CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

RONAL ALEXIS MARTINEZ CERON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

RONAL ALEXIS MARTINEZ CERON

GRUPO: 2

DIRECTOR DE CURSO
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

CONTENIDO

Pág.

LISTA DE FIGURA

Pág.

GLOSARIO

Amenaza persistente avanzada (APT): es un ataque cibernético sofisticado y sostenido dirigido a una organización específica con el objetivo de infiltrarse y recopilar información valiosa durante un largo período de tiempo.

Ataque de phishing: es una técnica de ingeniería social en la que los ciberdelincuentes envían mensajes fraudulentos a través de correo electrónico, redes sociales u otros medios para engañar a las personas y obtener información confidencial como contraseñas y datos bancarios.

Autenticación: es el proceso de verificar la identidad de un usuario para permitir el acceso a un sistema o red informática. Los métodos comunes de autenticación incluyen contraseñas, tokens de seguridad y huellas dactilares.

Ciberseguridad: es el conjunto de técnicas, herramientas y políticas de seguridad informática diseñadas para proteger los sistemas, redes y datos contra ataques malintencionados.

Cifrado: es la técnica de codificar datos para protegerlos contra accesos no autorizados. El cifrado se utiliza para proteger la privacidad de los datos y evitar que sean interceptados o modificados por terceros.

Denegación de servicio (DoS): es un ataque cibernético en el que se sobrecarga un servidor o red con tráfico malicioso para evitar que los usuarios legítimos accedan al servicio. Los ataques de denegación de servicio pueden ser muy dañinos para los negocios y las organizaciones.

Firewall: es un software o hardware que se utiliza para bloquear el acceso no autorizado a un sistema o red informática. El firewall actúa como una barrera de seguridad entre la red interna y los usuarios externos.

Ingeniería inversa: es el proceso de desmontar y analizar un software para comprender su funcionamiento interno. La ingeniería inversa se utiliza comúnmente para descubrir vulnerabilidades de seguridad en aplicaciones y sistemas.

Malware: es un software malicioso que se utiliza para dañar o infiltrarse en los sistemas informáticos. Los tipos comunes de malware incluyen virus, troyanos, gusanos y spyware.

RESUMEN

Este trabajo ha recopilado información de diferentes fuentes relacionadas con la ciberseguridad y el mejoramiento continuo de los procesos organizacionales. En primer lugar, se abordó el tema de los ciberataques y los tipos más comunes, como el phishing y el malware, así como las medidas preventivas que pueden tomarse para evitarlos. También se destacó la importancia de mantener actualizados los sistemas de seguridad y realizar pruebas de penetración para detectar posibles vulnerabilidades.

Posteriormente, se hizo énfasis en la necesidad de implementar una cultura de mejora continua en las empresas, y la importancia de aprender de los errores, tanto propios como ajenos. Asimismo, se destacó la importancia de actualizar los equipos, implementar políticas de seguridad y realizar capacitaciones para el personal, como medidas para fortalecer la seguridad informática de la organización.

Por último, se mencionó la importancia de monitorear constantemente el cumplimiento de las políticas de seguridad y realizar auditorías regulares a las diferentes áreas de la empresa, como una forma de garantizar el correcto funcionamiento de los controles de seguridad implementados. En resumen, la ciberseguridad y el mejoramiento continuo son elementos fundamentales para garantizar la protección de los datos y la información de las empresas, y es necesario implementar medidas preventivas y de control para minimizar los riesgos de los ciberataques.

INTRODUCCION

En la actualidad, los sistemas informáticos son fundamentales para el avance de las actividades humanas, organizacionales y sociales. Sin embargo, esto también implica riesgos y posibles ataques cibernéticos que pueden poner en peligro la seguridad y operación de una organización. Es por esto por lo que los equipos Red Team y Blue Team se han vuelto tan importantes, ya que su objetivo es brindar seguridad a través de la realización de pruebas que simulan ataques y defensas de la organización.

Estas pruebas permiten detectar vulnerabilidades y cerrar brechas de seguridad, mitigando así las posibles consecuencias de un ataque cibernético. Además, es importante que se cuenten con los controles necesarios para reducir al mínimo la posibilidad de explotación de vulnerabilidades y, en caso de ser necesario, contar con herramientas que permitan la realización de pruebas, análisis y contención de incidentes informáticos básicos.

En este sentido, el presente trabajo no se enfoca en la realización de pruebas de penetración o ataques simulados, sino que aborda temas relacionados con la protección de los recursos informáticos desde una perspectiva legal, operativa y técnica.

1 OBJETIVO GENERAL:

presentar una recopilación de las actividades relevantes y su análisis con el fin de formular recomendaciones y conclusiones que permitan mejorar la seguridad de una organización.

1.1 OBJETIVOS ESPECÍFICOS:

- Realizar un resumen completo de las actividades realizadas y destacar los aspectos más importantes relacionados con la seguridad informática.
- Identificar los factores críticos que pueden influir en el éxito de las estrategias de seguridad de Red Team y Blue Team.
- Elaborar estrategias de contención de riesgos y vulnerabilidades, mediante un análisis exhaustivo de los mismos.
- Proponer recomendaciones concretas y efectivas para mejorar los aspectos de seguridad de la organización.

2 NORMATIVIDAD ASOCIADA AL CASO DE ESTUDIO

2.1 LEYES QUE APLICABLES EN COLOMBIA

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación leyes, decretos existen actualmente y las características principales de cada ley.

El 5 de enero de 2009, el Congreso de la República de Colombia expidió la Ley 1273, que entre otras cosas modifica el Código Penal, crea un nuevo bien jurídico protegido denominado De la Protección de la Información y los Datos, y preserva integralmente los sistemas que utilizan tecnologías de la información y la comunicación.

Es crucial que las empresas se protejan legalmente para evitar incurrir en cualquiera de los actos delictivos que fueron ilegalizados por el estatuto antes mencionado en relación con el procesamiento de datos personales.

No debemos perder de vista que los avances tecnológicos se están utilizando cada vez con más frecuencia en todo el mundo para obtener de manera fraudulenta activos de otras personas a través de la clonación de tarjetas bancarias, el acceso no autorizado y la modificación de sistemas informáticos con el fin de recibir servicios, y transferencias electrónicas de fondos fraudulentas a través de la manipulación de software y afectaciones de cajeros automáticos, entre otros métodos. Según la Revista Cara y Sello, los delitos informáticos costaron a las empresas colombianas más de 6.600 millones de pesos solo en 2007.

En esta Ley se tipifican las siguientes infracciones de índole informático:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.

- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269I: Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos.

Si la persona que incurre en estas conductas tuviere a su cargo la administración, manejo o control de dicha información, además de la pena de prisión y/o multa por cantidad significativa de dinero, además de la pena de inhabilitación ejercer una profesión relacionada con los sistemas de información procesados con equipos de cómputo se impondrá hasta por tres años.

Es evidente que los delitos informáticos constituyen una práctica que no sólo pone en riesgo la seguridad de los usuarios sino que también representa una amenaza para la economía de una nación. Muchos autores sostienen que este es un tema de cultura general, y como tal, toda persona tiene la responsabilidad de establecer mecanismos de protección informática al momento de utilizar su información personal en medios digitales.

3 ETAPAS DEL PENTESTING

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como 2 pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Pentesting es un ataque cibernético simulado contra su sistema informático para verificar vulnerabilidades explotables. En el contexto de la seguridad de las aplicaciones web, las pruebas de penetración se usan comúnmente para aumentar un firewall de aplicaciones web (WAF).

Las pruebas de penetración pueden implicar el intento de violación de cualquier número de sistemas de aplicaciones (por ejemplo, interfaces de protocolo de aplicaciones (API), servidores front-end/back-end) para descubrir vulnerabilidades, como entradas no desinfectadas que son susceptibles a ataques de inyección de código.

La información proporcionada por la prueba de penetración se puede utilizar para ajustar sus políticas de seguridad WAF y parchear las vulnerabilidades detectadas.

3.1 ETAPAS:

3.1.1 Reconocimiento:

Es la fase principal, durante la cual recopilamos la mayor cantidad de datos posible utilizando varios métodos, que incluyen:

- Recopilación de dominios/IPs/puertos/servicios
- Recopilación de metadatos

- Uso de Google Dorks
- Recopilación de información gracias a servicios de terceros

Ejemplo:
FOCA: El objetivo principal de este programa, según FOCA, es descubrir datos y metadatos ocultos en los documentos que está viendo. Estos registros se pueden encontrar en las páginas web. Los documentos que se pueden estudiar varían mucho; los más populares son archivos de Microsoft Office, Open Office o PDF, aunque también puede analizar otros tipos de archivos, como Adobe InDesign o svg. Se utilizaron tres motores de búsqueda diferentes, incluidos Google, Bing y DuckDuckGo, para encontrar estos documentos.

3.1.2 Análisis de vulnerabilidades**:**

En esta etapa, examinaremos los datos recopilados en la etapa anterior y las vulnerabilidades encontradas.
Ejemplo: Hay varias tecnologías disponibles, como escáneres de vulnerabilidades de red y escáneres de vulnerabilidades web. La herramienta NMAP mencionada anteriormente se destaca entre los escáneres de puertos de los escáneres de vulnerabilidades de red. Tenga en cuenta que si bien esta herramienta nos permite ver qué puertos o servicios son accesibles en una red, un pentest también debe realizar análisis utilizando otras herramientas para identificar vulnerabilidades en general. Otros escáneres incluyen Nessus, OpenVas y Nexpose, el último de los cuales, por ejemplo, busca vulnerabilidades en las bases de datos.
3- Explotación: La fase de explotación implica realizar todas las tareas que podrían poner en peligro el sistema auditado, los usuarios o los datos que controla. Principalmente verifica que ciertos tipos de ataques no se puedan ejecutar:

- Inyección de código
- Inclusión de ficheros locales o remotos
- Evasión de autenticación
- Carencia de controles de autorización
- Ejecución de comandos en el lado del servidor
- Ataques tipo Cross Site Request Forgery
- Control de errores
- Gestión de sesiones
- Fugas de información
- Secuestros de sesión
- Comprobación de las condiciones para realizar una denegación de servicio
- Carga de ficheros maliciosos
-

Ejemplo: METASPLOIT es una herramienta de prueba de penetración que permite identificar, usar y validar vulnerabilidades. Metasploit Framework y sus equivalentes con fines de lucro, incluido Metasploit Pro, están incluidos en la plataforma.

3.1.3 Post explotación:

Se realizarán procedimientos adicionales para confirmar la criticidad de la vulnerabilidad si se descubre una vulnerabilidad que permita realizar otras operaciones en el sistema auditado o en su entorno.
Se intentarán las siguientes actividades posteriores a la explotación, dependiendo de las opciones que permita una vulnerabilidad específica:

- Obtención de información confidencial
- Evasión de mecanismos de autenticación
- Realizar acciones del lado de los usuarios

- Realizar acciones o ejecutar comandos en el servidor que aloja la aplicación
- Privilegios disponibles en el servidor, si se consigue acceso al mismo
- Otros sistemas o servicios accesibles desde la aplicación comprometida
- Posibilidad de impersonalización del usuario
- Realizar acciones sin el consentimiento o conocimiento de los usuarios

Al realizar el análisis de riesgo, también se tendrán en cuenta escenarios que incluyan la combinación de varias vulnerabilidades para obtener acceso a un nivel superior o eludir las medidas de seguridad.

5 Informes: El paso final de una prueba de penetración siempre es crear un resumen informativo, que es un informe sobre cómo fue la prueba. Este documento enumerará todas las vulnerabilidades descubiertas, así como las exposiciones que los atacantes podrían aprovechar.

Además, un documento debe contener una recopilación de todos los resultados de las pruebas. Podríamos pensar en ello como una muestra de los datos que habría recopilado un atacante.

Finalmente, si se acordó previamente, debe existir un documento que detalle las contramedidas para aliviar (o minimizar) estos problemas tanto como sea posible.

4 HERRAMIENTAS DE CIBERSEGURIDAD

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:
Herramientas:

4.1 METASPLOIT:

es un marco de prueba de penetración que simplifica la piratería. Es una herramienta esencial para muchos atacantes y defensores. Es un marco completo. Es una plataforma de prueba de penetración modular basada en Ruby que le permite escribir, probar y ejecutar código de explotación, es flexible y extremadamente robusta y tiene toneladas de herramientas para realizar varias tareas simples y complejas.
Metasploit tiene tres ediciones disponibles:

- Metasploit Pro
- Comunidad Metasploit
- Marco Metasploit

Nmap: Nmap es la abreviatura de Network Mapper. Es una herramienta de línea de comandos de Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.
Nmap permite a los administradores de red encontrar qué dispositivos se están ejecutando en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades.
Gordon Lyon (seudónimo Fyodor) escribió Nmap como una herramienta para ayudar a mapear una red completa fácilmente y encontrar sus puertos y servicios abiertos.

Nmap se ha vuelto muy popular y aparece en películas como The Matrix y la popular serie Mr. Robot.

• OpenVas: Es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad.

El escáner obtiene las pruebas para detectar vulnerabilidades de un feed que tiene un largo historial y actualizaciones diarias.

5 SERVICIOS EN LÍNEA

• ExploitDB: Exploit Database (ExploitDB) es un archivo de exploits con fines de seguridad pública y explica lo que se puede encontrar en la base de datos.

ExploitDB es un recurso muy útil para identificar posibles debilidades en su red y para mantenerse actualizado sobre los ataques actuales que ocurren en otras redes. Este archivo nos permite aprender más sobre los métodos de los piratas informáticos y aumentar nuestra propia seguridad en consecuencia.

• CVE: CVE, abreviatura de Vulnerabilidades y exposiciones comunes, es una lista de fallas de seguridad informática divulgadas públicamente. Cuando alguien se refiere a un CVE, se refiere a una falla de seguridad a la que se le ha asignado un número de identificación de CVE.

Los avisos de seguridad emitidos por proveedores e investigadores casi siempre mencionan al menos una ID de CVE. Los CVE ayudan a los profesionales de TI a coordinar sus esfuerzos para priorizar y abordar estas vulnerabilidades para hacer que los sistemas informáticos sean más seguros.
El objetivo principal de CVE es ayudar a las organizaciones a mejorar sus defensas de seguridad. Para ello, identifica y proporciona un catálogo de vulnerabilidades de software o firmware y lo pone a disposición como diccionario gratuito.

6 HERRAMIENTAS UTILIZADAS

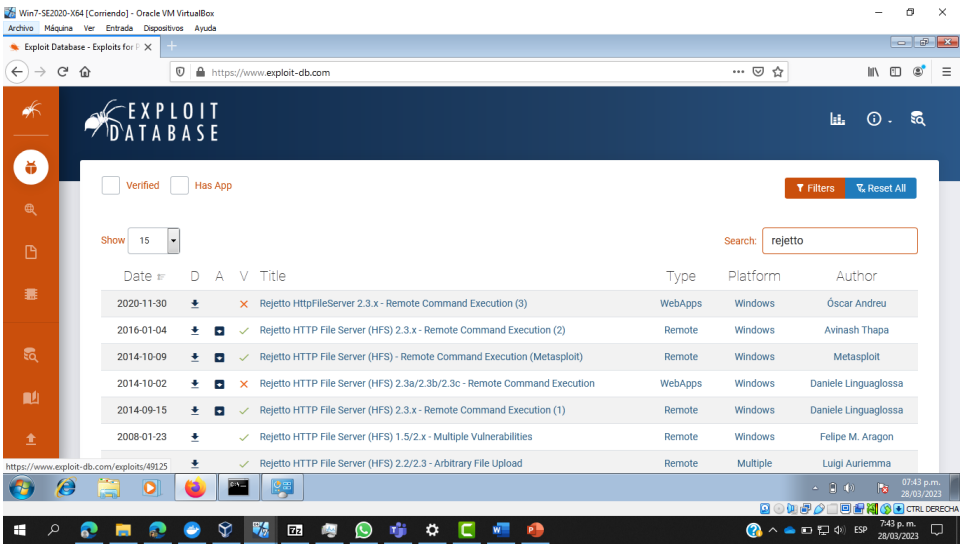
De acuerdo con las fases de pentesting, describa los métodos y herramientas utilizados para resolver la situación del RED TEAM.

Los procesos de pentesting para la situación específica se pueden crear de la siguiente manera, según el análisis que se realizó en la documentación proporcionada.

fase de identificación

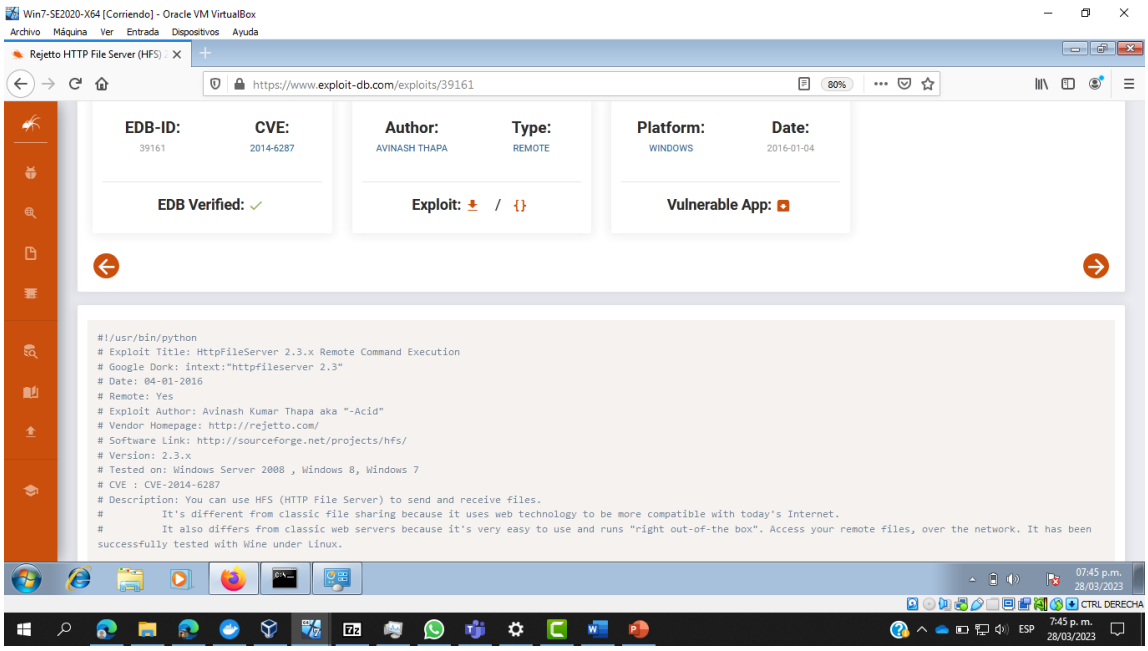
Se examinó la documentación del caso, y allí se pudieron encontrar varias pistas a seguir. Una de estas es la aplicación rejetto v2.3, sobre la cual se realiza una investigación, y en la cual encontramos diversas fallas de seguridad. También tenemos acceso a información clave sobre el host de destino, incluido su sistema operativo y arquitectura.

Ilustración 1 Información sobre rejetto en www.exploit-db.com



Fuente: propia.

Ilustración 2 Exploit seleccionado

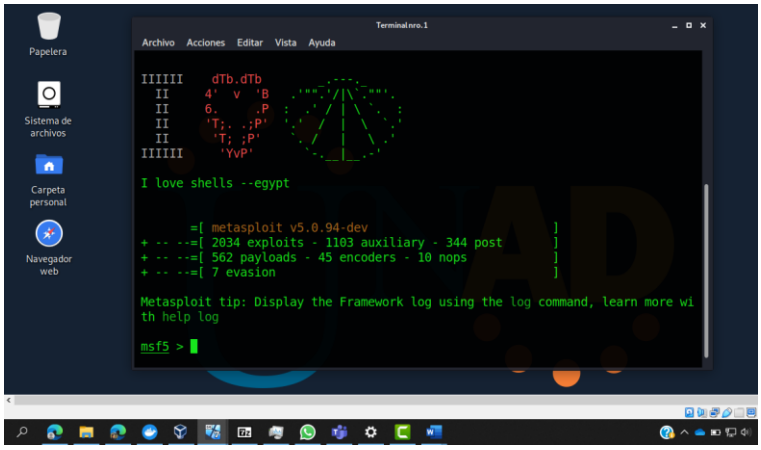


Fuente: propia.

6.1 ETAPA DE ESCANEO DE PUERTO, SERVICIO Y SISTEMA OPERATIVO

Para capturar todos los datos que recopilamos con cada comando, primero utilizaremos la aplicación Metasploit Framework lista para usar que se incluye con Kali Linux. Iniciamos la aplicación y creamos el proyecto de pentesting con los siguientes comandos.

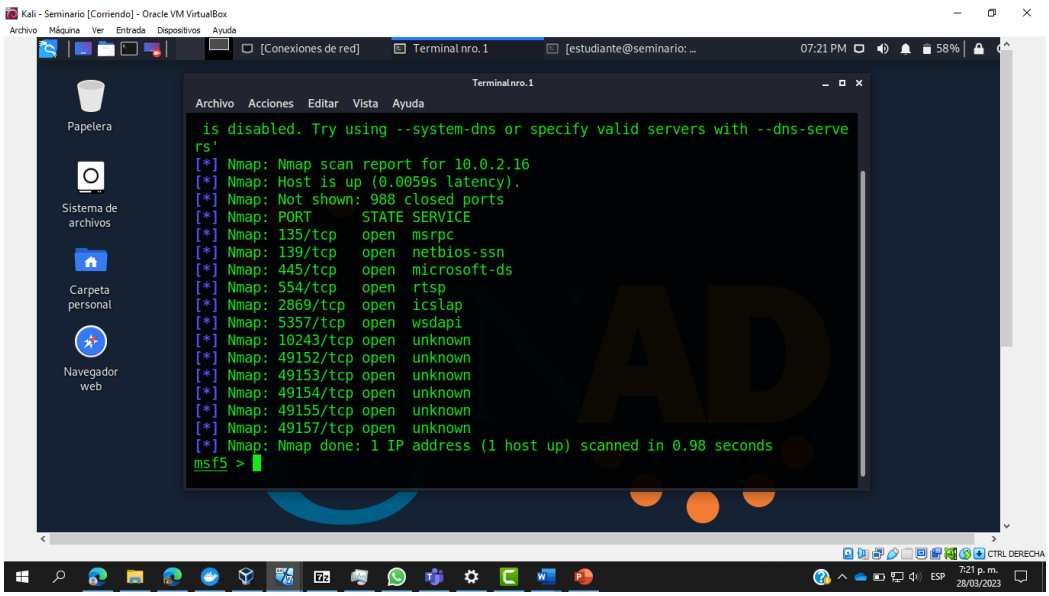
Ilustración 3 Ilustración 3 Creación de espacio de trabajo en metasploit



Fuente: propia.

NMAP Una vez que tenemos el espacio en metasploit, ejecutamos un análisis con el comando DB NMAP, que me permite utilizar la aplicación NMAP de metasploit, recopilando toda la información pertinente que descubrimos. Esta herramienta es crucial para escanear el objetivo.

Ilustración 4 Ilustración 4 Escaneo del host objetivo



Fuente: propia.

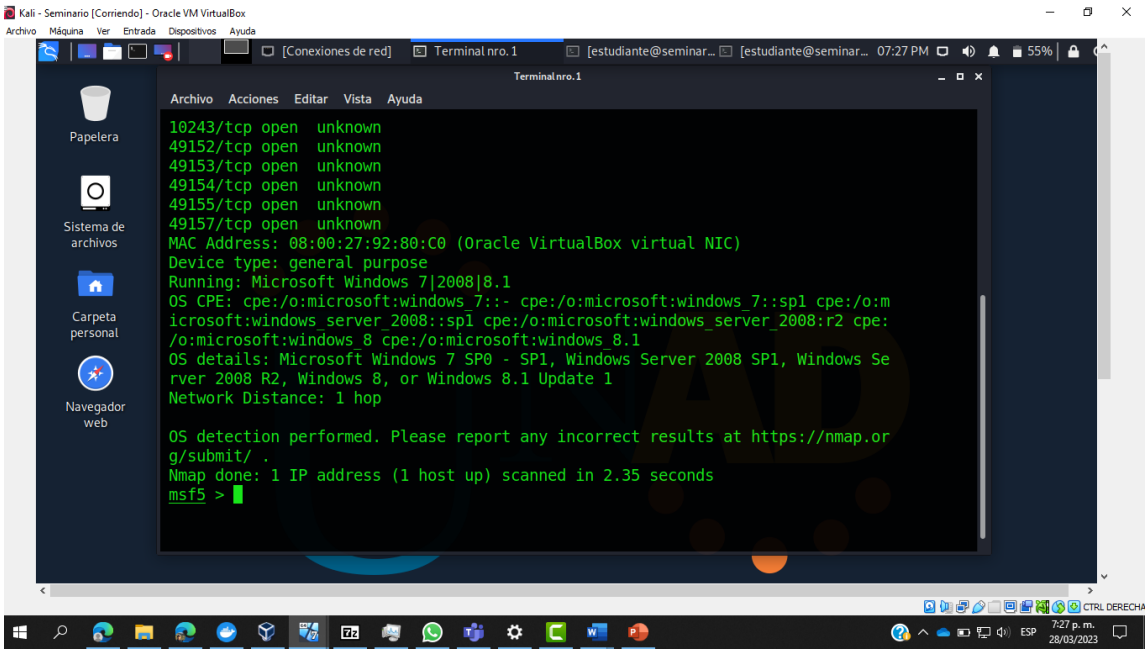
El objetivo del reconocimiento es encontrar más vulnerabilidades usando Nessus, una aplicación diferente y bien conocida.

Ilustración 5 Búsqueda de vulnerabilidades con Nessus

Fuente: propia.

El sistema operativo, los puertos y los servicios de la máquina de destino se identifican mediante búsquedas más precisas.

Ilustración 5 Ilustración 6 Buscando más detalles del host



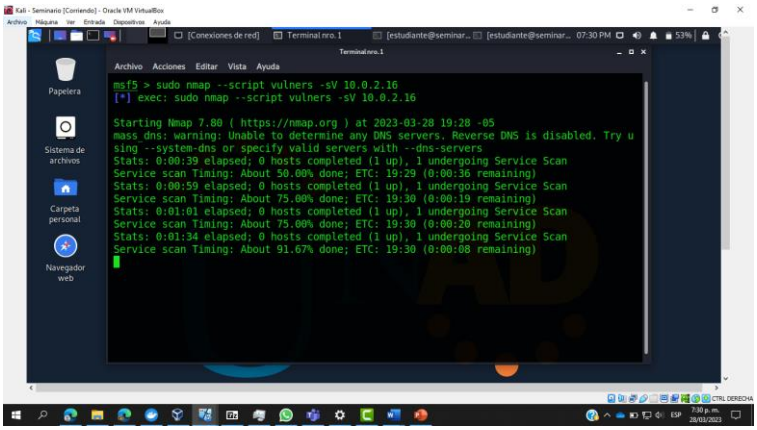
Fuente: propia.

6.2 IDENTIFICACIÓN Y ANÁLISIS DE VULNERABILIDADES

Se realiza un estudio mediante el comando NMAP, que permite verificar mediante las bases de datos de exploits las vulnerabilidades de los equipos.

Podemos determinar la vulnerabilidad conocida para la que existe un exploit identificado con el ID 6287 comparando y validando las vulnerabilidades reconocidas con los datos recopilados.

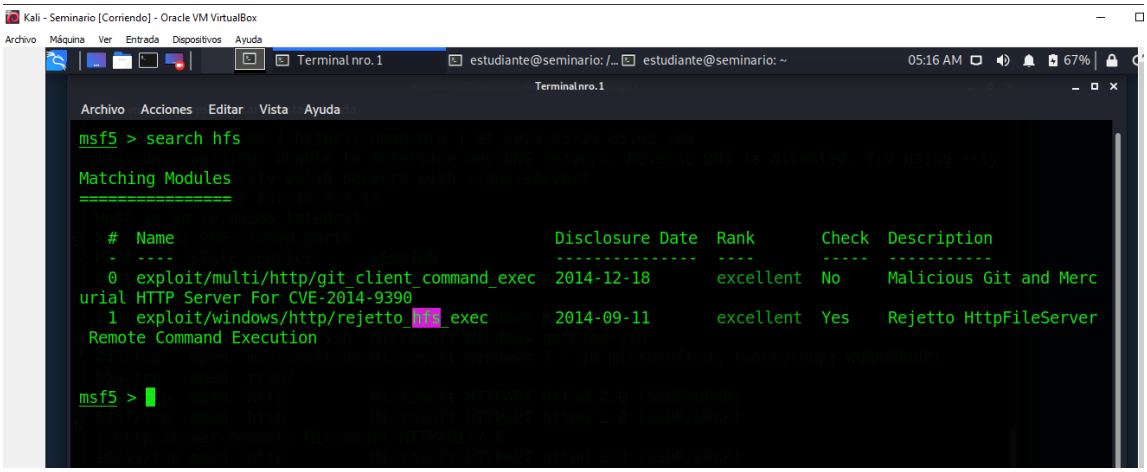
Ilustración 6 Ilustración 7 Búsqueda de vulnerabilidades con NMAP



Fuente: propia.

La búsqueda se realiza con el programa Metasploit luego de que Metasploit Framework tenga los datos del exploit a utilizar, permitiéndonos buscar los exploits vinculados a un nombre característico de la aplicación susceptible o un número de identificación del exploit.

Ilustración 7 Ilustración 8 Búsqueda de vulnerabilidades

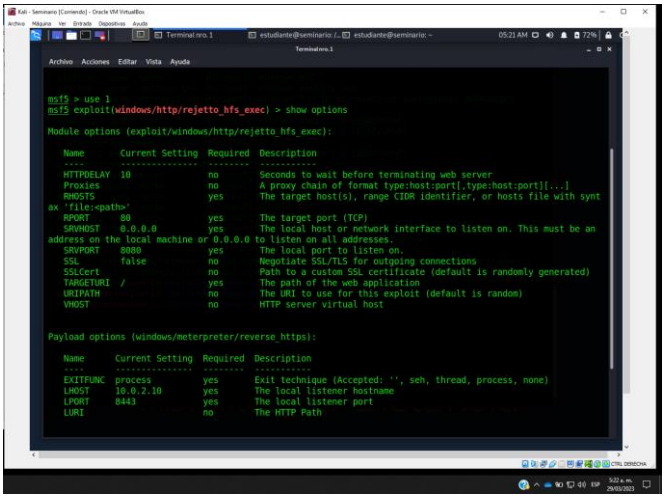


Fuente: propia.

Etapa de Explotación de Vulnerabilidad

Elegimos el exploit en el programa Metasploit Framework y confirmamos la configuración que necesitamos para configurarlo ya que tenemos toda la documentación e investigación previa de las vulnerabilidades y exploits a utilizar.

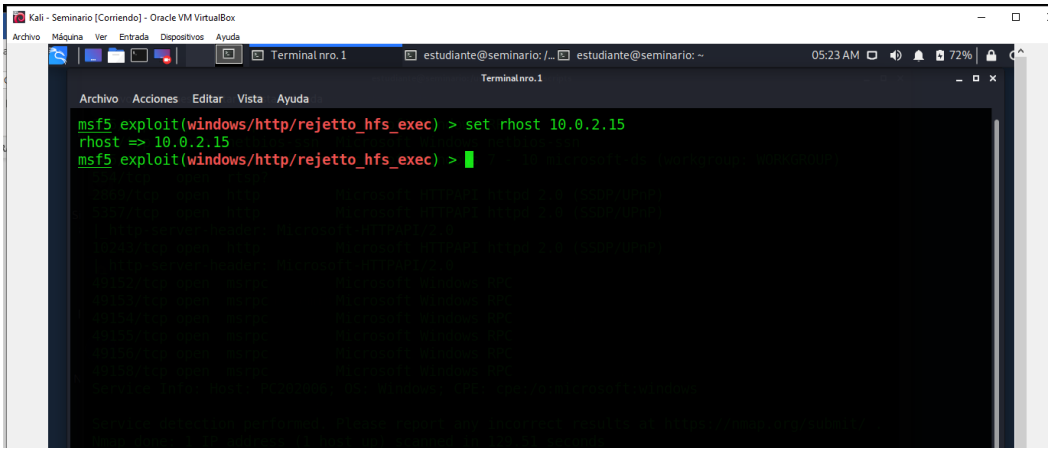
Ilustración 8 Ilustración 9 Opciones del exploit



Fuente: propia.

Se deben configurar los RHOSTS que identifican el host de destino.

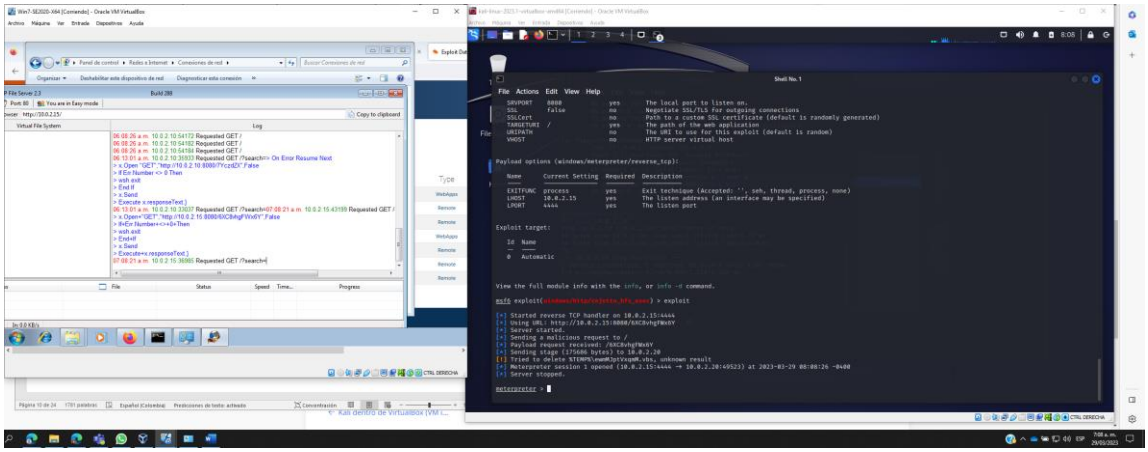
Ilustración 9 Ilustración 10 Configuración de host objetivo explot



Fuente: propia.

Como las configuraciones relevantes se establecieron con precisión de antemano, no es necesario validarlas en este caso. Con el comando exploit, pasamos a explotar la falla y la aplicación comienza a ejecutar el script del exploit elegido.

Ilustración 11 Explotando vulnerabilidad



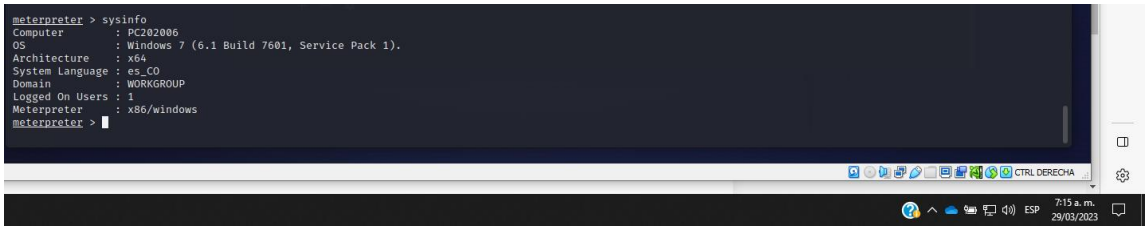
Fuente: propia.

6.3 ETAPA DE ELEVACIÓN DE PRIVILEGIOS

Actualmente, estamos usando la herramienta Metasploit, que crea un conjunto de comandos que se ejecutan en el host de destino con la ayuda de los usuarios que fueron reclutados para el ataque.

El siguiente comando se puede usar con esta herramienta para habilitar una sesión de comando de Windows con tokens o permisos asociados.

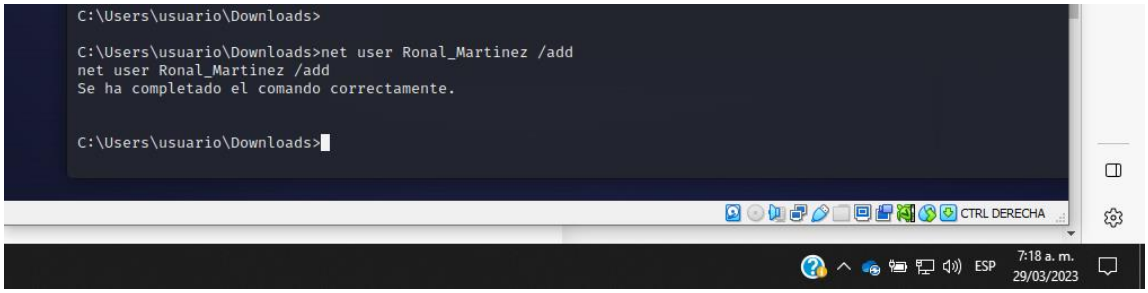
Ilustración 10 Ilustración 12 Comando para abrir ventana de comando windows



Fuente: propia.

Ahora que la sesión de comando está activa, podemos crear el usuario que ilustra el impacto potencial en el host de destino.

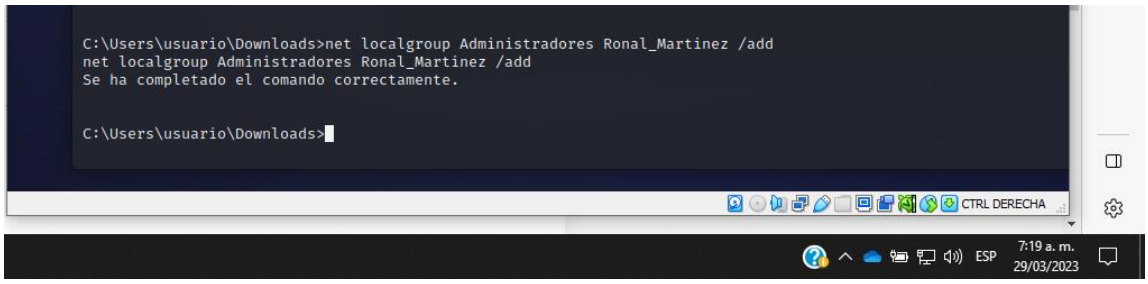
Ilustración 11 Ilustración 13 Comando para crear usuario en windows



Fuente: propia.

concesión de permisos de usuario.

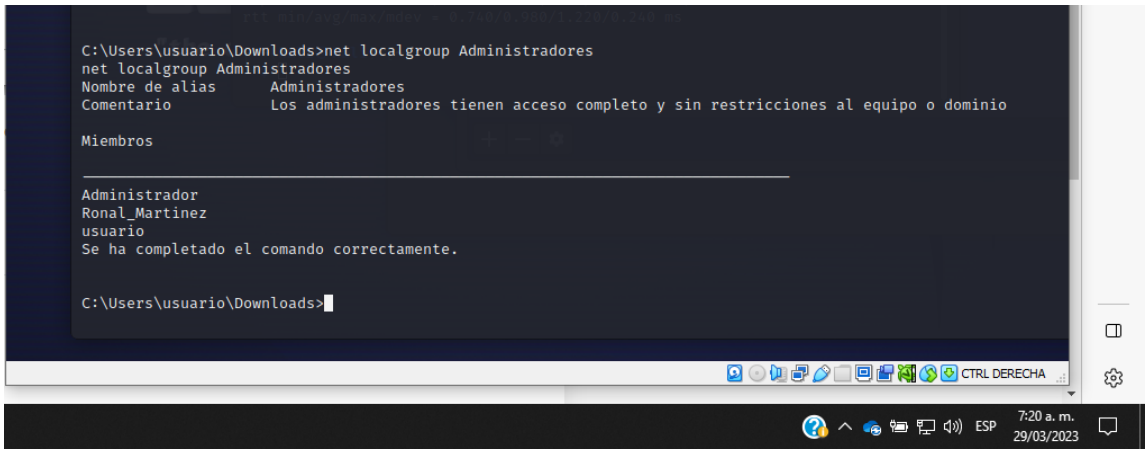
Ilustración 12 Ilustración 14 Asignar grupo al usuario creado



Fuente: propia.

Validación de la creación del usuario con sus respectivos permisos.

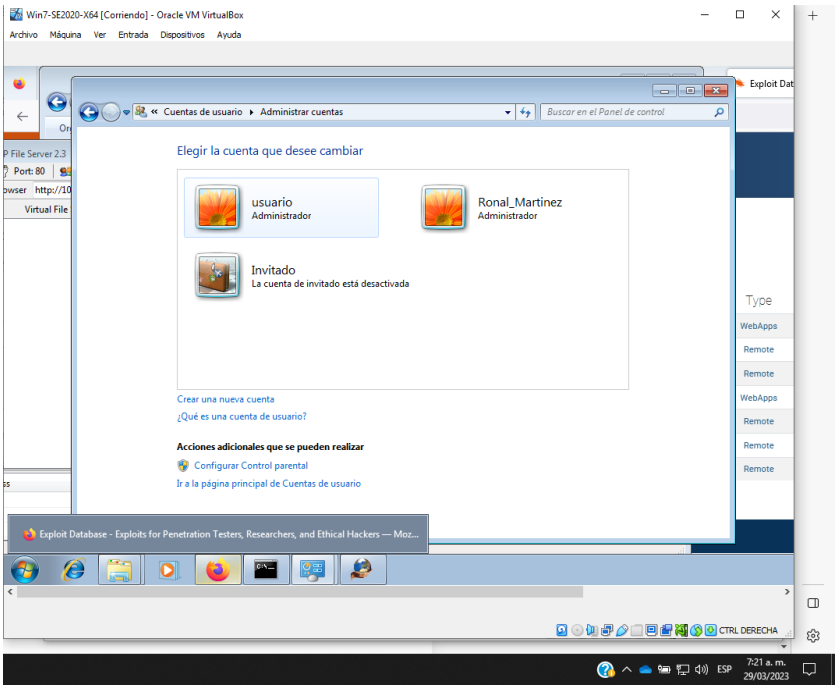
Ilustración 13 Ilustración 15 Consulta de usuarios del objetivo



Fuente: propia.

Validación de cada salida producida por comandos dentro del equipo objetivo.

Ilustración 14 Ilustración 16 Validación en el host objetivo



Fuente: propia.

6.4 INFORME CON ANÁLISIS DEL CASO DE RED TEAM, QUE PERMITIÓ DAR SOLUCIÓN AL FALLO IDENTIFICADO

Fue esencial la información dada en el anexo 4, ya que disminuyó considerablemente varios aspectos de la investigación.

- Rejetto: este dato de la aplicación que está asociado al equipo donde posiblemente se está generando una fuga de información, fue clave porque con solo una búsqueda en Google, se puede identificar varios exploit asociados a este.
- Versión: este dato también es elemental, porque en la etapa de reconocimiento se encontró que el exploit atacaba diferentes versiones, solo con algunas se podía lograr correctamente el ataque.
- Shell reversa: también sirvió para reducir la búsqueda en el exploit, indicándonos el método final de explotación.
- Elevación de privilegios: esto ayudo a identificar uno de los objetivos iniciales al ejecutar el ataque.
- Versión del SO: esto ayudo para poder seleccionar el exploit que servía y correspondía con el sistema operativo a atacar.
- Copia del servidor: esta copia fue fundamental ya que, sin ella no se podría realizar el laboratorio de pentesting.

Informe de herramientas utilizadas para dar identificar fallos en el escenario propuesto.

Se uso la herramienta NMAP y NESSUS, en ambas se pudo ver la vulnerabilidad activa en el puerto 80 sobre la máquina de Windows 7, esto claro con la aplicación rejetto funcionando, al realizar la explotación y establecer la conexión con meterpreter se identifica que se escucha desde la maquina atacante con el puerto 4444, y la sesión se establece con el puerto 49165.

Análisis del ataque presentado a cada una de las maquinas identificadas.

Básicamente el ataque permite la ejecución o manipulación de la maquina Windows 7, desde una consola de comandos con privilegios system, esto según entiendo por medio de la función findMacroMarker en parserLib.pas que se encuentra en Rejetto HTTP File Server antes de la versión 2.3c, ya en la consola el atacante puede llegar a ejecutar programas arbitrariamente, o profundizar su ataque a otros equipos de la red donde este la máquina, comprometiendo toda la red y sus sistemas.

Las herramientas utilizadas en este análisis de seguridad incluyeron el sistema operativo Kali Linux y la herramienta Metasploit para llevar a cabo el ataque y explotar la vulnerabilidad en la máquina de Windows 7 de 64 bits. La herramienta Nmap se utilizó para la identificación de los puertos abiertos en la máquina objetivo, y se determinó que la aplicación vulnerable estaba utilizando el puerto 80.

El uso del puerto 80 es comúnmente utilizado para publicar sitios web utilizando el protocolo HTTP, el cual no es seguro y es propenso a los ataques. La explotación de vulnerabilidades en equipos o software puede ser devastadora para las empresas y los usuarios de tecnología de la información si no se realizan actualizaciones de seguridad adecuadas.

Para explotar la vulnerabilidad en la máquina Windows 7 de 64 bits, se llevaron a cabo diversos pasos que incluyeron la instalación de dos máquinas virtuales, la desactivación del firewall en la máquina objetivo y la creación de un usuario con privilegios de administrador. La herramienta Nmap se utilizó para analizar los puertos abiertos en la máquina de Windows 7 y se identificó la aplicación rejetto v.2.3 como la responsable de la fuga de información. Finalmente, se ejecutó el ataque desde Kali y se obtuvo acceso para el ataque solicitado.

7 RETENCIÓN DE FALLOS SEGÚN ATAQUE

PRIMER PASO

Es fundamental para cualquier organización identificar el método de ataque utilizado y las posibles vulnerabilidades que están siendo explotadas. Esto debe ser explorado en línea con el modelo de seguridad implementado y los pasos previamente definidos para minimizar los daños a la organización.

Un paso crítico en este proceso es realizar un análisis de pentesting para identificar posibles puntos de ataque activos y detectar las vulnerabilidades explotadas en los sistemas comprometidos. Es esencial identificar los sistemas comprometidos para poder aislarlos sin necesidad de deshabilitar todos los servicios o dispositivos en la infraestructura tecnológica.

Una vez que el ataque se ha contenido en los sistemas comprometidos, se puede prevenir la propagación del ataque a otros sistemas conectados en la red. Es importante tomar una copia forense de los sistemas infectados para poder analizarlos más a fondo y detectar las vulnerabilidades explotadas y entender el impacto del ataque.

7.2 SEGUNDO PASO

Para validar las vulnerabilidades en un entorno controlado, se pueden utilizar herramientas gratuitas como Metasploit combinado con NMAP, Armitage, entre otras. Una vez que se han validado las vulnerabilidades con herramientas de pentesting, es importante buscar los posibles exploits utilizados en el ataque para ejecutar los controles necesarios en los sistemas o dispositivos en la red que puedan ser vulnerables.

7.3 TERCER PASO

Finalmente, una vez que se ha llevado a cabo la explotación en el laboratorio, es esencial validar cualquier posible impacto que no se haya considerado y ampliar

la búsqueda en cualquier sistema en producción que haya sido posiblemente atacado. Con estas medidas, se puede minimizar el daño causado por un ataque y proteger la infraestructura tecnológica de la organización.

8 HARDENIZACIÓN

Acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.

Después de llevar a cabo el proceso de laboratorio por parte del equipo de redteam, se han identificado varias debilidades que deben ser abordadas para reducir y mitigar las vulnerabilidades de nuestro servidor.
Se proponen las siguientes medidas de endurecimiento (hardenización):

- En primer lugar, se debe validar los usuarios que utilizan los dispositivos, y si no necesitan tener privilegios de administración, se deben eliminar y solo permitir la autorización para ejecutar las tareas autorizadas.
- Es necesario actualizar todo el software utilizado, incluyendo el sistema operativo, aplicaciones, antivirus, entre otros.
- Validar los puertos habilitados en el host, y corregir o cerrar cualquier posible puerto que pueda generar alguna vulnerabilidad.
- Revisar y cambiar las credenciales de los usuarios afectados.
- Verificar si todos los usuarios del dispositivo son necesarios o si solo se debiera tener uno para consultas o producción.
- Implementar medidas de seguridad con un firewall, que permita la identificación de vulnerabilidades, como IDS, IPS, entre otras.
- Establecer políticas de seguridad que permitan limitar el alcance de los usuarios y prevenir posibles brechas de seguridad mediante estándares de configuración.
- Subdividir la red si es posible, para tener servicios aislados que no deban estar expuestos a posibles accesos malintencionados.

9 CIS CENTER FOR INTERNET SECURITY

Análisis sobre la pertinencia de trabajar con cis center for internet security como propuesta de aseguramiento por parte de un equipo de blue team.

En primer lugar, es importante definir CIS como una organización sin fines de lucro que lidera una comunidad global de profesionales de TI para desarrollar y evolucionar continuamente las mejores prácticas reconocidas a nivel mundial para proteger los sistemas y datos de TI a través de CIS Controls y CIS Benchmarks. Esta organización proporciona productos y servicios que permiten a las empresas protegerse de manera proactiva contra las amenazas emergentes, como las CIS Hardened Images, que proporcionan entornos informáticos escalables, seguros y bajo demanda en la nube.

Al implementar las pautas de CIS, se pueden proteger los sistemas y dispositivos tecnológicos mediante la configuración adecuada de hardware y software, ya sean equipos de cómputo, dispositivos móviles o servidores. Estas pautas también se pueden utilizar para desarrollar una estructura del programa de seguridad de la información y una política que permita una metodología de seguridad óptima con funciones claras. Al implementar estas buenas prácticas, las empresas pueden contar con medidas defensivas que les permitirán prevenir ataques a la infraestructura tecnológica.

En resumen, CIS es una organización que lidera una comunidad global de profesionales de TI y proporciona las mejores prácticas reconocidas a nivel mundial para proteger los sistemas y datos de TI. Al implementar estas pautas, las empresas pueden proteger sus sistemas y dispositivos tecnológicos y desarrollar una estructura de seguridad informática sólida.

10 ANÁLISIS SOBRE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM.

SIEM (Security Information and Event Management) es una herramienta que brinda una serie de características y funciones para el análisis de seguridad en tiempo real. Su principal objetivo es identificar y alertar sobre eventos de seguridad potencialmente peligrosos, generados por dispositivos de redes o aplicaciones.

Para lograr esto, SIEM se basa en dos métodos de administración: SIM (Security Information Management) y SEM (Security Event Management). SIM se encarga de almacenar y analizar información de seguridad, mientras que SEM se enfoca en el monitoreo en tiempo real y la validación de eventos.

Entre las funciones más importantes de SIEM se encuentran la identificación de falsos positivos y ataques reales, la centralización del monitoreo de amenazas potenciales, la generación de alertas redirigidas según la clasificación de las alertas, la documentación y registro de todas las etapas del proceso de detección, actuación y resolución, y el cumplimiento de las leyes y normas de protección de datos y seguridad.

El software SIEM recopila datos de eventos y registros generados por diferentes dispositivos y aplicaciones de seguridad en una organización, y los reúne en una única plataforma centralizada. Estos datos pueden incluir registros de firewall, eventos antivirus y otras fuentes, y son clasificados en diferentes categorías para facilitar su análisis.

En resumen, SIEM proporciona una solución integral de seguridad para la identificación y prevención de amenazas en tiempo real, y permite a las organizaciones documentar y registrar todas las etapas de los procesos de seguridad para cumplir con las leyes y normas de protección de datos y seguridad.

11 HERRAMIENTAS QUE PERMITAN CONTENER ATAQUES INFORMÁTICOS.

11.1 SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT):

Esta herramienta proporciona análisis en tiempo real de alertas que pueden ser identificadas como peligrosas, ya sean generadas por equipos de redes o aplicaciones. Ofrece funciones como la identificación de falsos positivos y ataques reales, la centralización del monitoreo de todas las amenazas potenciales, la generación de alertas redirigidas dependiendo de la clasificación de las alertas, y el registro y documentación de todas las etapas en un proceso de detección, actuación y resolución.

11.2 CIS (CENTER FOR INTERNET SECURITY):

CIS es una organización sin fines de lucro que lidera una comunidad global de profesionales de TI para hacer evolucionar continuamente los estándares de CIS Controls y CIS Benchmarks, que son las mejores prácticas reconocidas a nivel mundial para proteger los sistemas y datos de TI. Ofrece productos y servicios para protegerse de manera proactiva contra las amenazas emergentes, y las CIS Hardened Images proporcionan entornos informáticos escalables, seguros y bajo demanda en la nube.

11.3 IPS (INTRUSION PREVENTION SYSTEM)

Es un sistema de prevención de intrusiones que tiene como objetivo detectar y prevenir ataques antes de que puedan causar daños al sistema o a la red. El IPS puede analizar el tráfico de red en tiempo real y detectar patrones de tráfico maliciosos, además de bloquear el tráfico malicioso antes de que alcance su destino.

El IPS utiliza técnicas como la detección de firmas, la inspección de paquetes profundos y la heurística para detectar y bloquear los ataques. También puede integrarse con otras herramientas de seguridad, como firewalls y sistemas SIEM, para proporcionar una protección más completa.

El IPS es una herramienta importante en la defensa contra ataques informáticos, ya que puede detectar y bloquear los ataques antes de que puedan causar daños graves. Sin embargo, como con cualquier herramienta de seguridad, es importante configurar el IPS correctamente y mantenerlo actualizado para garantizar que proporcione una protección efectiva contra los ataques informáticos más recientes.

12 RECOMENDACIONES

12.1 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM

En el ámbito de la seguridad, se reconoce la importancia del trabajo en equipo y la planificación estratégica para garantizar el éxito de las medidas implementadas en los equipos. Entre los aspectos cruciales para tener en cuenta, destacan los siguientes:

Comunicación entre equipos: es fundamental establecer canales de comunicación efectivos entre los equipos para permitir el intercambio de información sobre los avances en cada aspecto de los equipos, así como las investigaciones que se estén llevando a cabo.

Planes de acción: se deben documentar todas las actividades realizadas por los equipos para poder monitorear detalladamente su progreso y proporcionar retroalimentación continua para mejorar los procesos.

Capacitación: es esencial proporcionar una capacitación constante a los equipos, ya que las amenazas cibernéticas evolucionan y mejoran constantemente.

Pruebas: es importante realizar prácticas de ataques y simulaciones de restauración de desastres, así como cualquier otra actividad que permita validar los planes establecidos y recrear incidentes que puedan mejorar la respuesta de los equipos ante situaciones de emergencia.

13 MEDIDAS DE HARDENIZACIÓN PROPUESTAS PARA EVITAR FUTUROS ATAQUES

Lo primero que se debe hacer es aprender de los errores, por lo cual se deben cerrar las brechas de seguridad que se identificaron en el ataque, luego de esto, sería importante tener en cuenta lo siguiente:

- Actualizar o adquirir antivirus que permitan el escaneo de los sistemas en tiempo real y su respectivo alertamiento.
- Crear políticas de instalación de programas en los equipos de la empresa o en aquellos que se conecten a la red, y también llevar a cabo la desinstalación de programas que no sean utilizados y representen un potencial peligro.
- Mantener actualizados los equipos de la compañía y los sistemas operativos que se utilizan.
- Solo permitir el acceso remoto a través de una VPN y con la autorización previa de la gerencia de TI.
- Si los firewalls de Windows no están activos, deben ser instalados.
- • Los usuarios con privilegios de administrador no deben ser utilizados por personal ajeno al área de informática.
- Realizar pruebas de vulnerabilidad de manera periódica.

Tambien se puede realizar la implementación de un framework que cobije todos los paso necesarios para la protección del dato e infraestructura de la compañía. Desenvolver e implementar as salvaguardas apropiadas para garantir a entrega de servicios de infraestructura crítica. A continuación, las medidas específicas que se deben tomar en cada una de las áreas clave de ciberseguridad: protección, detección, respuesta y recuperación.

En el área de Protección, se deben establecer controles de acceso para limitar quiénes tienen acceso a los activos y las instalaciones, y se deben proporcionar

concientización y entrenamiento sobre seguridad cibernética al personal y los socios de la organización. Además, se deben gestionar los datos e información de acuerdo con la estrategia de riesgo de la organización, y se deben mantener procesos y procedimientos de protección de información.

En el área de Detección, se deben implementar actividades para identificar eventos de seguridad cibernética, incluyendo la detección oportuna de actividad anómala, el monitoreo continuo de seguridad y la realización de pruebas regulares de los procesos de detección.

En el área de Respuesta, se deben desarrollar y ejecutar procesos y procedimientos de respuesta para garantizar una respuesta oportuna a los eventos de seguridad cibernética. Se deben coordinar las actividades de respuesta con partes interesadas internas y externas, y se deben realizar análisis y mitigaciones para prevenir la expansión de eventos y apoyar la recuperación.

Finalmente, en el área de Recuperación, se deben desarrollar y ejecutar planes de recuperación para restaurar los sistemas o activos afectados por eventos de seguridad cibernética, y se deben mejorar estos planes incorporando las lecciones aprendidas de eventos anteriores. Las actividades de recuperación también deben coordinarse con partes internas y externas, incluyendo centros de coordinación y proveedores de servicios de Internet.

14 RECOMENDACIONES PERSONALES PARA ASEGURAMIENTO

La importancia de las estrategias de mejora radica en aprender de los errores, no solo los propios sino también de los de otros. Es esencial mantenerse actualizado sobre las operaciones realizadas en diferentes organizaciones, cómo se ejecutaron, controlaron y mitigaron. Además, es crucial que las empresas comprendan la relevancia de la actualización de equipos, la adquisición de antivirus, la creación de políticas de seguridad, el control de usuarios y accesos, entre otros aspectos de seguridad. La cooperación de estos factores endurece la seguridad de las organizaciones.

Por otro lado, el factor humano no debe ser ignorado, ya que es una de las principales vulnerabilidades para los accesos no autorizados a los sistemas e información. La capacitación constante y la sensibilización sobre las normas de seguridad y sus consecuencias son obligatorias. Por último, es fundamental realizar un monitoreo constante de la empresa u organización, verificar el cumplimiento de las políticas de seguridad informática y de la información, auditar las diferentes áreas y aplicar controles efectivos para abordar las inconformidades detectadas.

15 LINK DE VIDEO

https://youtu.be/VRbEMxxDnx4

16 CONCLUSIONES

- La seguridad informática es un aspecto fundamental en cualquier organización, y para lograrla es necesario estar actualizado en cuanto a las operaciones realizadas en otras empresas, implementar políticas de seguridad, mantener equipos actualizados y realizar capacitaciones constantes para el personal.
- La importancia de aprender de los errores propios y ajenos en el ámbito de la seguridad informática no puede ser subestimada, ya que esto permitirá fortalecer los aspectos de seguridad de la organización y mitigar los riesgos.
- El factor humano es una de las principales brechas de seguridad en la informática, por lo que es fundamental llevar a cabo una capacitación constante y sensibilización en cuanto a las normas de seguridad y sus posibles consecuencias.
- La monitorización constante, la verificación de cumplimiento de las políticas de seguridad informática y la aplicación de controles efectivos son herramientas esenciales para detectar y corregir inconformidades en la seguridad informática de las organizaciones.

BIBLIOGRAFIA

ANDERSON, R. J. Ingeniería de la seguridad: Guía para la construcción de sistemas distribuidos confiables 2ª ed.. John Wiley & Sons. 2008.

ANDRESS, J. Los fundamentos de la seguridad de la información: Entendiendo los fundamentos de InfoSec en teoría y práctica. Syngress. 2011.

BEJTLICH, R. La práctica de la monitorización de la seguridad de redes: Entendiendo la detección y respuesta de incidentes 2ª ed.. No Starch Press. 2013.

ERICKSON, J. Hacking: The Art of Exploitation. No Starch Press.

HARRIS, S., & MAYMI, F. J. Guía completa para el examen CISSP 8ª ed.. McGraw Hill. 2018.

JAQUITH, A. Métricas de seguridad: Reemplazando el miedo, la incertidumbre y la duda. Addison-Wesley Professional. 2007.

KIM, P. The hacker playbook 3: Guía práctica para la prueba de penetración. Independently published. 2018.

LAKHANI, N. K., & SISTRUNK, J. GRAY Hat Hacking: The Ethical Hacker's Handbook 3rd ed.. McGraw-Hill Education. 2019.

MCCLURE, S., SCAMBRAY, J., & KURTZ, G. Hacking Exposed: Secretos y soluciones de seguridad de redes 7ª ed.. McGraw Hill. 2015.

MEEUWISSE, R. Ciberseguridad: La guía para principiantes. IT Governance Publishing. 2014.

Metasploit Unleashed. n.d.. https://www.offensive-security.com/metasploit-unleashed. 2008.

MITNICK, K. D., & SIMON, W. L. El arte del engaño: Controlando el elemento humano de la seguridad. Wiley. 2003.

MUNIZ, J., MCINTYRE, G., & ALFARDAN, N. Centro de operaciones de seguridad: Construcción, operación y mantenimiento de su SOC. Cisco Press. 2018.

PINTO, M. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing. 2015.

STALLINGS, W. Fundamentos de seguridad de redes: Aplicaciones y estándares 6ª ed.. Pearson. 2017.

Sullivan, B., & Liu, V. 2014. Seguridad de aplicaciones web: Una guía para principiantes. McGraw Hill. 2001.

VIEGA, J., & MCGRAW, G. Construyendo software seguro: Cómo evitar problemas de seguridad de la manera correcta. Addison-Wesley Professional.
WHITMAN, M. E., & MATTORD, H. J. Principios de seguridad de la información 6ª ed. Cengage Learning. 2016.