta te permite consultar una amplia lista de scripts debidamente documentados para fines muy específicos permitiendo elegir los más actualizados y se ajusten a la necesidad.

Nmap

Una herramienta especializada en el área de ciberseguridad de código abierto cuyo objetivo es dirigido a realizar exploraciones y auditorias de red tales como escaneo de puertos, mapeo de la red, identificación los hosts conectados y servicios disponibles en la red para determinar las vulnerabilidades de los activos identificados.

OpenVas

Es un sistema cuyo objetivo es identificar vulnerabilidades para sistemas, es un software de código abierto que tiene a su disposición una base de datos de vulnerabilidades para detectar fallos de seguridad en redes internas y externas, es utilizado para realizar ejercicios de pentesting y así poder mejorar la seguridad de la red.

ExploitDB

Es una aplicación web desarrolladas por Offensive Security donde concentran una gran cantidad de exploits para ser ejecutados por pentester de forma gratuita en auditorias de seguridad.

CVE

Common Vulnerabilities and Exposures, estándar cuya finalidad es poder informar, advertir y colaborar con los profesionales de ciberseguridad sobre la documentación correspondiente a las vulnerabilidades de seguridad en sistemas informáticos ya detectadas e incluso en como poder mitigar dichas vulnerabilidades, además son identificadas a partir de un consecutivo único con el cual son guardadas y compartidas con otras bases de datos, por ejemplo: CVE-2024-43701, esta página https://cve.mitre.org/ es de las más reconocidas y tiene un base datos muy amplia y actualizada con información de los CVE.

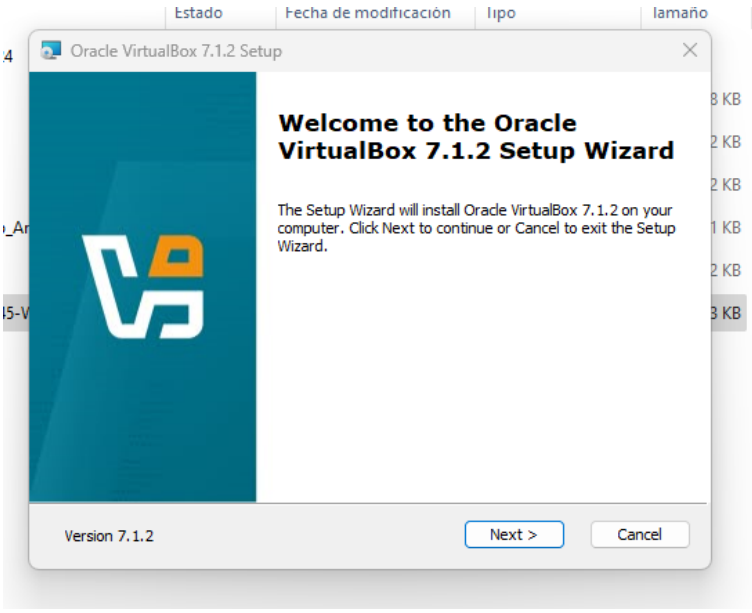
Instalación, Configuración y Evidencia de Preparación del "Banco de Trabajo"

Paso A

Se realiza la instalación de la herramienta Virtual Box en su última versión 7.1.2 a continuación la evidencia de instalación, como se muestra en las figuras 1 y 2.

Figura 1

Inicio de Instalación Virtual Box del Sitio Oficinal



Fuente. El Autor.

Figura 2

Se Muestra Virtual Box Instalado en su Última Versión 7.1.2

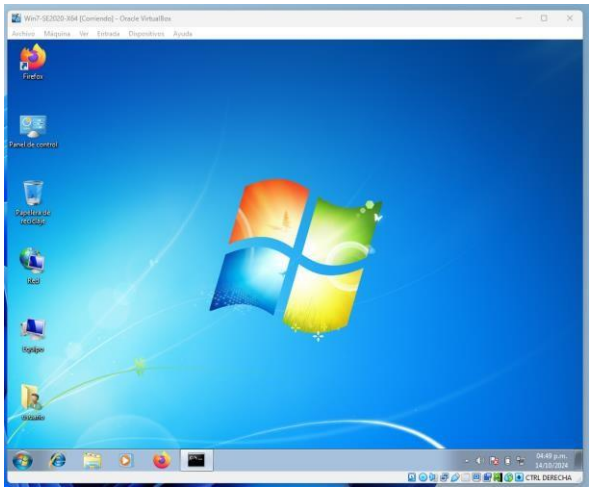
Fuente. El Autor.

Paso B

Se ingresa al link RedTeam&BuleTeam2024 para descargar la imagen en formato .OVA de Windows 7 y se hace la importación como se muestra en la figura 3.

Figura 3

Máquina Virtual con Windows 7

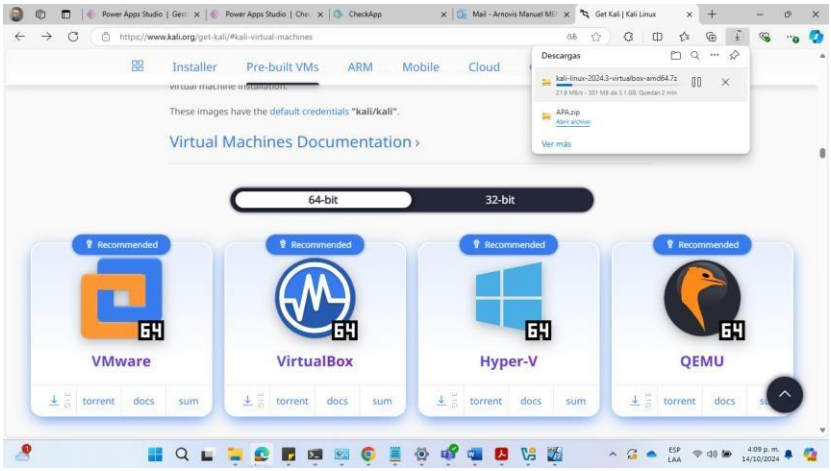


Fuente. El Autor.

A continuación, se muestra la descarga y evidencia de instalación de la máquina virtual Kali Linux descarga del sitio oficial como se muestra en las figuras 4 y 5.

Figura 4

Descarga Imagen Kali Linux desde su Sitio Oficial



Fuente. El Autor.

Figura 5

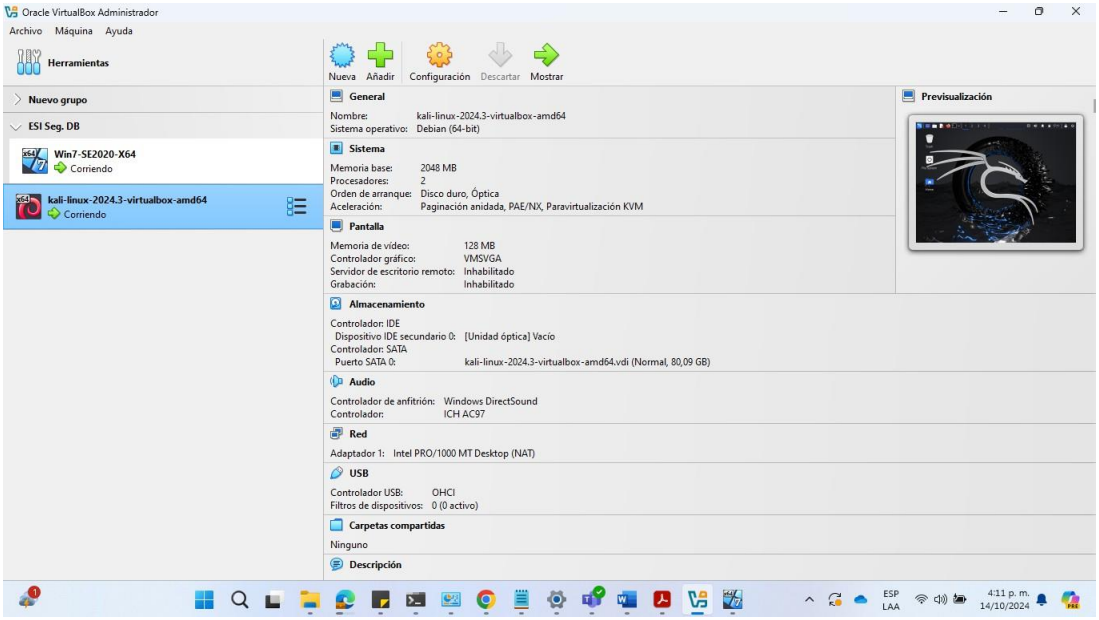
Instalación Finalizada Máquina Virtual Kali Linux

Fuente. El Autor.

En la figura 6 se muestra las máquinas virtuales de Windows 7 y Kali Linux instaladas.

Figura 6

Instalación con Virtual Box Windows 7 y Kali Linux



Fuente. El Autor.

Se Describe de Manera Específica la Metodología y Herramientas Software Utilizadas para Llevar el Ejercicio de Red Team.

Para poner a prueba el sistema se utilizará la metodología pentesting.

Reconocimiento

En esta etapa con la información suministrada lo que se hace es hacer un perfilamiento, se sabe que es una maquina Windows que debe tener puertos, que debe de estar conectada en la red LAN de la organización, tiene una aplicación vulnerable y esta permite acceder a través de Shell y escalar privilegios para llegar como administrador de sistema.

Lo anterior permite elegir una herramienta como NMAP instalada en KALI LINUX para realizar un escaneo de puertos y buscar la aplicación vulnerable en la siguiente fase.

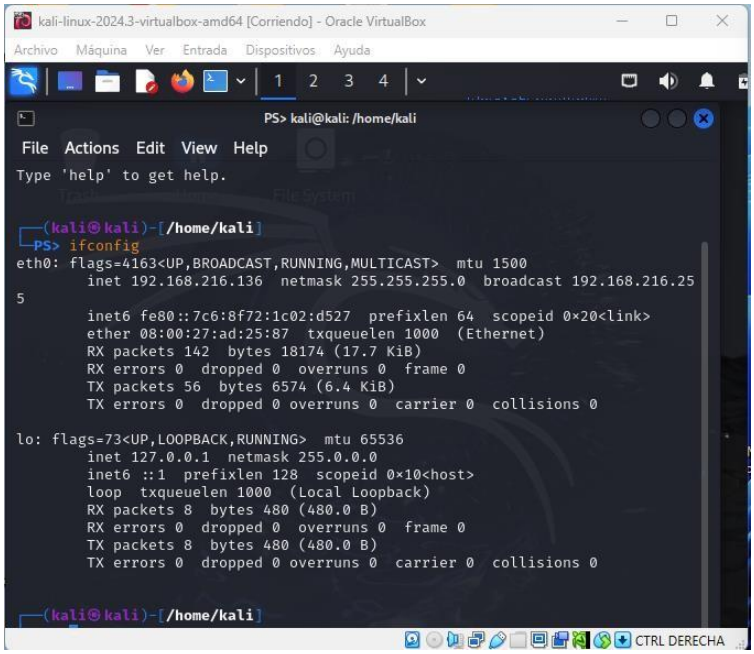
Escaneo

Se tiene la herramienta NMAP definida para realizar el escaño de puertos y aplicaciones vulnerables por donde se pueden estar haciendo fugas de información, a continuación, se mostrará las figuras con el paso a paso.

Como en contexto estamos en una red LAN debemos de ubicar primero la maquina objetivo desde donde se puede estar presentando la fuga de información, para esto se debe hacer un escaneo de red desde la herramienta NMAP como lo muestra la figura 7 y figura 8 a continuación.

Figura 7

Obtención Dirección IP para Rango de Escaneo de Direcciones IPs

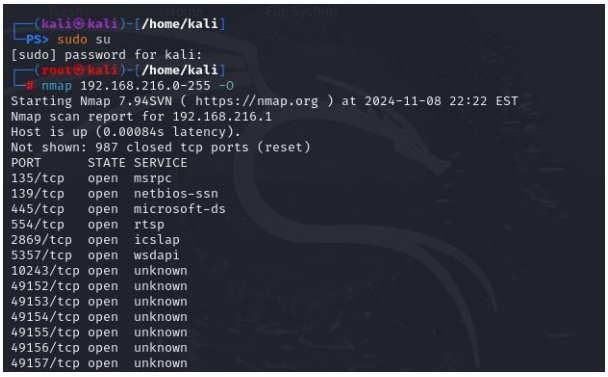


Fuente. El Autor. Nota. La dirección IP de maquina Kali Linux es 192.168.216.136.

Se debe realizar un escaneo de IP con el rango 192.168.216.0 - 192.168.216.255 y el parámetro -O para identificar el sistema operativo, debe ser Windows como se muestra en la figura 8 y figura 9, el objetivo es poder saber que máquinas se encuentran conectadas a la red con esta característica.

Figura 8

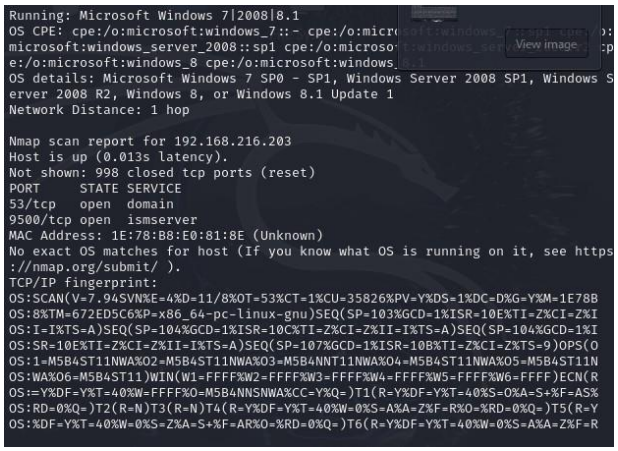
Inicio Escaneo IPs Rango 192.168.216.0 - 192.168.216.255



Fuente. El Autor.

Figura 9

Resultado del Escaneo de IPs 192.168.216.0 - 192.168.216.255

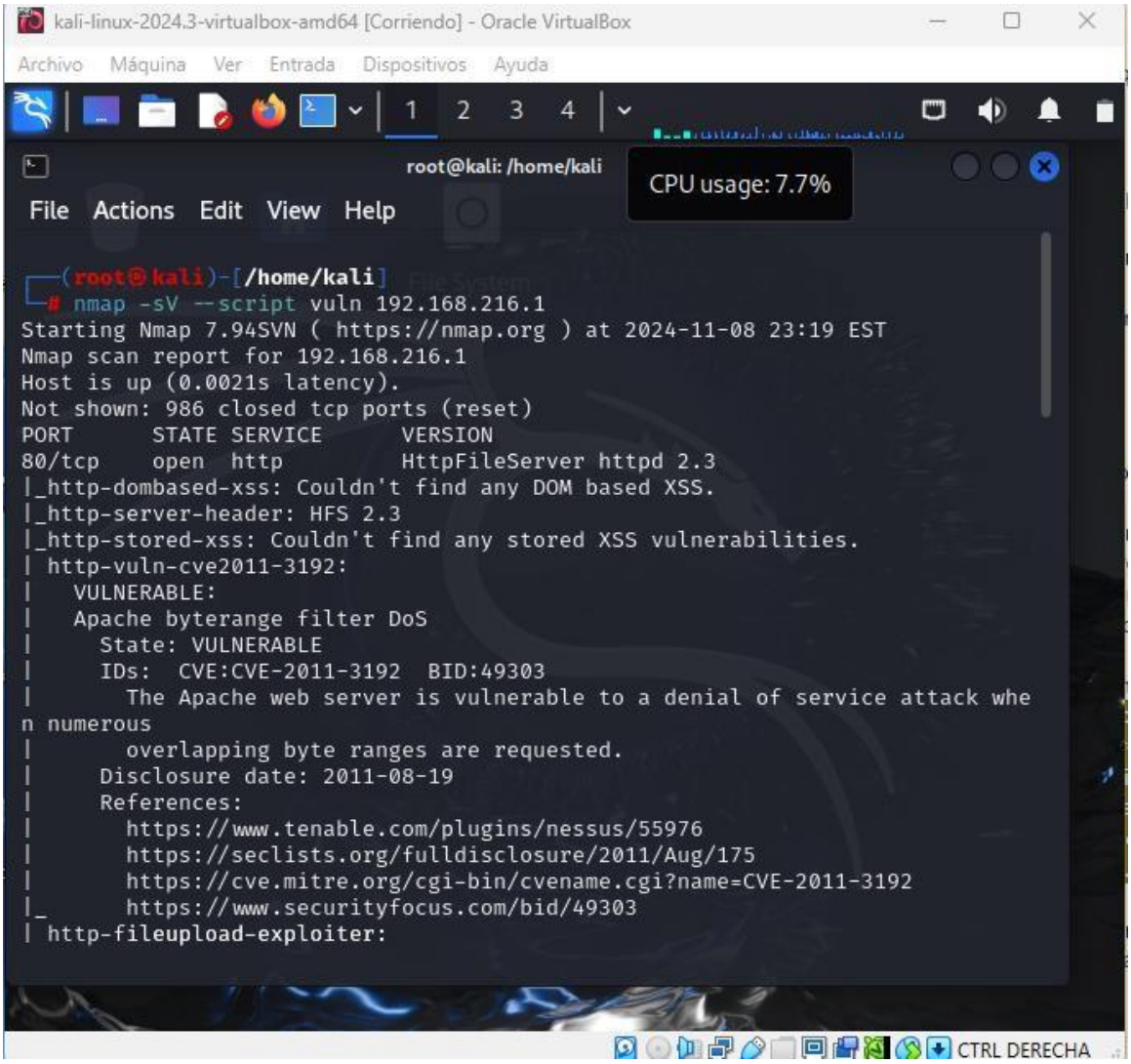


Fuente. El Autor.

De los resultados obtenidos por fortuna son pocas maquinas, pero se puede apreciar que la maquina con IP 192.168.216.1 tiene sistema operativo Windows, versión 7, con esto se puede enfocar en esta máquina para profundizar el escaño como se muestra en la figura 10.

Figura 10

Profundizando el Escaneo Sobre la Dirección 192.168.216.1

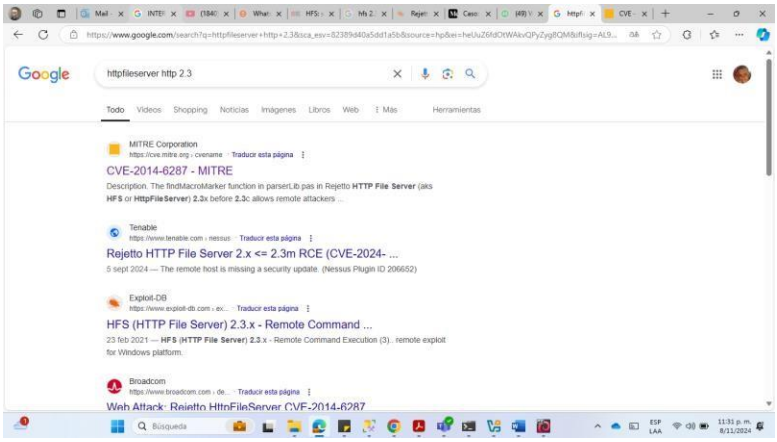


Fuente. El Autor.

De acuerdo con el resultado anterior de todas las vulnerabilidades encontradas llama la atención el puerto 80 que está abierto con una aplicación corriendo httpfileserver http 2.3 a primeras es un servicio para compartir archivos, sin embargo, se busca en internet para más información sobre este, en las figuras 11 y 12 encontramos información sobre esto.

Figura 11

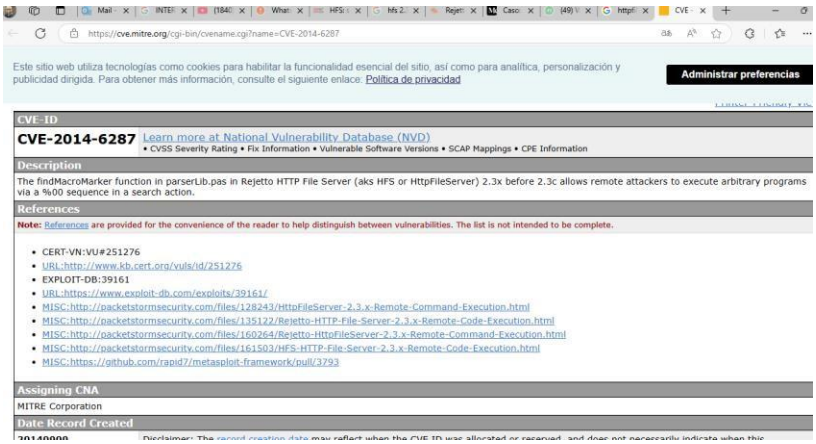
Indagando en internet sobre httpfileserver http 2.3



Fuente. El Autor.

Figura 12

Página de MITRE donde se Muestra Más Sobre esta Vulnerabilidad



Fuente. El Autor.

Nota. Mitre es un repositorio web donde se pueden encontrar muchas vulnerabilidades con su respectivo código CVE, descripción, como explotar la vulnerabilidad y mitigarla.

Esta vulnerabilidad corresponde al código CVE – 2014-6287 (Miltre, 2004), que indica que es un servidor de archivos llamado HFS que permite a un atacante ejecutar cualquier programa en el sistema, también nos muestra cómo podemos ejecutar comandos remotos y hacer el ataque.

La aplicación HFS de acuerdo con (Rejetto,2024), es una aplicación cuya función es tener un servicio para compartir archivos desde el disco duro a través del protocolo http, ofrece funcionalidades y facilidades para acceder desde la web a los archivos del disco duro en computadora.

Es importante destacar que en la página del fabricante oficial denotan que la versión antigua v2, específicamente 2.3 y 2.4 no se deben usar debido a que hay una vulnerabilidad que permite a un atacante controlar la computadora, recomiendan usar desde la versión 3 donde según ellos no existe esta vulnerabilidad como se muestra en la figura 13.

Figura 13

Página Web Oficial Aplicación HFS, se Indica Vulnerabilidad

Fuente. El Autor.

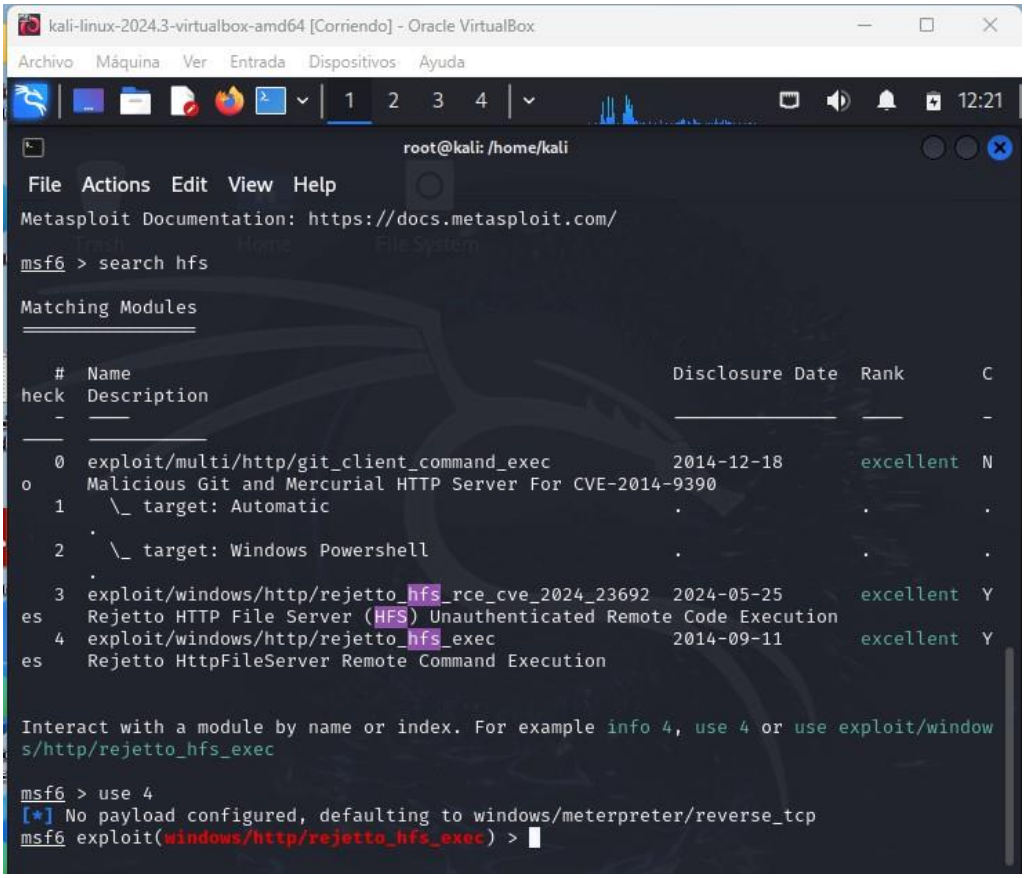
Obtención de Acceso

En esta etapa se usará la herramienta Metasploit que ayudará a explotar las vulnerabilidades encontradas con la herramienta NMAP en el paso anterior.

Con el comando msfconsole y posterior se busca con el comando search los exploit relacionados con HFS para elegir el más indicado de acuerdo con la necesidad que se tenga como se muestra en la figura 8.

Figura 14

Elección el Exploit #4 que es para Windows

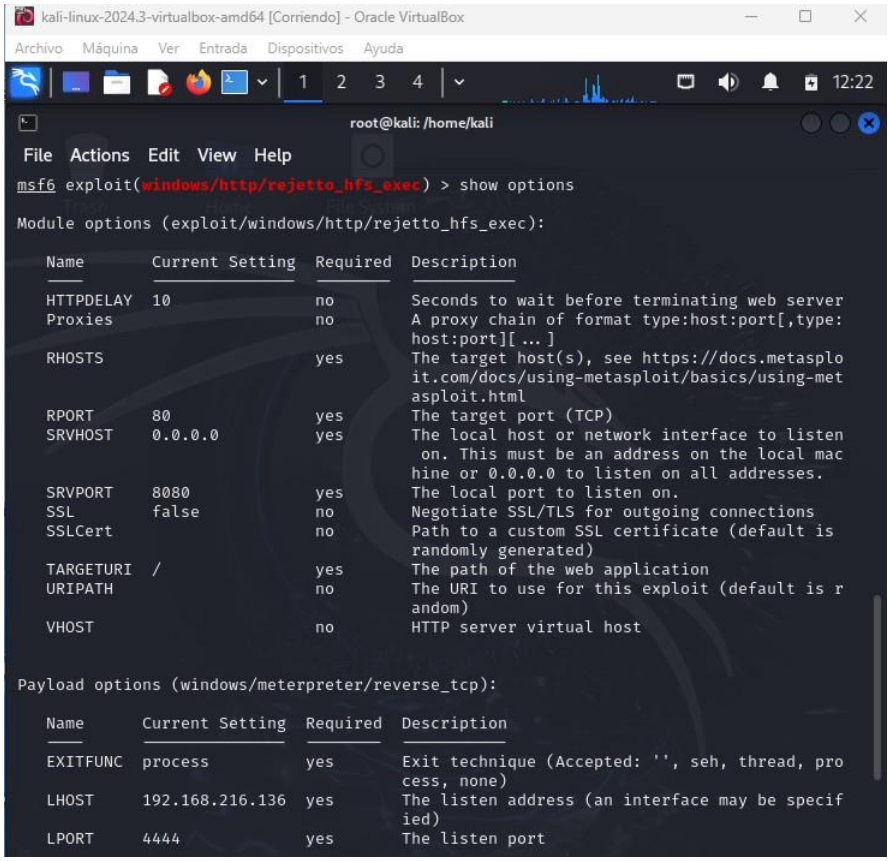


Fuente. El Autor.

Con el comando show options se deben visualizar las opciones para configurarlas como se muestra en la figura 15.

Figura 15

Parámetros del Exploit son Mostrados para Poder Configurar



Fuente. El Autor.

Solamente es necesario configurar el host objetivo o host remoto (RHOSTS) que de acuerdo con las opciones falta indicar, para las opciones como RPORT 80 y LHOST 192.168.216.136 no es necesario realizar configuración debido a que la aplicación objetivo se está ejecutando en el puerto 80 y el exploit tomó por defecto la dirección IP del equipo local (KALI LINUX) de manera correcta como se muestra en las figuras 16 y 17.

Figura 16

Asignando con el Comando Set la Dirección del Host Remoto

Fuente. El Autor.

Posteriormente a la configuración del exploit se procede a ejecutarlo para iniciar con el ataque, es decir para poder penetrar en la maquina objetivo, se escribe en la consola el comando run como se muestra en la figura 17.

Figura 17

Iniciando el Ataque a la Maquina Objetivo 192.168.216.1

Fuente. El Autor. *Nota.* Al quedar el cursor con el indicativo meterpreter> significa que se tuvo éxito en el acceso a la maquina remota, es decir ya estamos dentro de nuestro objetivo y podemos iniciar con la elevación de los privilegios para ejecutar los comandos que sean necesarios.

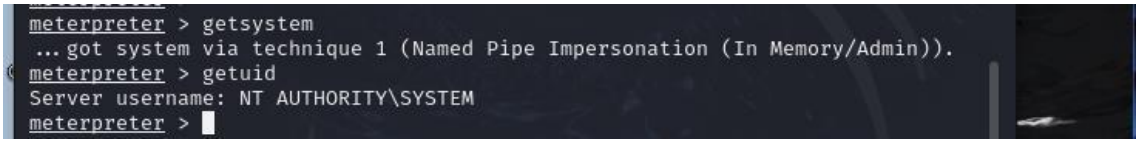
Mantenimiento del acceso

Para mantener el acceso se realiza la creación de una cuenta que ayude para seguir teniendo acceso a la máquina, en este caso también para demostrar que se pudo tener acceso y realizar elevación de privilegios paso anterior y en este crear la cuenta administrador.

A continuación, se elevan los privilegios con el comando getsystem y son validados con el comando getuid, la indicación de Server username: NT AUTHORITY\SYSTEM significa que tenemos privilegios de super usuario o usuario administrador como se observa en la figura 18.

Figura 18

Elevación de Privilegios Comando getsystem.

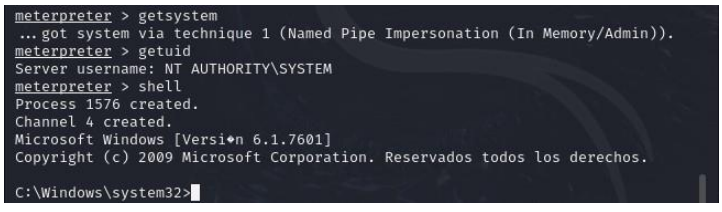


Fuente. El Autor.

Ahora se debe usar el comando Shell para tener acceso al cmd del equipo remoto, el equipo objetivo que es la maquina Windows 7 para poder crear el usuario con permisos de administrador como se muestra en la figura 19.

Figura 19

Comprobación Nuevos Permisos de Super Usuario o Administrador

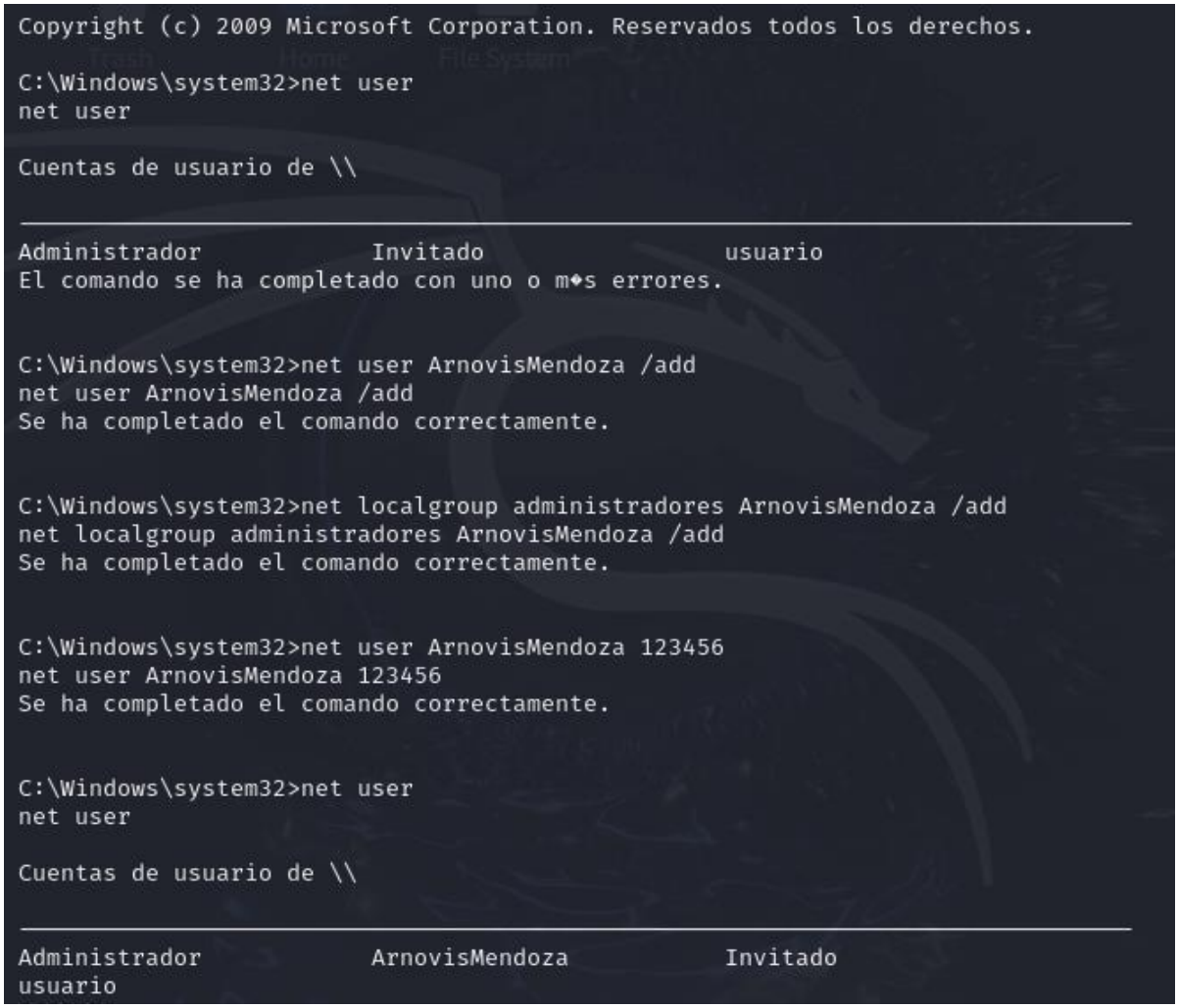


Fuente. El Autor.

En la figura 20 se crea el usuario administrador ArnovisMendoza y se le asigna la contraseña 123456 usando los comandos de net user.

Figura 20

Usuarios Actuales en la Maquina Remota 192.168.216.1



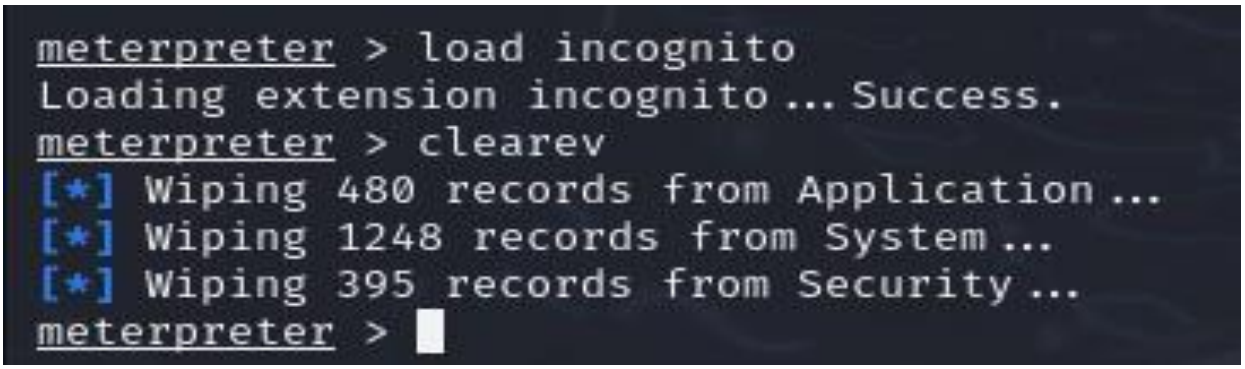
Fuente. El Autor.

Borrado de huellas

Se eliminan las huellas desde la herramienta Metasploit de la manera siguiente apoyados desde el meterpreter con los comandos load incognito y clearrev para eliminar todo el rastro de las conexiones como lo muestra la figura 21.

Figura 21

Eliminación de Huellas Comando clearrev



Fuente. El Autor.

Elaboración del reporte

A continuación, se entrega reporte al equipo de blue team de los hallazgos:

Se realizar un escaneo con la herramienta NMAP al rango de la red 192.168.216.0 - 192.168.216.55, solamente se encuentra el equipo de cómputo 192.168.216.1 el cual se evidencia que es una maquina Windows 7.

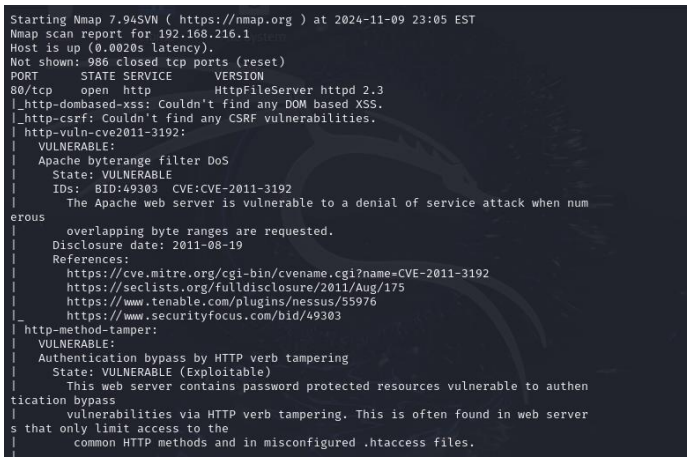
Se realiza un escaneo profundo a la maquina 192.168.216.1, identifica que a través de la aplicación HFS - HTTP file server versión 2.3, cuyo fabricante es Rejetto quien reconoce que esta versión tiene una vulnerabilidad grave, es por donde hay un fallo de seguridad el cual permite a cualquier atacante poder ejecutar cualquier código en la computadora 192.168.216.1 cuyo sistema operativo es Windows 7, esta aplicación se está ejecutando desde el puerto http 80.

Se debe tener en cuenta que estas aplicaciones para compartir archivos no están bajo un control de la organización y cualquier usuario podrá enviar información sin que la organización pueda hacer el debido monitoreo de que se comparte y a quien.

También la maquina 192.168.216.1 tiene otras vulnerabilidades y puertos abiertos como se muestra en las figuras 22, 23, 24 y 25 a continuación.

Figura 22

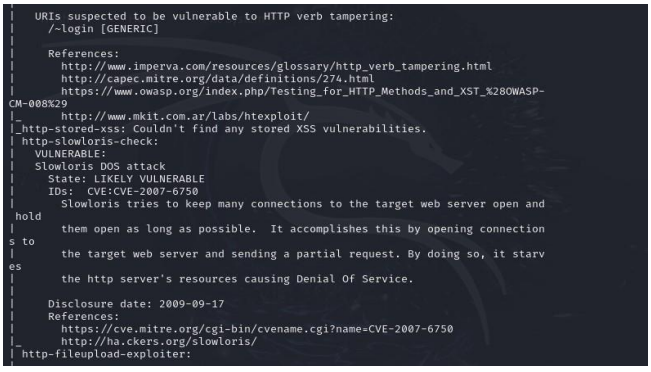
Página 1 Resultado Escaneo Vulnerabilidades IP 192.168.216.1



Fuente. El Autor.

Figura 23

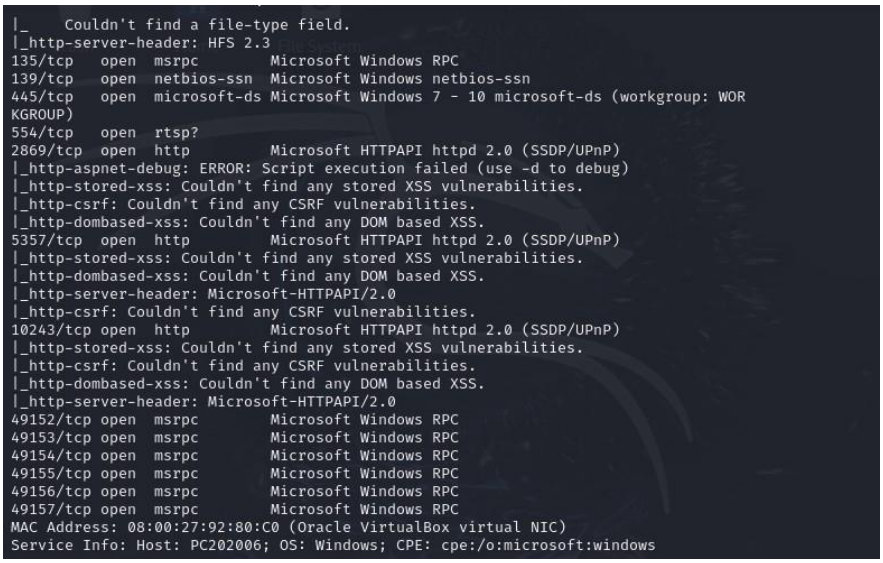
Página 2 Resultado Escaneo Vulnerabilidades IP 192.168.216.1



Fuente. El Autor.

Figura 24

Página 3 Resultado Escaneo Vulnerabilidades IP 192.168.216.1



Fuente. El Autor.

Figura 25

Página 4 Resultado Escaneo Vulnerabilidades IP 192.168.216.1

Fuente. El Autor.

Herramienta Utilizada Para Poder Identificar Los Fallos De Seguridad De La “Máquina Windows”

La herramienta que se utilizó para poder identificar los fallos de seguridad de la maquina Windows se llama NMAP, el puerto que abre la aplicación del anexo es el 80 http.

Impacto y afectación del ataque en la máquina (Windows)

Las afectaciones pueden ser muy diversas, pero en este caso el ataque se realiza a través del puerto 80 debido a que es usado código maliciosos para obtener el acceso indebido, de esta manera es posible lograr acceso a la maquina y posteriormente ganar privilegios de super usuarios o administrador para realizar movimientos laterales desde la maquina Windows lo que comprometería aspectos mencionados en la figura 26, tales como:

Figura 26

Afectaciones Directas e Indirectas Sobre la Maquina Windows

Fuente. El Autor.

Primeras Acciones Durante un Ataque Informático en Tiempo Real

Siendo especialista en seguridad informática, haría los siguiente:

Validar que realmente me estén atacando, identificando el ataque y su tipo, revisar logs, eventos del sistema, revisar los procesos en el sistema operativo por medios del administrador de tareas para identificar la amenaza.

Desconectar la máquina de la red e internet, el propósito es aislarla para evitar a toda costa la transferencia de información o que el atacante haga movimientos laterales.

Se deben tomar las evidencias que se está siendo víctima de un ataque de manera rápida para una recopilación de pruebas, cadena de custodia y posterior análisis forense.

Se debe buscar en internet información sobre la amenaza detectada para saber cómo se puede eliminar de manera segura del equipo.

Se debe habilitar el firewall para bloquear la dirección IP desde donde se está haciendo el ataque.

Validar desde el administrador de equipos de Windows, que recursos están siendo compartidos, que usuarios están conectados y que archivos están abiertos para deshabilitar los accesos.

Se debe realizar escaneo de distintos antivirus para eliminar cualquier virus, se debe reparar las entradas del registro de Windows, revisar con la herramienta Autoruns de Microsoft las aplicaciones autorizadas de autoinicio al momento de encender el equipo.

Validar la integridad de todos los archivos guardados en el sistema de Windows.

Se debe realizar una revisión a todas las máquinas de la red para validar si el atacante alcanzó a hacer movimientos laterales.

Medidas de Hardenización Propuestas

Debe considerar el S.O. Windows 7 no tiene un soporte o respaldo de su fabricante Microsoft debido a que está descontinuado, por lo tanto, se debería siempre tener la versión más actualizada del sistema operativo que sería la versión Windows 11, esto garantiza que las actualizaciones más recientes y la mitigación de riesgo estaría al día.

Se deben aplicar las siguientes medidas de hardenización:

La cuenta del usuario administrador e invitado debe estar deshabilitada, debe de haber una cuenta administradora, pero con otro nombre.

La cuenta de usuario debe ser de tipo estándar, lo que limita a los permisos de ejecución en el sistema.

Se le debe hacer cumplir al usuario para que todas las contraseñas sean robustas, es decir mínimo con 12 caracteres alfanuméricos, combinados con caracteres especiales y con minúsculas y mayúsculas. Las contraseñas todas deben de ser caducables, deben de ser cambiadas mínimo a un periodo no mayor a 3 meses.

Restricción de software, se debe permitir la ejecución de solamente las aplicaciones autorizadas, el resto no se debe permitir su ejecución.

Deshabilitar el acceso remoto, ya sea por escritorio remoto, FTP y SSH.

Deshabilitar los puertos USB, pueden ser la entrada de un virus o pueden facilitar la fuga de datos por parte del usuario.

En la red, después del router del proveedor de internet ISP, se debe instalar un firewall de nueva generación, puede ser un Pfsense para bloquear todos los, solo dejar abiertos los puertos estrictamente necesarios.

Instalación de un antivirus y comprobar que siempre esté actualizado.

Se debe instalar contraseña a la BIOS SETUP del equipo con una contraseña robusta para evitar cambios en el boot del sistema.

Se debe instalar y configurar el cifrado de disco con la herramienta BitLocker lo que evita poder ingresar a las carpetas y archivos que se tengan en el disco duro.

Deshabilitar la ejecución de scripts a través de PowerShell y cmd en Windows.

Diferencias equipo Blueteam y CSIRT

En la tabla 1, se describen las principales diferencias.

Tabla 1

Comparación entre blue team y CSIRT

Blue team	CSIRT
La tarea principal actuar de manera proactiva, siempre este equipo está activo es búsqueda de defender los sistemas, la redes y la información de la organización.	Este equipo es reactivo, se activa posterior a un incidente de seguridad.
Previene la ocurrencia de un ataque, siempre está enfocado en la detección y mitigación de amenazas y/o vulnerabilidades.	Su objetivo es poder contener y minimizar el impacto que esté o haya causado un incidente de seguridad.
Toma medidas de hardening para fortalecer la seguridad de la infraestructura, estableciendo políticas nuevas y actualizando las existentes.	Este equipo debe de realizar los análisis para entender lo sucedido en momentos posteriores a un incidente con el fin de poder reforzar las medidas de seguridad y evitar que se repita.
Monitorea la seguridad de redes y sistemas en búsqueda de actividades anormales, implementa sistema de prevención como firewall IDS, antivirus.	Gestiona los incidentes de seguridad, realiza investigación, análisis y reportes forenses comunicando a los interesados en la organización, tras sufrir algún incidente de seguridad para evaluar su impacto y ayuda en la normalización y recuperación posterior a un incidente.
Realiza análisis de vulnerabilidades, auditorias y pruebas de pentesting simulando ataques, todo con el objetivo de mejorar y minimizar los riesgos.	

Fuente. El Autor. *Nota.* Comparación entre las principales diferencias entre Blue team y CSIRT.

Uso e Importancia de Trabajar con CIS

El CIS (Center Internet Security) entidad sin ánimos de lucro, que a nivel mundial por su perspectiva en progreso de la seguridad informática donde se han venido desarrollando estándares, buenas prácticas, marcos de referencias y herramientas que han fortalecido la ciberseguridad.

El CIS se utilizaría con el fin de poner en práctica los controles y acciones defensivas para prevenir ataques de alto impacto y más peligrosos, también en el cumplimiento de múltiples marcos jurídicos, normativos y reglamentarios en los distintos países.

El CIS provee una guía a las organizaciones para aumentar el nivel de seguridad de manera eficaz en los siguientes 4 enfoques:

En las organizaciones les da una estructura, marco y estrategia a los programas de seguridad.

Ayuda a priorizar las medidas y técnicas más eficaces siendo especifico de acuerdo con las necesidades de cada organización.

Enfoque robusto y probado en la gestión de los riesgos según la organización.

Cumplimiento con regulaciones y marcos ya existentes como ISO27001, BUTS, NERC, FISMA, entre otros.

SIEM Características Principales

(Security Information and Event Management), permite registrar, almacenar para analizar y detectar anomalías con relación a los datos de seguridad de otras fuentes para dar respuesta en tiempo real.

Entre las principales funcionales son:

Registro y normalización de datos de la infraestructura como firewall IDS/IPS, bases de datos, servidores, sistemas entre otros, con estos se pueden realizar análisis para tomar acciones de ser necesarias.

Identificación de eventos sospechosos o de comportamiento malicioso que ayudan a la detección de los ataques.

Generación e informes resumidos y detallados sobre las actividades en la infraestructura, cumplimiento de políticas, regulaciones o normas.

Cuando ocurren incidentes un SIEM ayuda sobre el análisis forense dando más información para esclarecer lo ocurrido y el nivel de impacto.

Aspectos que Aporten al Desarrollo de Estrategias de Redteam &Blueteam.

Existen elementos que de manera importante cumbre y apoyan las estrategias de red team y blue team a nivel general en las organizaciones, deben de ser incluidas desde la estrategia corporativa y la gobernanza TI.

Además, no se debe dejar de lado los objetivos y alcances para la conformación de los equipos, perfil profesional, legal, actividades ejecutadas, pruebas, resultados y comunicación a los interesados con los planes de acción para minimizar los riesgos de las brechas o vulnerabilidades encontradas.

Los aspectos que aportan en desarrollar y mejorar la estrategia de equipos red team y blue team son los siguientes:

Aspectos red team:

Ético y Legal

En este ámbito se debe mirar en dos sentidos, sobre los colaboradores que conformen los equipos de red team y sobre los clientes que se les presente el servicio o siendo lideres miembros

en las organizaciones, considerar que para asegurar la privacidad de la información, se debes establecer acuerdos de confidencialidad con los colaboradores u organizaciones prestadores de servicio, apoyados en normas como ISO 27001 o NITS se deben establecer controles y políticas claras sobre el control de acceso, aceptación de herramientas y políticas, capacitaciones y acompañamiento a los procesos críticos con la respectiva supervisión, sobre lo segundo se le debe de dar acceso mínimo, es decir que solo pueda ver o revisar puntualmente lo requerido y queden registros en logs auditables en las herramientas utilizadas para tal fin, con esto se busca asegurar el cumplimiento de la ley y la actuación dentro de las normas para evitar filtraciones que pueda ocasionar daños y perjuicios.

Para generar confianza, las organizaciones deben ante todo hacer un contrato donde queden clausulas y acuerdos de confidencialidad puntuales y claros donde la empresa contratada pueda responder en caso de alguna violación o mal manejo que se le pueda llegar dar a la información.

Mano de Obra

Los colaboradores involucrados en los equipos de red team son una pieza clave debido a que de ellos depende la efectividad de los procesos realizados dentro del equipo, por lo tanto, deben de tener las habilidades técnicas adecuadas de acuerdo con su rol dentro del equipo, certificaciones técnicas y experiencia que ameriten para dar frente a los retos a los que se vean expuestos.

Herramientas

Existen un sin números de herramientas de pago y gratis, también las que puedan ser construidas por el mismo equipo, la clave de las herramientas es poder elegir de acuerdo con las necesidades.

Las herramientas permiten realizar los test de vulnerabilidades ya sean básicos o sofisticados, depende del objetivo y el contexto elegir una u otra, se debe tener siempre presente que estas herramientas se les debe dar buen uso, de manera ética y respectando las leyes del país donde se ejecuten, entre las herramientas más importante se tienen:

Kali Linux

Es un sistema operativo Linux especializado en ciberseguridad para realizar pruebas de pentesting, auditorias de seguridad que viene dotada para realizar ataques, escaneos de puertos, explotación, entre otras.

NMAP

Esta herramienta se especializa en realizar escaneos de puertos, redes, host que se encuentren en determinada red con alcance de NMAP para identificar vulnerabilidades.

Miltre

Es una base de datos en la web donde se pueden consultar las vulnerabilidades encontradas por NMAP y donde especifican como pueden ser explotadas estas vulnerabilidades y también como mitigarlas, sirve de referencia para saber el grado de riesgo y de impacto, estas vulnerabilidades tienen un código característico CVE (Common Vulnerabilities and Exposures), es un código único de referencia que identifica y clasifica las vulnerabilidades de hardware o software.

Metasploit

El objetivo principal de esta herramienta es realizar la prueba de penetración, tiene exploit o scripts preconfigurados que solamente se deben parametrizar para ejecutar un ataque a un sistema determinado, los parámetros depende de cada script donde se pueden solicitar datos como dirección IP, puerto, entre otros, posterior al ataque y teniendo acceso al sistema se puede

continuar con la explotación y pos-explotación permitiendo realizar ataques a profundidad o movimiento laterales.

Wireshark

Esta aplicación cuya razón de ser es poder capturar paquetes de datos de red que estén en transmisión en una red para dejarlos a disposición de manera detallada donde se describen tipos de paquetes, datos de origen y destino, protocolo, entre otros.

Para los equipos de red team es de vital importancia debido a que muestran todas las actividades y servicios que se vienen ejecutando en una red permitiendo poder identificar activos informáticos de alto valor para la realización de nuevas pruebas de pentesting y profundizar las pruebas.

Metodología

El pestenting es una metodología usada para poner a prueba los sistemas informáticos de una organización, es poder simular un ataque de un hacker quien buscaría buscas las vulnerabilidades y luego explotarlas para lograr su objetivo.

Por medio de los resultados del pentesting se pueden tomar medidas para mejorar y mitigar las vulnerabilidades encontradas de acuerdo con las prioridades de la organización.

Afectaciones y Alcances del Ataque

Las afectaciones y alcance denotan el éxito de las pruebas y la capacidad de la infraestructura en resistir un ataque de un hacker que realmente aproveche robando la información y causando estragos.

Los equipos de red team se proponen en alcanzar los activos informáticos de alto valor de una organización, tal cual como lo haría un hacker tratando de llegar a tener acceso no autorizado a sistemas, datos, comprometer cuentas con privilegios de administrador, dejar

accesos permanentes de manera remota, también probar los accesos físicos a las instalaciones, hacer permanente su acceso con malware o backdoors, comprobar que pueden también tener afectaciones sobre los servicios vitales de la organización que pueden tener impacto en sus operaciones y económicas.

Capacidades del Equipo Blue Team

Cuando los equipos de red team operan, ponen a prueba los controles, medidas, políticas, monitoreo y todas las acciones que tomaron los equipos blue team para evitar que la organización sufra un ataque, de manera que el éxito del equipo red team muestra de manera inversamente proporcional el éxito o fracaso del equipo blue team, la importancia de esto radica en que el equipo blue tomara las acciones para fortalecer las brechas identificadas y explotadas por el equipo red.

Informes y Comunicación

El equipo red team al finalizar todas las acciones debe entregar un informe detallado de los hallazgos y alcances de las pruebas, demostrar hasta donde pudo llegar y las afectaciones que pudo realizar a la infraestructura informática, este informe es de vital importancia hacerlo comunicar de manera clara y concisa para que el equipo blue pueda realizar el hardering necesario y los directivos de la organización sea consientes a lo que están expuesto y puedan asignar recursos de ser necesario para la mitigación de estas brechas detectadas por el equipo red.

Aspectos blue team:

Ético y Legal

Al igual que los equipos red team, los equipos blue deben de tener un cumplimiento legal con respecto a las leyes del país donde se encuentre conformado, también ético debido que los miembros de los equipos blue tiene acceso a cuentas con privilegios e información confidencial

que puede ser divulgada y aprovechada con un ciberdelincuente, es importante poder tener en los contratos laborales clausulas claras de confidencialidad al igual que otras medidas como la segregación de funciones por roles dentro del equipo para así ayudar a que nadie tenga un alcance total con respecto a la gestión de los sistemas.

Mano de Obra

Deben ser profesionales idóneos que tengan el perfil adecuado para ejercer las funciones de contención de ataques y con experiencia en el área, de unos buenos miembros harán un gran equipo, deben de estar en constante capacitación debido a que las formas y características de un ataque son múltiples y vienen en aumento.

Herramientas

Existen muchas herramientas, pero lo ideal es dependiendo de la organización elegir las idóneas, el contexto de todas las organizaciones no es igual y no tienen los mismos activos, entre las herramientas de contención existen las siguientes:

Pfsense

Es un firewall de última generación que permite establecer reglas de trafico de la red haciendo que el nivel de seguridad se vea aumentando, también filtra los paquetes y rechazando conexiones no habituales con la red de la organización.

Snort

IDS/IPS de código abierto que mientras el IDS detecta sobre alguna intrusión, el IPS actúa aislando o bloqueando esa actividad maliciosa en tiempo real.

AlienVault OSSIM

SIEM que identifica, pero que también alerta al os administradores de la infraestructura para contener algun ataque informático.

OKTA

Autenticador multifactor que ayuda a que el usuario sea el realmente genuino proporcionando una doble autenticación para garantizar su legitimidad.

Metodología/Estándares

El éxito del equipo blue team es evitar que la organización sea víctima de un ataque cibernético, por lo tanto, debe enfocarse en aspectos tales como: políticas de seguridad de la información, de acceso, de contraseñas, uso aceptable de TI, aplicaciones autorizadas, gestión de contraseñas, políticas de backup, políticas de gestión de incidentes y recuperación de desastres, entre otras. Las anteriores deben de estar sujetas actualizaciones e ir de manera paulatina endureciendo los controles de dichas políticas. Estas deben de tener como base algunos de los estándares ya conocidos como las norma ISO 27001, NITS, CIS, entre otras.

Controles

Los controles además de las políticas ayudan en fortalecer y agregar capas de seguridad a la infraestructura tecnológica de manera que se hace más fuerte y minimiza la posibilidad de ser víctima de un ataque, estos controles deben de ser efectivos, entre los controles se deben implementar firewall, autenticación multifactor MFA, accesos mínimos necesarios, segregación de funciones a través de asignación de roles, segmentación de la red, implementación de antivirus, implementar IDS/IPS, SIEM, entre otros.

Alertas

Los equipos de blue team deben de estar en monitoreo activo para prevenir y detectar cualquier amenaza en tiempo real, se deben apoyar utilizando sistemas de monitoreo SIEM para la detección de alguna anomalía. Los equipos también deben de estar monitoreando los logs de los principales sistemas, dispositivos de red y servidores.

Forense

En caso de sufrir un incidente el equipo CSIRT debe comunicar lo ocurrido, alcance e impacto del ataque al equipo blue team para que puedan corregir y actualizar los controles que conlleve la mitigación de la vulnerabilidad y evitar volver a sufrir un incidente igual.

Planes de Acción

El equipo blue team debe desarrollar planes de acciones ya sea debido a incidentes ya sea por haber sido víctimas de ataque, por medio de un informe a través de los equipos de red team u otras vulnerabilidades que sea reportada, este plan de acción debe asegurar que las debilidades presentadas son fortalecidas y el riesgo mitigado en su máxima expresión, todos los hallazgos o reportes deben de estar cerrados en la brevedad máxima posible.

Auditorias de Cumplimiento

Los equipos de blue team deben de solicitar auditorías internas y externas para validar el cumplimiento de las políticas en toda la organización.

Informes y Lecciones Aprendidas

Los equipos de blue team deben reportar los incidentes y lecciones aprendidas, estas deben de ser divulgadas dependiendo del caso a la organización para generar conciencia y evitar que vuelva a ocurrir, también se debe revelar a la dirección informes donde se muestre un manejo mes a mes de los indicadores de interés de la organización.

Recomendaciones para el Planteamiento de Estrategias que Permitan Endurecer los Aspectos de Seguridad En una Organización

Las recomendaciones para endurecer aspectos de seguridad en una organización tendríamos actualizaciones oportunas a las políticas de seguridad, de backup, de TI y seguridad de la información, realizar capacitaciones continuas sobre ciberseguridad abordando temas como

el phishing, implementación de MFA, de firewall y seguridad perimetral, segmentación de la red, IDS/IPS, teniendo los sistemas operativos actualizados, se debe tener Windows 11 a hoy, evaluación de análisis de riesgos, tener política de actualización a las aplicaciones críticas, monitoreo y administración por consola del antivirus, se debe contar con asesorías y auditorias de expertos de entidades externas y procedimiento de recuperación ante cualquier eventualidad para la asegurar la continuidad del negocio.

Conclusiones que Permitan la Construcción del Conocimiento Desde el Enfoque de a Ciberseguridad

Entre las conclusiones tenemos las siguientes:

Colombia tiene un marco regulatorio sobre los datos personales y delitos informáticos que dan una pauta para el cumplimiento de estos y el saber cómo actuar dentro de la ley.

Es importante que ante el ejercicio de la ciberseguridad se sepa visualizar la línea de los legal e ilegal, ya es decisión de cada uno en que línea debe estar.

Con respecto a las organizaciones se deben de tomar las medidas para generar confianza en las actuaciones tanto como empresa contratista, cliente al momento de realizar actividades que involucren información confidencial de cualquiera de las dos partes, se puede apoyar en las normas NIST e ISO 27001, manejo de tercero o proveedores.

Es importante y valioso para un ejercicio pentesting realizar cada una de las etapas que son claves porque de esta misma manera un hacker llevaría a cabo un ataque, lo que permite poder encontrar vulnerabilidades que serán mitigadas y para este caso permitió identificar desde donde se estaba dando la fuga de información lo que permite hacer el reporte al equipo de blue team para que continue con el plan acción para su minimización.

Controles técnicos NITS firewall, MFA, antivirus, actualizaciones, filtro de correo contra el phishing, capacitación del personal.

Las herramientas para llevar a cabo la metodología de pentesting juegan un papel crucial, a pesar de que son gratuitas tienen mucho que aportar debido que cuenta con una amplia comunidad y siempre es posible encontrar información al respecto, también son fácil de usar, con NMAP se pudo realizar el escaneo de vulnerabilidades, poder identificarlas y con se pude elegir el exploit para hacer la explotación adecuada de la vulnerabilidad.

No es suficiente con realizar la explotación a la vulnerabilidad sino también de revisar como puede un ciberdelincuente también hacer permanencia sobre las maquinas que logre explotar o infectar pudiendo dejar puertas traseras, cuentas de usuarios u otra forma para garantizar su conexión a los equipos.

El informe final se debe redactar de manera muy clara porque de este trabajo dependente la buena actuación de los equipos Blue team para poder realizar los planes de acción consecuentes con los hallazgos que sean reportado desde los equipos de red team.

Para las organizaciones públicos o privadas es de vital importancia saber cómo actuar frente a un incidente de seguridad ya sea si está ocurriendo activar el equipo CSIRT y posterior, saber que herramientas usar, el equipo de Blue team para fortalecer los controles, ambos son importantes para prevenir nuevos ataques y evitar que se repitan aprovechando las mismas vulnerabilidades para realizar la acción maliciosa.

Las medidas de hardenizacion en conjunto con el marco CIS para endurecer los controles proporcionados y en conjunto se cumple con los estándares ya desarrollados de manera internacional como NIST e ISO27000 entre otros, esto ayuda a fortalecer las medidas en las organizaciones y en minimizar los riesgos de sufrir un incidente.

Los equipos SIEM junto con las herramientas de contención ayudan a poner una capa adicional de seguridad, pero la importancia de los equipos SIEM en poder identificar por donde hay actividades sospechosas.

Conclusiones

Para las organizaciones públicos o privadas es de vital importancia saber cómo actuar frente a un incidente de seguridad ya sea si está ocurriendo y posterior, saber que herramientas usar y que equipos deben activarse, el equipo de blue team para fortalecer los controles y el equipo CSIRT posterior al ataque, ambos son importantes para prevenir nuevos ataques y evitar que se repitan aprovechando las mismas vulnerabilidades donde fue aprovechado para realizar la acción maliciosa.

Las medidas de hardenizacion en conjunto con el marco CIS para endurecer los controles proporcionados y en conjunto se cumple con los estándares ya desarrollados de manera internacional como NIST e ISO27000 entre otros, esto ayuda a fortalecer las medidas en las organizaciones y en minimizar los riesgos de sufrir un incidente.

Los equipos SIEM junto con las herramientas de contención ayudan a poner una capa adicional de seguridad, pero la importancia de los equipos SIEM en poder identificar por donde hay actividades sospechosas.

Referencias

Alcarria, P. (2023). Pasos para asegurar tus sistemas. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

Andreu, O. (2020). Rejetto HttpFileServer 2.3.x Remote Command Execution. https://packetstormsecurity.com/files/160264/Rejetto-HttpFileServer-2.3.x-Remote-Command-Execution.html

Araujo, A. (2024). 10 herramientas de Seguridad Informática y cómo usarlas. https://blog.hackmetrix.com/10-herramientas-de-seguridad-informatica-y-como-usarlas/#:~:text=Un%20firewall%20es%20un%20programa,atacantes%20accedan%20a%20su%20red.

Architecture. https://www.researchgate.net/profile/Mansoor-Ulhaq/publication/371173436_Effective_Security_Monitoring_Using_Efficient_SIEM_Architecture/links/650a623882f01628f032e51b/Effective-Security-Monitoring-Using-Efficient-SIEM-Architecture.pdf

Campusciberseguridad. (2024). Metasploit: La herramienta esencial en Ciberseguridad. https://www.campusciberseguridad.com/blog/item/180-metasploit-herramienta-esencial-ciberseguridad.

Chandel, R. (2017). Artículos de piratería. https://www.hackingarticles.in/post-exploitation-remote-windows-password/

Cilleruelo, C. (2024). ¿Qué es ExploitDB?. https://keepcoding.io/blog/que-es-exploitdb/

Cilleruelo, C. (2024). Fases de un pentest. https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/

Cilleruelo, C. (2024). Que es OpenVAS. https://keepcoding.io/blog/que-es-openvas/

De Luz, S. (2024). Configura pfSense para proteger tu hogar o empresa con este firewall. https://www.redeszone.net/tutoriales/seguridad/pfsense-firewall-profesional-configuracion/

Elhacker. (2021). Desactivar scripts PowerShell para evitar ataques de ransomware o malware. https://blog.elhacker.net/2020/12/deshabilitar-desactivar-scripts-powershell-traves-de-gpo-gpedit.html

Ferrer, A. (2021). Agrega un usuario al grupo de administradores local en Windows vía comando. https://www.mundodeportivo.com/urbantecno/windows/agrega-un-usuario-al-grupo-de-administradores-local-en-windows-via-comando

Gomez, J. (2024). Las 12 mejores herramientas de seguridad informática para empresas. https://www.deltaprotect.com/blog/herramientas-seguridad-informatica

Grupo Smartekh. (2012). Tips Tecnológicos, De Configuración Y Negocio Que Complementan Tu Seguridad. https://blog.smartekh.com/que-es-hardening

IBM. (2024). ¿Qué es la gestión de eventos e información de seguridad (SIEM)?. https://www.ibm.com/mx-es/topics/siem

Incibe. (2024). Vulnerabilidades. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades

Jotelulu. (2024). ¿Qué es Bitlocker y cómo puedes beneficiarte de él?. https://jotelulu.com/blog/que-es-bitlocker-y-como-puedes-beneficiarte-de-el/

Keepcoding (2024). ¿Cómo hacer un escaneo de red con Nmap?. https://keepcoding.io/blog/escaneo-de-red-con-nmap/

Kossakowski, K (2019). Computer Security Incident Response Team (CSIRT). https://reposit.haw-hamburg.de/handle/20.500.12738/4504

M, J. (2020). Eliminación de huellas tras una intrusión. https://jaymonsecurity.es/eliminacion-huellas-intrusion/

Manageengine. (2024). CSIRT – ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)? https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Mejia, R. (2008). Red team Versus Blue Team: How to Run an Effective Simulation. http://aldeilis.net/mumbai/0682.pdf

Mendivil, J. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. https://idus.us.es/handle/11441/145488

Mendoza, M. (2015). ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Microsoft. (2024). Autoruns v14.11. https://learn.microsoft.com/es-es/sysinternals/downloads/autoruns

Miltre (2024). CVE-2014-6287. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

Muhammad, S. (2023). Effective Security Monitoring Using Efficient SIEM

Nedigital. (2024). Herramientas comunes del Blue Team. https://www.nedigital.com/es/blog/hardening-de-servidores-windows

Ninjaone. (2024). Herramientas comunes del Blue Team. https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

NMAP. (2024). Guía de referencia de Nmap. https://nmap.org/man/es/index.html.

Policía. (2009). Ley 1273 [LEY_1273_2009].Policía. (pp. 1-4).https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Rejetto (2024). HFS ~ Servidor de archivos HTTP. https://www.rejetto.com/hfs/

Sampaio, D. (2017). Evaluation of Firewall Open Source Software. https://www.scitepress.org/PublishedPapers/2017/63612/pdf/index.html

Secureit. (2024). CSIRT – Equipo de respuesta ante incidentes de seguridad. https://www.secureit.es/csirt/

Sepulveda, M. (2023). Metasploit: Que es NMAP y como utilizarlo. https://ciberseguridad.club/que-es-nmap-y-como-utilizarlo/

Solvetic. (2024). Cómo deshabilitar línea de comandos CMD en Windows 10, 8, 7. https://blog.elhacker.net/2020/12/deshabilitar-desactivar-scripts-powershell-traves-de-gpo-gpedit.html

Tarlogic. (2023). 18 controles CIS críticos para una estrategia de ciberseguridad. https://www.tarlogic.com/es/blog/cis-controles-de-seguridad-criticos/

Zuluaga, M. (2017). Hacking Ético Basado En La Metodología Abierta De Testeo De Seguridad – Osstmm, Aplicado A La Rama Judicial, Seccional Armenia. https://repository.unad.edu.co/handle/10596/17410