Capacidades Técnicas, Legales y de Gestión para Equipos Red Team y Blue Team

Oscar Isidro Rodriguez Uyaban

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2024

_____

Nombre Director de Trabajo de Grado

_____ _____

Jurado Jurado

2024

Resumen

Los equipos Red Team y Blue Team desempeñan papel fundamental para el fortalecimiento de la ciberseguridad dentro de una organización, ya que al trabajar de forma complementaria permite realizar la identificación y mitigación de posibles riesgos este trabajo en conjunto da como resultado un fortalecimiento en la infraestructura de las organizaciones.

El equipo de Red Team tiene como objetivo realizar diferentes simulaciones de ataque que se puedan llegar a presentar en contra de una organización, para estas simulaciones el equipo Red Team utilizara técnicas y procedimientos que un actor malicioso podría usar. La ejecución de estos simulacros permite realizar la identificación de posibles fallos de seguridad, también permite evaluar la capacidad de respuesta que puede tener la organización si es víctima de un ataque de ciberseguridad.

Por otro lado, el equipo Blue Team se encarga de realizar monitoreos constantes, establecer controles y crear medidas de respuesta a incidentes, su enfoque está en fortalecer las medidas de protección implementadas en la organización y aplicar medidas correctivas generadas de las lecciones aprendidas.

Palabras clave**:** Ciberseguridad, Defensa Proactiva, Red Team, Blue Team, Vulnerabilidades, Gestión del Riesgo, Fortalecimiento de defensas, Monitoreo, Simulación de ataques.

Abstract

Red Team and Blue Team play a fundamental role in strengthening cybersecurity within an organization. By working collaboratively, they enable the identification and mitigation of potential risks. This joint effort results in a more robust organizational infrastructure.

The Red Team's objective is to conduct various attack simulations that an organization might face. These simulations involve using techniques and procedures that a malicious actor could employ. Carrying out such drills helps identify potential security flaws and also assesses the organization's response capabilities in the event of a cybersecurity attack.

On the other hand, the Blue Team is responsible for continuous monitoring, establishing controls, and creating incident response measures. Their focus is on reinforcing the protective measures implemented within the organization and applying corrective actions based on lessons learned.

Keywords**:** Cybersecurity, Proactive Defense, Red Team, Blue Team, Vulnerabilities, Risk Management, Defense Strengthening, Monitoring, Attack Simulation.

Tabla de contenido

Lista de Figuras

Glosario

Ciberseguridad: Se encarga de proteger los activos digitales de una organización en los que se incluyen hardware, software, datos almacenados y procesados dentro de la infraestructura de la organización.

Red Team: El equipo de Red Team tiene como principal función realizar ataques simulados mediante la utilización de estrategias, técnicas y métodos usados por ciberatacantes, este equipo realiza auditorias de seguridad dentro de las empresas por medio técnicas de hacking ético que permite hacer descubrimiento de las vulnerabilidades existentes

Blue Team: La función del equipo Blue Team es la de fomentar procesos de mejora dentro de la organización basándose en los informes generados por el Red Team, el Blue Team planea estrategias que permiten robustecer la seguridad informática dentro de las organizaciones.

Vulnerabilidades: Es una debilidad o un fallo presente en un sistema, hardware, aplicación, etc. Estas vulnerabilidades al ser explotada pueden lograr el compromiso de la integridad, confidencialidad o disponibilidad de los sistemas.

Gestión del Riesgo: Es el proceso de identificar, analizar y evaluar posibles riesgos que puedan afectar el correcto funcionamiento de los servicios dentro de una organización, el propósito de la gestión del riesgo es la de minimizar el impacto de los riesgos dentro de una organización.

Respuesta a incidentes: Es un conjunto de procedimientos establecidos desde el equipo Blue Team que permite tomar acciones coordinadas dentro de una organización cuando se presenta un incidente de seguridad.

Introducción

La ciberseguridad dentro de las organizaciones se ha convertido en uno de los pilares fundamentales cuando se habla de la protección de activos de información y entornos digitales. Dentro de este contexto, aparecen los equipos de Red Team y Blue Team los cuales son componentes estratégicos dentro de una organización ya que estos equipos se enfocan en anticipar posibles ataques, además de detectar y responder cuando se presenta un incidente de seguridad.

Este documento aborda el análisis detallado de las funciones y estrategias utilizadas por los equipos Red Team y Blue Team en el caso de estudio planteado durante el seminario, el cual plantea el robo de información mediante una vulnerabilidad identificada en una aplicación destinada para la transferencia de datos. Dentro de este documento se busca ilustrar la participación de ambos equipos y como actúa cada uno de estos equipos cuando se presenta un incidente de seguridad.

A lo largo de informe podremos ver la forma en la que el equipo Red Team mediante la utilización de técnicas ofensivas, simula y realiza la explotación de la vulnerabilidad identificada, una vez el equipo Red Team termine de realizar la documentación de la forma en la que ocurrió el incidente de seguridad, el equipo Blue Team participara realizando las recomendaciones necesarias, aplicando medidas correctivas y generando un informe de lecciones aprendidas frente al incidente de seguridad.

Justificación

En la actualidad las amenazas cibernéticas están teniendo un crecimiento en alcance, frecuencia y presencia en el mundo. Es por esto por lo que las organizaciones están enfrentadas a tener que pensar en nuevas formas de salvaguardar sus activos críticos y garantizar la continuidad del servicio. Es por esto por lo que las organizaciones han comprendido lo vital que es adoptar estrategias de seguridad que permitan garantizar el correcto funcionamiento de su infraestructura.

Es por esto por lo que en desarrollo de este documento se busca dar a conocer la importancia de un trabajo mancomunado entre el equipo Red Team y Blue Team dentro de una organización para lograr mejorar la ciberseguridad dentro de una infraestructura.

Objetivos

Objetivo General

Comprender las funciones del equipo Red Team y Blue Team dentro del caso de estudio relacionado al robo de información dentro de una organización, con el propósito de identificar la función de cada uno de los equipos y su impacto dentro de una organización.

Objetivos Específicos

Evaluar las técnicas utilizadas por el equipo Red Team dentro de la practica simulada, identificando la vulnerabilidad empleada, la forma de explotación utilizada y el alcance de la explotación de la vulnerabilidad.

Identificar las acciones y recomendaciones adoptadas por el equipo Blue Team como acciones de respuesta al incidente de seguridad identificado por el equipo Red Team todo esto enfocado en la contención y mitigación de futuros incidentes de seguridad.

Descripción del escenario.

En el escenario se plantea un incidente de seguridad relacionado con la fuga de información dentro de una organización, el presunto origen de este incidente es atribuido a un servidor cuyo sistema operativo es Windows y cuenta con una aplicación para la transferencia de archivos.

Se hace entrega al equipo de Red Team una copia del servidor desde donde se originó la falla de seguridad con el propósito de indagar cual fue la vulnerabilidad usada en el robo de información. Al momento de la entrega de la copia del servidor se solicita al equipo de Red Team la documentación de la explotación de la vulnerabilidad encontrada, además de esto se solicita realizar el escalamiento de privilegios para comprobar el alcance del ataque inicial y de qué forma podría afectar la organización.

Acciones del equipo Red Team

Normatividad

Debemos tener en cuenta que cualquier acción tomada por un equipo Red Team dentro de una organización está regida por normatividad asociada a la protección de datos y delitos informáticos esto permite garantizar la confidencialidad de la información obtenida dentro de las actividades pertinentes de un Red Team, es por esto por lo que se debe garantizar un contrato de confidencialidad entre las partes interesadas.

En Colombia se aplican leyes de protección de datos y confidencialidad de la información para garantizar este cumplimiento se deberá aplicar las siguientes leyes establecidas dentro de las normas vigentes relacionadas a protección de datos y delitos informáticos.

Ley 1273 de 2009: se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”

Artículo 269A: Hace referencia al acceso abusivo a un sistema informático, por ejemplo, cuando se accede sin autorización o cuando se exceden los límites establecidos inicialmente, este articulo también aplica para la permanencia dentro de un sistema por agentes externos a la organización que no cuenten con autorización previa.

Artículo 269B: Aplica cuando se obstaculiza de forma predeterminada un sistema informático o de telecomunicaciones sin contar con la autorización de propietario del sistema.

Artículo 269C: El que, sin orden judicial o autorización expresa del administrador del sistema intercepte datos informáticos.

Artículo 269E: El que sin estar facultado haga uso de software malicioso dentro de un sistema sin autorización previa.

Ejecución de actividades del equipo Red Team.

El trabajo del equipo Red Team consiste en realizar la simulación de ataques informáticos utilizando las mismas técnicas que un atacante común utilizaría para vulnerar una infraestructura, a este proceso de búsqueda y explotación de vulnerabilidades se le conoce como pentesting. Para la realización de proceso de pentesting se debe tomar en cuenta los siguientes pasos:

Planeación y recolección de información: Se establece la metodología que usaremos, se establecen los objetivos, el alcance, el enfoque y las restricciones a las cuales estamos sujetos dentro de la ejecución del pentesting.

La recolección de la información permite comprender la infraestructura a la cual estamos realizando el pentesting y cuáles son los servicios y servidores que será excluidos de las pruebas.

Identificación de vulnerabilidades: en esta fase se inicia el trabajo dentro de la red se la organización, se utiliza un pool de herramientas que permitan recolectar información de la infraestructura que será usada posteriormente para la explotación de vulnerabilidades.

Verificación de vulnerabilidades: Una vez recolectada la información se inicia el proceso de análisis de las vulnerabilidades encontrada, de esta forma se descartan los falsos positivos y además se mide el impacto de las vulnerabilidades encontradas.

Realización del informe: Se realizará un documento técnico donde se especifique detalladamente cada proceso del pentesting, cada vulnerabilidad encontrada y la forma en la que fue hallada, a su vez se explicara la forma en la que dicha vulnerabilidad afecta el sistema y cuál podría ser la forma de corregir dicha falla de seguridad. (ciberseguridad, s.f.)

Ejecución del Pentesting al escenario planteado

Fase de Enumeración de puertos y servicios:

Mediante la herramienta nmap se ejecuta el siguiente comando "**namp -p- -sCV -script vuln 192.168.1.82**" realizamos el scaneo de todos los puertos y además identificamos las posibles vulnerabilidades existentes en los puertos que identifique.

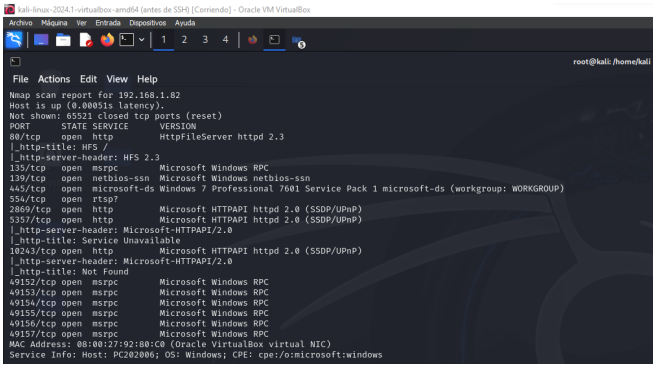

Ilustración 1-Puertos

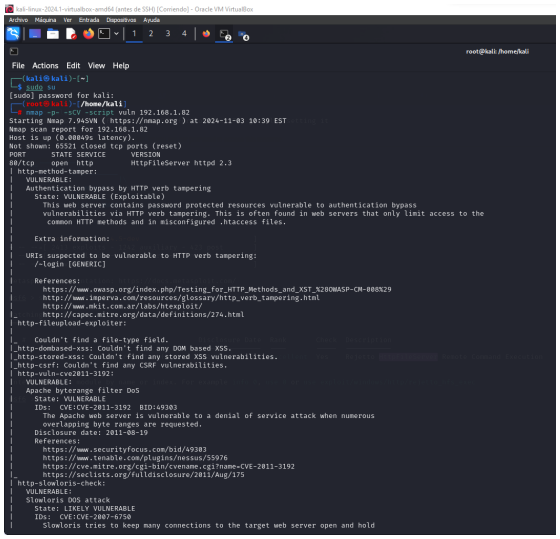

Ilustración 2-Servicios

Podemos identificar que el puerto 80 es vulnerable mediante el puerto 80/tcp servicio http versión HttpFileServer httpd 2.3

Al ser una aplicación web lo que está corriendo en el puerto 80 podemos abrirla en un explorador para poder observar algunas características como por ejemplo la versión y comprobar la información encontrada con nmap.

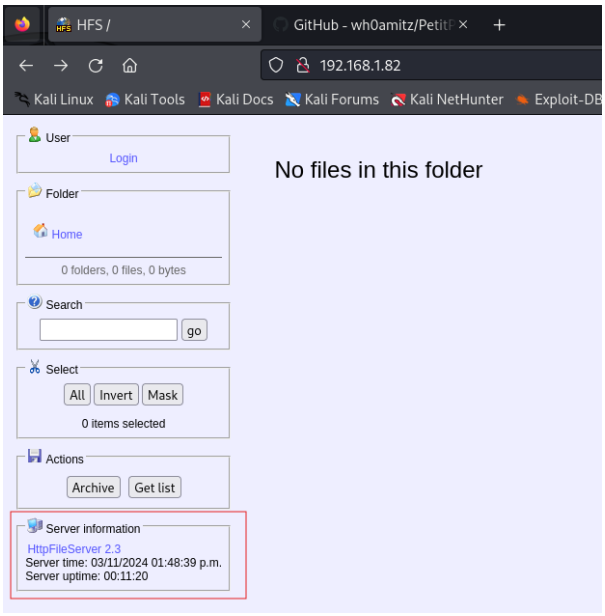

Ilustración 3-Aplicación

Evidenciamos la que la aplicación que corre en el puerto 80 es HttpFileServer 2.3 al igual que el que se muestra en el scaneo con nmap.

Fase de Explotación:

Ahora vamos a usar la herramienta metasploit para buscar algún exploit que podamos usar para explotar la vulnerabilidad asociada a la aplicación HttpFileServer 2.3. Para esto usamos los siguientes comandos "**search HttpFileServer 2.3**" esto nos arroja un resultado.

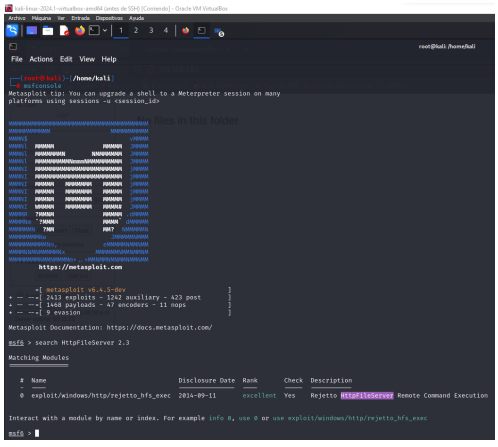

Ilustración 4-Metaexploit1

Seleccionamos el exploit con el comando "**use exploit/windows/http/rejetto_hfs_exec**"

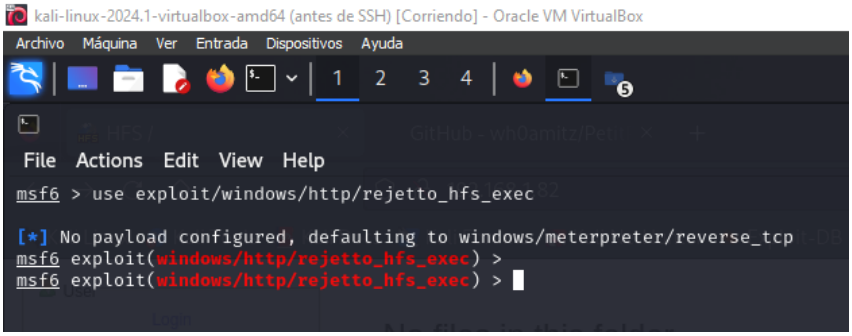

Ilustración 5-Exploit

Ahora usamos el comando “show options” para ver los requerimientos del exploit

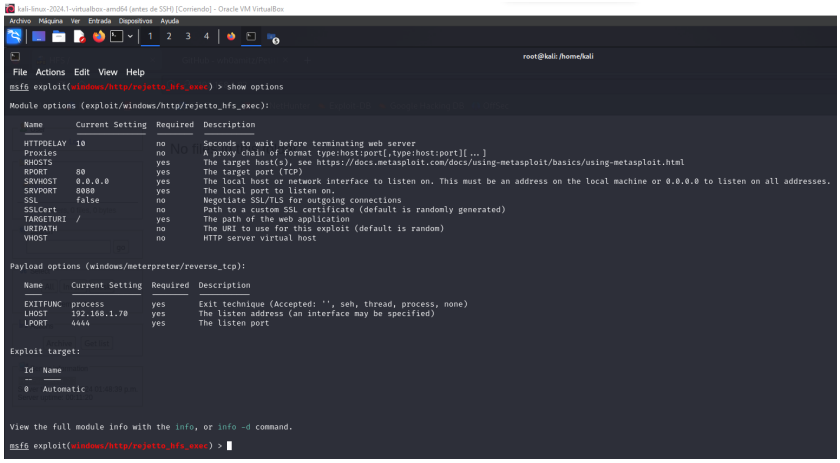

Ilustración 6-ShowOptionsExploit

Ahora vamos asignar los valores que están marcados como requeridos, debemos verificar que la información ya asignada es la correcta. Para ingresar información a la variable RHOSTS usaremos el comando “**set RHOSTS 192.168.1.82**”.

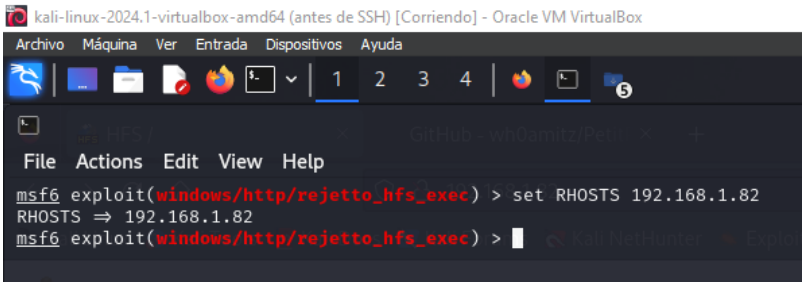

Ilustración 7-SetOptions

Volvemos a comprobar con el comando “**show options**”

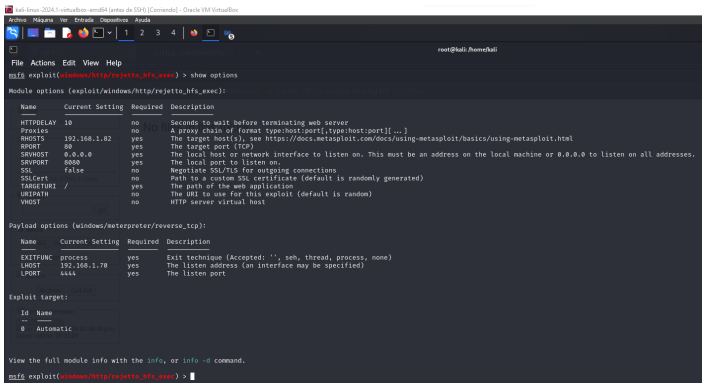

Ilustración 8-ShowOptions2

Ahora iniciamos la ejecución del exploit con el comando "**exploit**"

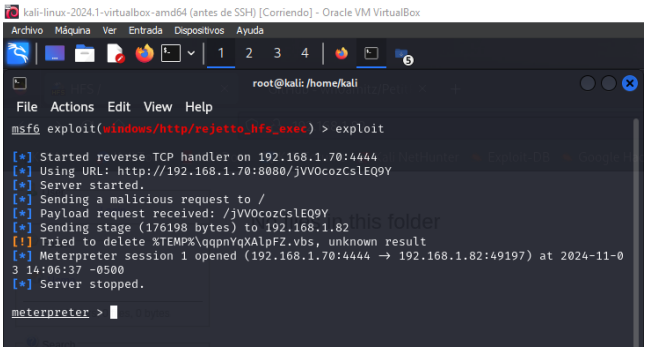

Ilustración 9-RunExploit

Podemos ver que el exploit creo una sesión meterpreter desde donde podemos observar diferentes características del sistema atacado usando los siguientes comandos:

"Sysinfo", "pwd", "ifconfig".

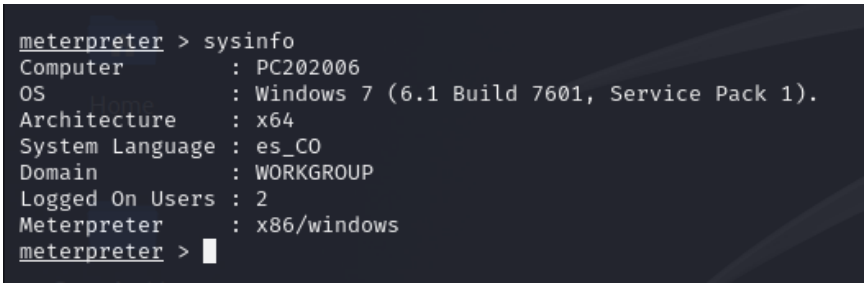

Ilustración 10-Meterpreter

Acá podemos ver el directorio en el que nos encontramos y la dirección ip de la maquina a la cual estamos conectados.

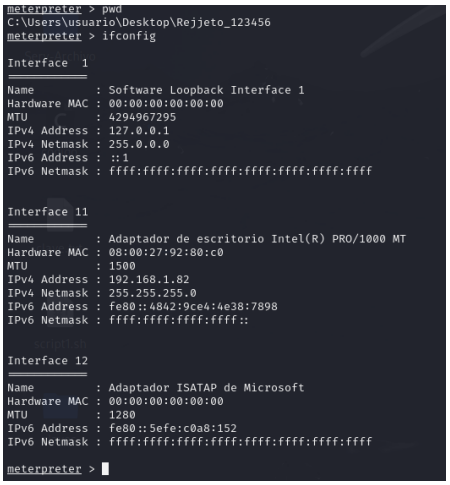

Ilustración 11-InfoMeterpreter

Fase de pos-explotación:

Ahora que ya tenemos acceso a la maquina vulnerable debemos identificar que privilegios tenemos en el usuario con el que estamos accediendo en este momento, esto lo hacemos con el “getuid”.

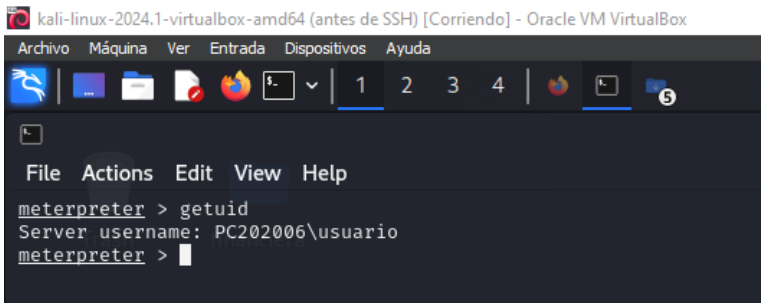

Ilustración 12InfoRhosts1

Podemos ver que solo tenemos acceso de usuario sin privilegios, por lo que vamos a realizar un escalado de privilegios de forma vertical, para esto usaremos el comando “**getsystem**”

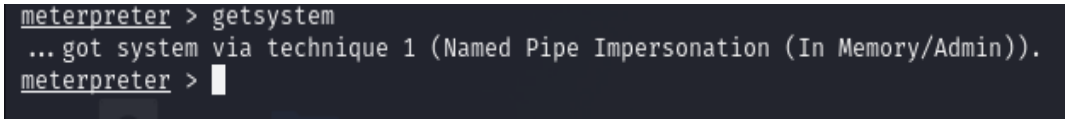

Ilustración 13-EscaladoPrivilegios

Ahora volvemos a ver que privilegios tenemos con el comando “**getuid**”

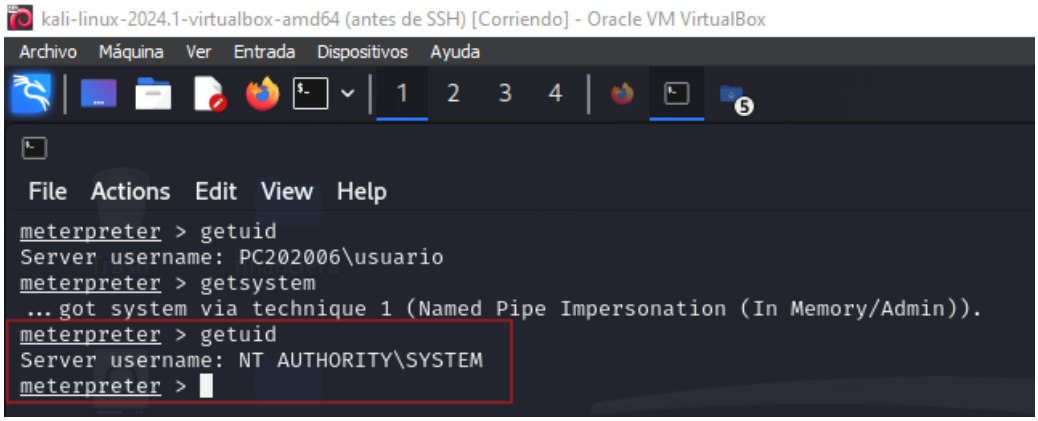

Ilustración 14-PerfilUsuario

Ahora vamos a usar el comando "**getprivs**"

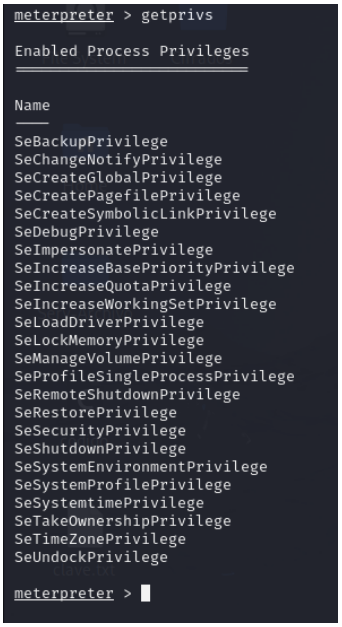

Ilustración 15-DescripcionPrivilegios

En este momento ya tenemos acceso como usuario administrador al equipo víctima, para poder generar un ataque persistente vamos a crear una cuenta de usuario, para esto necesitamos ejecutar una Shell de Windows en nuestra sesión meterpreter, para esto usamos el comando "**Shell**"

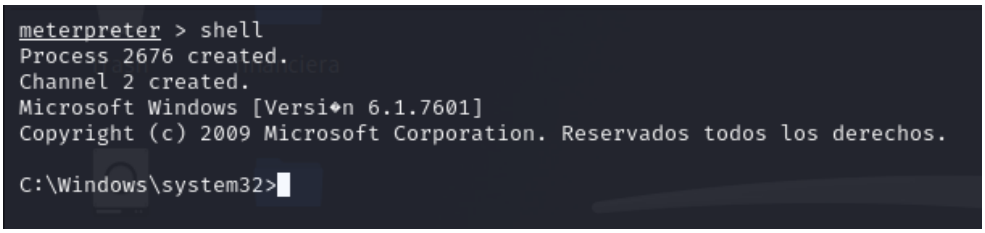

Ilustración 16-Shell

Ahora vamos a ver los usuarios existentes en la maquina víctima, para esto usamos el comando "**query user**" y "**net user usuario**"

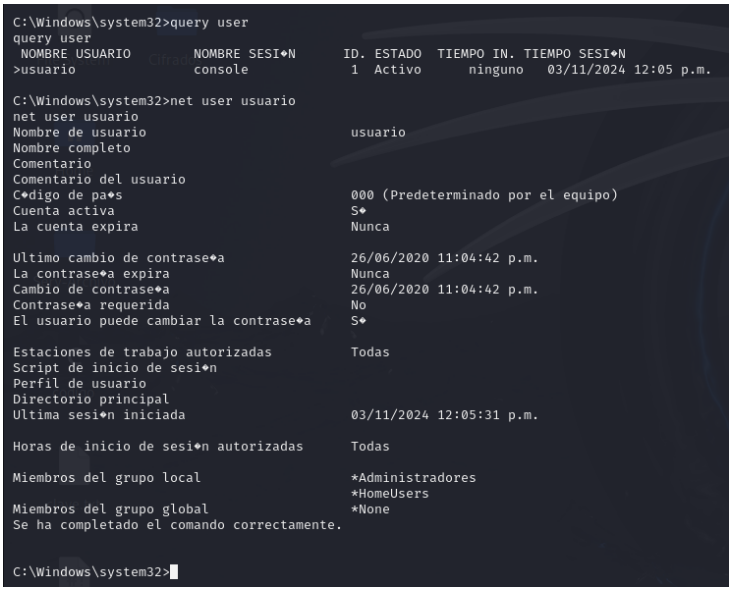

Ilustración 17-Usuarios Rhosts

Ahora desde la sesión Shell que tenemos conectada desde Kali vamos a crear la una cuenta nueva con permisos de administrador, para esto vamos a utilizar el siguiente comando "net user OscarRodriguez 123456 /add"

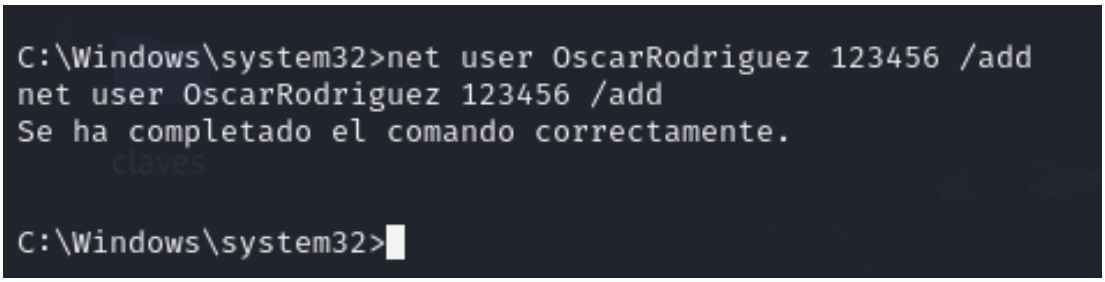

Ilustración 18-CreaciónDeUsuario

Ahora vamos a volver usuario administrador al usuario OscarRodriguez para esto vamos a usar el comando “net localgroup Administradores OscarRodriguez /add”

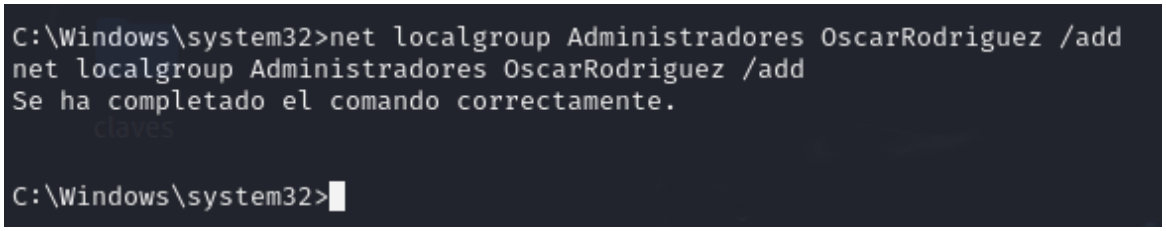

Ilustración 19-GrupoAdmnistradores

Ahora vamos a comprobar los usuarios existentes en la maquina víctima.

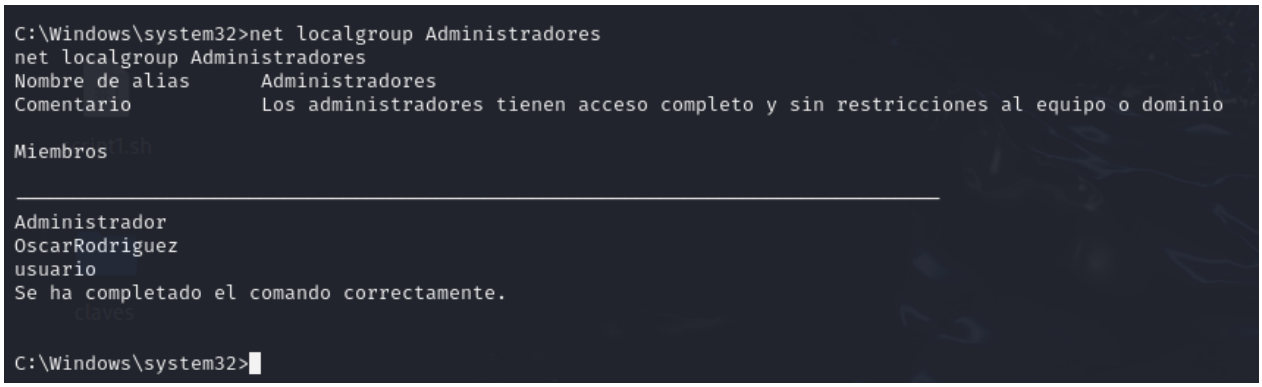

Ilustración 20-UsuarioCreado

Podemos observar que se creó un usuario llamado OscarRodriguez que pertenece al grupo de administradores locales de la máquina y por lo tanto tiene todos los privilegios.

Ahora vamos a ver directamente en la maquina Windows 7 los usuarios para comprobar que el usuario este creado.

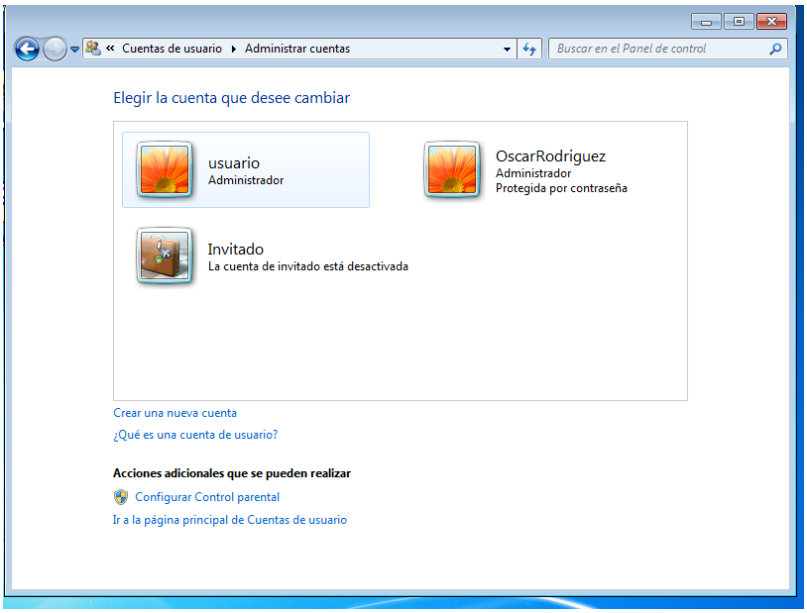

Ilustración 21-UsuarioAdministrador

Podemos observar que hemos creado un usuario llamado OscarRodriguez con un perfil de administrador.

Aportes para el correcto desarrollo de las actividades del equipo Red Team.

Es fundamental el diseño y la implementación de estrategias apropiadas para lograr un enfoque más efectivo a la hora de seleccionar la tácticas, técnicas y procedimientos adecuados para la identificación y explotación de vulnerabilidades dentro de una organización es por esto por lo que se debe tener en cuenta los siguientes aspectos para lograr un desarrollo eficaz en las actividades requeridas en un Red Team.

Cumplimiento normativo: Es de vital importancia tener en cuenta toda la normatividad vigente antes de iniciar procedimientos de identificación y explotación de vulnerabilidades dentro de una organización ya que es factible que, durante estas ejecuciones, el equipo Red Team acceda a información sensible de la organización.

Registro detallado de los procedimientos: Realizar un registro detallado de todo el proceso de descubrimiento de vulnerabilidades al igual que un informe detallado de recomendaciones permitirá a la organización ajustar sus controles y procedimientos de seguridad.

Reconocimiento de las amenazas y la forma en la que se pueden presentar: Un Red Team actualizado en los últimos reportes de ataques informáticos permite anticipar y mitigar acciones maliciosas en una organización, ya que facilita la toma de medidas correctivas enfocadas en el mejoramiento de la seguridad. Esto permite realizar búsquedas de vulnerabilidades asociadas a las amenazas vigentes.

Análisis de casos reales: Investigar casos reales permitirá anticipar un ataque de ciberseguridad ya que facilita la identificación de vulnerabilidades existentes en un sistema.

Acciones del equipo Blue Team

Este equipo está enfocado en defensa proactiva, el objetivo principal es mejorar la infraestructura de ciberseguridad, realizar la identificación de vulnerabilidades de forma activa. La responsabilidad del BlueTeam está centrada en el monitoreo continuo, realizar hardenización de la infraestructura, realizar simulación de ataques informáticos, realización de evaluaciones de riesgos y realizar análisis de seguridad de forma preventiva.

Ejecución de actividades del equipo Blue Team.

Al realizar un análisis del activo comprometido y el ataque realizado mediante el cual pudieron sustraer información podemos dar las siguientes recomendaciones para remediar y prevenir nuevos incidentes de seguridad.

Se identifico que la aplicación usada para transferencia de archivos contaba con una vulnerabilidad. Por lo que se recomienda hacer el cambio de la aplicación HFS por un servidor de archivos más robusto por ejemplo Apache o en su defecto utilizar una versión más actual de HFS.

El sistema operativo del servidor que aloja la aplicación de transferencia de archivos es Windows 7 el cual esta desactualizado y además cuenta con varias vulnerabilidades por lo que se recomienda hacer la migración a un sistema operativo basado en Windows server o migrar a una versión de Windows profesional actual.

Implementación de políticas de seguridad basada en roles de mínimo acceso, lo cual permite que solo los usuarios con privilegios puedan ejecutar y acceder a la información dentro de la infraestructura de la organización.

Aportes para el correcto desarrollo de las actividades del equipo Blue Team.

Monitoreo continuo: Implementación de soluciones de monitoreo que facilite la supervisión en tiempo real de la infraestructura de la organización, el uso de herramientas como SIEM mejora y facilita la identificación de patrones de comportamiento considerados como anómalos y que pueden ser parte de un posible incidente de seguridad.

Desarrollo del plan de respuesta a incidentes: Diseñar y documentar planes de acción que permitan la identificación, contención, mitigación y recuperación de un incidente de seguridad, garantiza una mejor gestión y atención de los incidentes de seguridad que se puedan presentar.

Capacitación y concienciación: Mantener a todos los actores de la organización actualizados en temas de ciberseguridad mediante capacitaciones permite minimizar los factores

de riesgos asociados a temas de ataques de ingeniería social y otros ataques dirigidos a una organización.

Gestión de vulnerabilidades: Implementación de políticas enfocadas en la ejecución de análisis de vulnerabilidades dentro de la infraestructura de la organización permite identificar de forma anticipada posibles vulnerabilidades existentes lo que permite crear planes de remediación eficaces.

Fortalecimiento de controles de seguridad: El análisis de vulnerabilidades permite a la organización identificar las posibles brechas de seguridad existentes, por lo que se puede hacer un mejor enfoque en la implementación de políticas de seguridad que ayuden a generar un fortalecimiento en los controles de seguridad dentro de la organización.

Evaluación de políticas de seguridad: La evaluación a las políticas de seguridad permite conocer el grado de efectividad de las acciones preventivas que están implementadas actualmente lo cual culmina en acciones de mejora contante para la seguridad de la organización.

Conclusiones

El análisis del caso de estudio nos permitió comprender como el trabajo entre los dos equipos Red Team y Blue Team fortalece el campo de la ciberseguridad dentro de la organización. El equipo Red Team, mediante la simulación de ataques reales permite identificar las vulnerabilidades criticas dentro de la organización, lo que permite anticipar posibles explotaciones de las vulnerabilidades presentes, mientras que el equipo Blue Team, mediante sus acciones de respuesta, logra implementar acciones de mitigación del impacto de posibles incidentes de seguridad.

Las técnicas usadas por el equipo Red Team permiten hacer simulaciones de ataques reales por parte de un actor malicioso, lo que permite evidenciar las falencias existentes dentro

de una organización, para el caso de estudio se evidencio la presencia de una aplicación vulnerable la cual fue explotada y de esta forma pudo se comprometer datos sensibles de la organización y su infraestructura.

Por otro lado, las recomendaciones realizadas por el equipo Blue Team, como la actualización de la aplicación de transferencia de archivos, la actualización del sistema operativo del servidor y la implementación de políticas de acceso permiten crear acciones de mejora de la seguridad informática dentro de la organización.

Es por esto que el trabajo en conjunto de los dos equipos permite la identificación de fallos y la optimización de estrategias enfocadas en tener una seguridad proactiva y adaptable a las necesidades que se presenten dentro de la organización.

Recomendaciones

Fortalecimiento del enfoque colaborativo entre el equipo Red Team y Blue Team mediante la ejecución de simulaciones que permitan mejorar la comunicación y la articulación de actividades que mejoren la capacidad de prevención y reacción frente a posibles ataques de seguridad de la información.

Actualización y seguimiento a los controles de seguridad, se deberán programar auditorias y simulaciones de efectividad a los controles establecidos dentro de la organización con el fin de poder identificar la efectividad y el cumplimiento de los controles de seguridad para cada uno de los procesos.

Mantener actualizados los equipos de Red Team y Blue Team en temas relacionados con ciberseguridad es crucial para comprender los diferentes riesgos que están presentes en el mundo, es de recordar que todos los días son encontradas nuevas vulnerabilidades en servicios y

aplicaciones que posiblemente usamos en nuestras organizaciones. Por lo tanto, tener equipos de seguridad informados y actualizados brinda una mejor capacidad de reacción y mitigación antes incidentes de seguridad.

Finalmente es de recalcar la importancia de documentar las lecciones aprendidas, estas son generadas después de cada simulación o incidente de seguridad que se presenta, de esta forma se crea un conocimiento que permite facilitar la mejora continua de los procesos de seguridad.

Referencias Bibliográficas

Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades (Vol. 46). 3Ciencias.

Candel, J. M. O. (2024). Ciberseguridad: manual práctico. Ecoe Ediciones.

Chinchilla, E. J. S., & Allende, J. S. (2017). Riesgos de ciberseguridad en las empresas. Tecnología y desarrollo, 15.

Ciberseguridad.com. (s.f.). Pruebas de penetración. Recuperado de https://ciberseguridad.com/herramientas/pruebas-penetracion/#Planificacion_y_preparacion.

Cisco. (s.f.). ¿Qué es la ciberseguridad? Recuperado de https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~how-cybersecurity-works

Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics. Packt Publishing Ltd.

Ley 1273 de 2009, por la cual se modifica el Código Penal y se establecen otras disposiciones en materia de delitos informáticos. Diario Oficial No. 47.467 del 5 de enero de 2009. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Llerena, A. E. R. (2020). Herramientas fundamentales para el hacking ético. Revista Cubana de Informática Médica, 12(1), 116-131.

Núñez Alcalá, C. (2021). Penetration testing: auditoría profesional.

Santo Orcero, D., & Santo Orcero, D. (2017). Pentesting Con Kali. BLURB Incorporated.

Vanegas Romero, A. Y. (2019). Pentesting, ¿Por qué es importante para las empresas?.

Vilà del Moral, P. (2024). Metodologia de pentesting (Bachelor's thesis, Universitat Politècnica de Catalunya).

Yoo, J. D., Park, E., Lee, G., Ahn, M. K., Kim, D., Seo, S., & Kim, H. K. (2020). Cyber attack and defense emulation agents. Applied Sciences, 10(6), 2140.

Zambrano Hernández, L. F. Capacidades técnicas, legales y de gestión para equipos blue team y red team.

Zambrano, S. M. Q., & Valencia, D. G. M. (2017). Seguridad en informática: consideraciones. Dominio de las Ciencias, 3(3), 676-688.

Anexos

https://youtu.be/FdIlq7qA-k8