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

JULIAN DAVID SOTO BALBUENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2024

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

JULIAN DAVID SOTO BALBUENA

SEMINARIO ESPECIALIZADO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

DIRECTOR DEL CURSO

EVER LUIS ARROYO BARÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2024

Contenido

Lista de Tablas

Lista de Figuras

GLOSARIO

Blue Team: Equipo comprometido con la supervisión proactiva de las redes y la gestión de cualquier dificultad de seguridad para garantizar la integridad de los datos de la organización.

Exploit: Método para penetrar en un sistema informático aprovechando sus puntos débiles y ejecutar acciones no permitidas.

Firewall: Barrera de protección que protege una red al inspeccionar y bloquear el tráfico de red que podría ser peligroso o no autorizado.

IDS/IPS: Herramientas de seguridad que monitorizan las redes en busca de actividades maliciosas. El IDS detecta, mientras que el IPS puede bloquear los intentos de intrusión.

Inyección SQL: Vulnerabilidad que permite a los piratas informáticos introducir código malicioso en las consultas SQL y conseguir acceso a un sistema de bases de datos a través de una aplicación web.

Payload: Componente de un ataque que ejecuta las tareas dañinas, como robar datos confidenciales, cifrar archivos o instalar otros tipos de malware.

Pentesting : simulación controlada de un ciberataque para evaluar las vulnerabilidades de un sistema, una red o una aplicación.

Red Team: Equipo de hackers éticos que imitan las acciones de cibercriminales para descubrir vulnerabilidades en los sistemas de una compañía.

Rootkit: Herramienta de ocultación utilizada por los hackers para mantener el control de un sistema infectado sin ser descubiertos.

Vulnerabilidad: Punto débil en la seguridad de un sistema que puede ser explotado para causar daño.

Zero-Day: Vulnerabilidad desconocida por los desarrolladores del software, lo que la hace especialmente peligrosa porque no hay parches de seguridad disponibles para mitigarla.

RESUMEN

Este estudio pone de relieve los equipos de ciberseguridad Red Team y Blue Team en el entorno colombiano. Estos equipos colaboran estrechamente para reforzar las defensas digitales de una organización. El Equipo Azul se encarga de implantar y mejorar las medidas de seguridad, mientras que el Equipo Rojo imita los ciberataques para encontrar puntos débiles. Esto crea un ciclo de aprendizaje sin fin que ayuda a las empresas a mantenerse por delante de las ciberamenazas.

La creciente amenaza de los ciberataques en Colombia ha tenido consecuencias significativas en diversas áreas, como pérdidas económicas debido al robo de datos financieros, la reducción de productividad y la exposición de información sensible. Ante este panorama, la colaboración entre los equipos de seguridad resulta crucial para anticiparse a los riesgos y mejorar la seguridad organizacional.

El Red Team desempeña un papel proactivo en la identificación de riesgos cibernéticos, al someter los sistemas de la empresa a pruebas de penetración rigurosas. Por su parte, el **Blue Team** se dedica a implementar estrategias de defensa, con el objetivo de minimizar el impacto de posibles intrusiones. El trabajo conjunto de estos equipos busca no solo identificar y corregir las vulnerabilidades, sino también crear un entorno más seguro para las empresas al reducir los riesgos asociados con los ataques cibernéticos.

INTRODUCCION

La creciente digitalización ha expuesto a las organizaciones de todo el mundo, incluyendo a las colombianas, a un panorama de amenazas cibernéticas cada vez más complejo. Para proteger información confidencial, activos financieros y garantizar la continuidad del negocio, la ciberseguridad se ha vuelto indispensable. En esta idea, los equipos Red Team y Blue Team juegan un papel fundamental en la contencion proactiva contra ciberataques

Las empresas colombianas pueden mejorar enormemente su enfoque en cuanto a la ciberseguridad integrando la experiencia del Equipo Rojo y el Equipo Azul. El Equipo Azul toma las precauciones necesarias para salvaguardar los sistemas y datos de la organización, mientras que el Equipo Rojo encuentra vulnerabilidades. Construir una ciberdefensa sólida, minimizar el impacto de los incidentes y anticiparse a los riesgos es posible gracias a este trabajo en equipo.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Examinar la actuación del Equipo Rojo y del Equipo Azul en Colombia para identificar las áreas que necesitan trabajo y reforzar la ciberseguridad.

1.2 OBJETIVOS ESPECÍFICOS

- Examinar los efectos de la legislación colombiana sobre protección de datos (Ley 1273 de 2009 y Ley 1581 de 2012) en los planes de seguridad de las empresas.
- Identificar las etapas de un ataque cibernético y optimizar los procesos de respuesta a incidentes para fortalecer las defensas de la organización.
- Reconstruir los incidentes de seguridad cibernética ocurridos en una organización, enfocándose en la vulnerabilidad de sistemas operativos y redes, con el fin de evaluar los puntos débiles y las lecciones aprendidas.

2 DESARROLLO DE TRABAJO – ETAPA 1

2.1 Normativa colombiana

2.1.1 Faltas Informáticas

En Colombia, la Ley 1273 de 2009 es la principal norma que protege la información y los datos, modificando el código penal para incluir delitos informáticos y salvaguardar los sistemas tecnológicos de comunicaciones[1].

La ley se compone:

- Capítulo 1- 8 artículos
- Capítulo 2 - 2 artículos

Capítulo Primero

La Ley 1273 de 2009 tipifica penalmente una variedad de conductas que atentan contra la protección de la información y los sistemas computacionales. La norma sanciona acciones como el hacking, la suplantación de identidad, el daño a sistemas informáticos y la obtención ilícita de datos personales. Al establecer un marco legal claro para la protección de la información, la ley contribuye a fortalecer la seguridad cibernética en Colombia y a disuadir a los ciberdelincuentes

Esta normativa resguarda la integridad y la disponibilidad de los sistemas computacionales al penalizar acciones como el daño, la alteración o la interrupción de su funcionamiento. Al establecer sanciones para quienes cometan estos delitos, la ley busca garantizar la continuidad de los servicios digitales y proteger la infraestructura crítica de las

[1] *Normatividad sobre delitos informáticos*. (2017, July 25). Policía Nacional de Colombia. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

organizaciones. Además, fomenta la adopción de medidas de seguridad para prevenir y responder a incidentes cibernéticos.

Tabla 1 Ley 173 de 2009-capitulo 1

Numero articulo	Título articulo	Pena prisión Meses	Multa en salario mínimo legal vigente
269A	Acceso abusivo a un sistema informático	48-96	100 a 1000
269B	Obstaculización ilegitima de sistema informático o red de telecomunicación	48-96	100 a 1000
269C	Interceptación de datos informáticos	36-72	100 a 1000
269D	Daño informático	48-96	100 a 1000
269E	Uso de software malicioso	48-96	100 a 1000
269F	Violación de datos personales	48-96	100 a 1000
269G	Suplantación de sitio web para capturar datos personales	48-96	100 a 1000
269H	Circunstancias de agravación punitiva		

Fuente: *Ley 1273 de 2009 - Gestor Normativo*. (2015, December). Funcionpublica.gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Capítulo Segundo:

Añade elementos relativos al robo y la transmisión ilegal de información, al tiempo que se concentra en la ciberdelincuencia y otros delitos. Estas infracciones conllevan duras penas, incluidas multas superiores a 1.500 salarios mínimos mensuales legales y penas de prisión de hasta 10 años[2].

2.1.2 Resguardo de la información personal

La información que nos identifica unívocamente como individuos se conoce como información personal, y se conserva en una variedad de bases de datos propiedad de organizaciones tanto públicas como comerciales. La Ley 1581 de 2012 en Colombia garantiza la conservación y manejo de esta información al tiempo que reconoce nuestro derecho a conocerla, actualizarla y rectificarla.

2.2 ETAPAS DEL PENTESTING

Las pruebas de penetración, a menudo conocidas como pentesting, se dividen en varias fases importantes. El primer paso es el reconocimiento, que recopila datos sobre el objetivo,

[2] *Ley 1273 de 2009 Congreso de la República de Colombia*. (2024). Bogotajuridica.gov.co. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

incluidas las direcciones IP y los servicios que se utilizan. A continuación, se detectan vulnerabilidades específicas mediante análisis más exhaustivos en la enumeración. La explotación es el siguiente paso, durante el cual se intenta utilizar las vulnerabilidades encontradas para obtener acceso a datos o sistemas. A continuación, viene la post-explotación, que consiste en determinar el alcance del acceso obtenido y si puede mantenerse. Por último, se elabora un informe en el que se exponen los resultados y se ofrecen sugerencias para mejorar la seguridad. Para detectar y reducir los riesgos en la infraestructura de un sistema, cada una de estas fases es esencial[3].

2.2.1 TIPOS DEL PENTESTING

Existen varios tipos de pentesting, cada uno enfocado en diferentes objetivos y metodologías. Los principales son:

2.2.1.1 Pentesting de Caja Blanca

Todos los datos del sistema, incluidas las configuraciones, el código fuente y la documentación, están a su disposición. Dado que el pentester puede encontrar fallos internos y problemas de diseño que podrían no ser evidentes en un ataque externo, este método permite una evaluación más completa.[4].

[3] TBSEK. (2023). *Etapas del proceso de pentesting: Una guía paso a paso*. Tbsek.mx. https://www.tbsek.mx/blog/2023/mayo/57.pentesting.html

[4] Servicios-Seguridad-Informatica. (2021, May 23). *Pentesting de Caja Blanca*. DragonJAR - Servicios de Seguridad Informática. https://www.dragonjar.org/pentesting-de-caja-blanca.xhtml

2.2.1.2 Pentesting de Caja Negra

En este enfoque, la prueba se realiza sin información previa sobre el sistema, simulando un ataque externo., donde el pentester actúa como un hacker que intenta descubrir vulnerabilidades sin ningún conocimiento interno. Esto permite identificar fallos de seguridad que podrían ser explotados por un atacante real[5].

2.2.1.3 Pentesting de Caja Gris

Este método combina elementos de los enfoques de las cajas negra y blanca. El evaluador tiene un conocimiento limitado del sistema, lo que le permite simular ataques más realistas y evaluar la seguridad de manera más completa. Este enfoque es útil para encontrar vulnerabilidades que un atacante con ciertos conocimientos internos podría aprovechar[6].

2.3 Fases del test de penetración

Estas fases proporcionan un marco estructurado que permite identificar y abordar de manera efectiva las vulnerabilidades de seguridad en los sistemas[7].

[5] José, J. (2024, June 30). *Pruebas de Caja Negra: Qué son, Técnicas y Cómo Implementarlas*. Deltaprotect.com; Delta Protect. https://www.deltaprotect.com/blog/pruebas-de-caja-negra

[6] *Pruebas de Caja Gris - TI Rescue*. (2024, August 29). TI Rescue. https://tirescue.com/pruebas-de-caja-gris/

[7] Nowak, S. (2022, November 28). *¿Qué es el Pentesting? Tipos, fases y herramientas*. Nuclio Digital School. https://nuclio.school/blog/que-es-el-pentesting/

2.3.1 Fase de Reconocimiento:

En esta etapa, el pentester recopila información sobre el objetivo de manera pasiva y activa. Se utilizan técnicas como la búsqueda de datos en dominios públicos, análisis de redes sociales y herramientas de escaneo para identificar direcciones IP, servicios activos y detalles sobre la infraestructura. El objetivo es obtener un perfil claro del sistema que se va a evaluar, lo que facilitará las siguientes fases.

2.3.2 Fase de Escaneo de Vulnerabilidades:

Después de obtener los datos necesarios, se realiza un análisis detallado para detectar posibles vulnerabilidades en el sistema, empleando herramientas automatizadas que examinan los puertos, servicios y aplicaciones en busca de debilidades conocidas. Esta fase es crucial para detectar fallos como configuraciones incorrectas, software desactualizado o vulnerabilidades de seguridad específicas.

2.3.3 Explotación de vulnerabilidades:

El pentester intenta aprovechar las vulnerabilidades encontradas en el paso anterior. Para acceder a los sistemas, aumentar los privilegios u obtener datos privados, se llevan a cabo ataques controlados. El objetivo es ilustrar el impacto real de las vulnerabilidades y cómo un atacante malintencionado podría aprovecharse de ellas.

2.3.4 Post Explotación:

Después de obtener acceso, el pentester evalúa el nivel de control alcanzado sobre el sistema. Se analizan las posibilidades de mantener el acceso, mover lateralmente dentro de la red o acceder a información crítica. Esta fase ayuda a comprender el alcance de un posible ataque y el daño que podría causar en una situación real.

2.3.5 Reporte:

Por último, pero no por ello menos importante, se redacta un informe exhaustivo en el que se describen todos los descubrimientos, incluidas las vulnerabilidades descubiertas, las técnicas de explotación empleadas y las posibles consecuencias. Además, se dan sugerencias específicas para reducir las vulnerabilidades y mejorar la seguridad del sistema. Para que la empresa comprenda sus riesgos y ponga en marcha las medidas correctivas adecuadas, este informe es crucial.

2.4 Recursos para la ciberseguridad

2.4.1 Metasploit:

Los expertos en seguridad pueden desarrollar, probar y ejecutar exploits en sistemas susceptibles utilizando esta plataforma de pruebas de penetración. Su gran base de datos de cargas útiles y exploits facilita el aprovechamiento de vulnerabilidades de sistemas operativos y aplicaciones. Esta metodología es muy útil para evaluar la seguridad de un entorno y modelar amenazas reales[8].

2.4.2 Nmap:

Herramienta de código abierto empleada para escanear redes y realizar auditorías de seguridad. Facilita la identificación de dispositivos en una red, la determinación de los servicios activos, la identificación de sistemas operativos y la detección de configuraciones de seguridad. Su versatilidad lo hace popular entre administradores de red y hackers éticos, quienes lo utilizan para evaluar la seguridad de la infraestructura[9].

[8] Verónica Arranz. (2024, May 21). *Metasploit: La herramienta esencial en Ciberseguridad*. Campusciberseguridad.com; Campus Internacional de Ciberseguridad. https://www.campusciberseguridad.com/blog/item/180-metasploit-herramienta-esencial-ciberseguridad

[9] Sepulveda, M. (2023, February 23). *Que es NMAP y como utilizarlo - El Club de la Ciberseguridad*. El Club de La Ciberseguridad. https://ciberseguridad.club/que-es-nmap-y-como-utilizarlo/

2.4.3 OpenVas:

Es una herramienta de gestión de vulnerabilidades que permite realizar análisis de seguridad en sistemas y redes. Proporciona un conjunto de escáneres que identifican vulnerabilidades conocidas en el software y las configuraciones. OpenVAS es una solución muy efectiva para realizar auditorías de seguridad y es especialmente valorada en entornos donde se busca cumplir con estándares de seguridad[10].

2.4.4 ExploitDB:

En esta base de datos de exploits y vulnerabilidades se puede encontrar información sobre diferentes vulnerabilidades de software. Ofrece una amplia gama de exploits, pruebas de concepto e información técnica para ayudar a los investigadores y profesionales de la seguridad a evaluar los sistemas. Además, ExploitDB es un gran recurso para conocer las vulnerabilidades más recientes que se han encontrado[11].

2.4.5 CVE:

Son un sistema para identificar y catalogar vulnerabilidades de seguridad en software y hardware. Cada vulnerabilidad se le asigna un identificador único, lo que simplifica la comunicación y gestión de riesgos en ciberseguridad. Al ofrecer descripciones detalladas, las

[10] 0x. (2024, March 16). *OPENVAS – Explorando tu Servidor - Ciberseguridad*. Ciberseguridad. https://ciberseguridad.art/2024/03/16/openvas-explorando-tu-servidor/

[11] https://www.facebook.com/grokkeepcoding. (2022, October 4). *¿Qué es ExploitDB? | KeepCoding Bootcamps*. KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-exploitdb/

CVE permiten a las organizaciones priorizar actualizaciones y auditorías, mejorando su defensa contra amenazas conocidas[12].

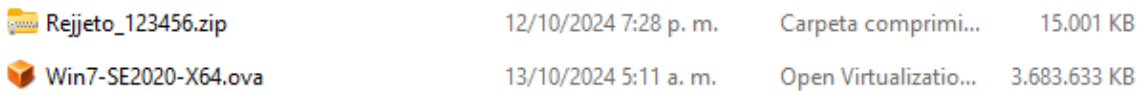
2.5 Plataforma de trabajo

Dos sistemas operativos -Windows 7 y Kali Linux, una variante de Debian diseñada para el avance de la auditoría y la seguridad informática, se instalarán en un entorno virtualizado para construir la arquitectura del Workbench. Desde la ruta indicada en el hilo, importaremos la máquina virtual Windows 7 x 64.

Figura 1 Descarga VirtualBox

Fuente: Elaboración propia

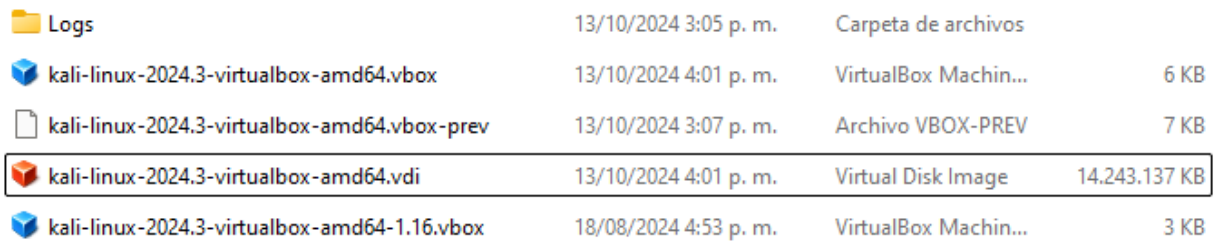
Figura 2 Descargar Windows 7.ova



Fuente: Elaboración propia

[12] *CVE (Common Vulnerabil... | Academia de Ciberseguridad*. (2024). Academia-Ciberseguridad.com. https://aprende.academia-ciberseguridad.com/books/conceptos/page/cve-common-vulnerabilities-and-exposures

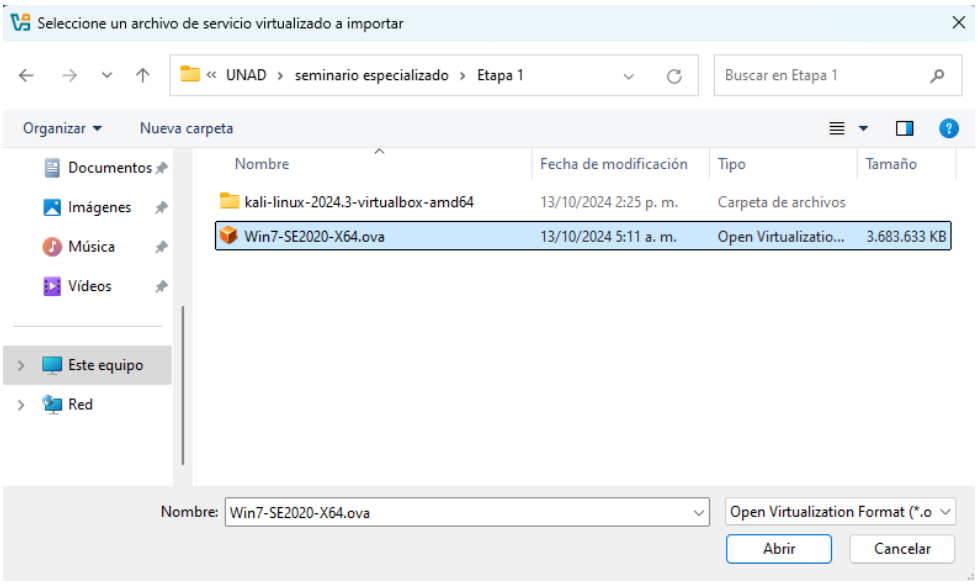
Figura 3 Descarga Kali Linux



Fuente: Elaboración propia

Se lleva a cabo la importación del archivo Windows en el entorno virtualizado de VirtualBox.

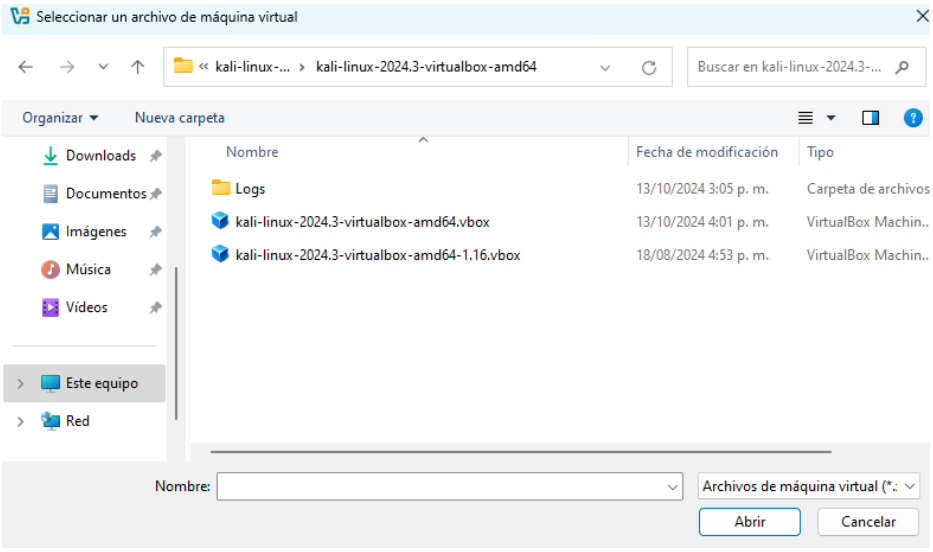
Figura 4 Importación archivo .ova Windows 7



Fuente: Elaboración propia

Se lleva a cabo la importación del archivo Kali Linux en el entorno virtualizado de VirtualBox.

Figura 5 Importacion Kali Linux



Fuente: Elaboración propia

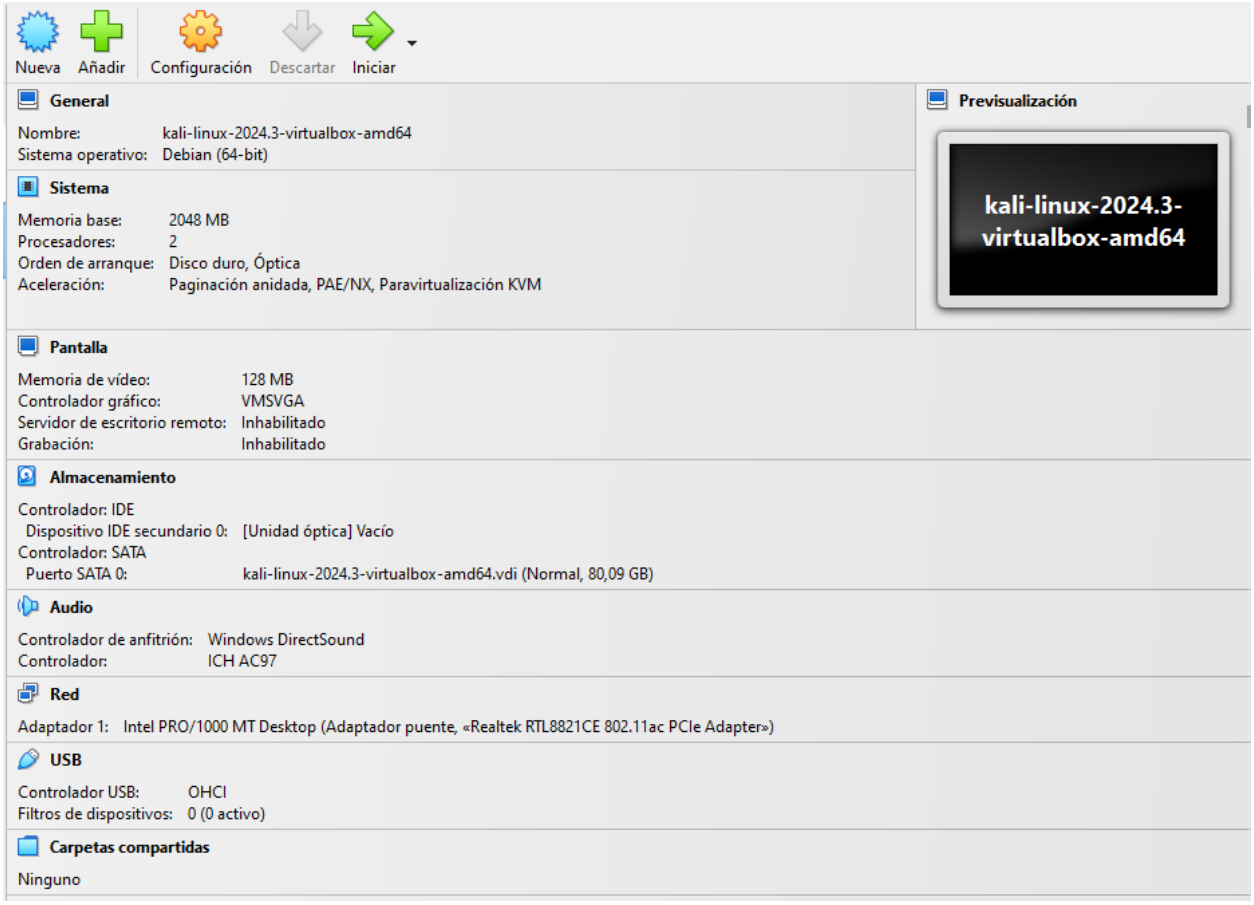
Después de importar al entorno virtualizado, verificamos los aspectos técnicos de la máquina virtual de Windows, cabe recordar que las redes se dejaron en modo adaptador puente para que puedan comunicarse entre sí:

Figura 6 Detalle técnico maquina Windows

Fuente: Elaboración propia

Después de importar al entorno virtualizado, verificamos los aspectos técnicos de la maquina virtual de Kali Linux

Figura 7 Detalle técnico máquina virtual Kali Linux



Fuente: Elaboración propia

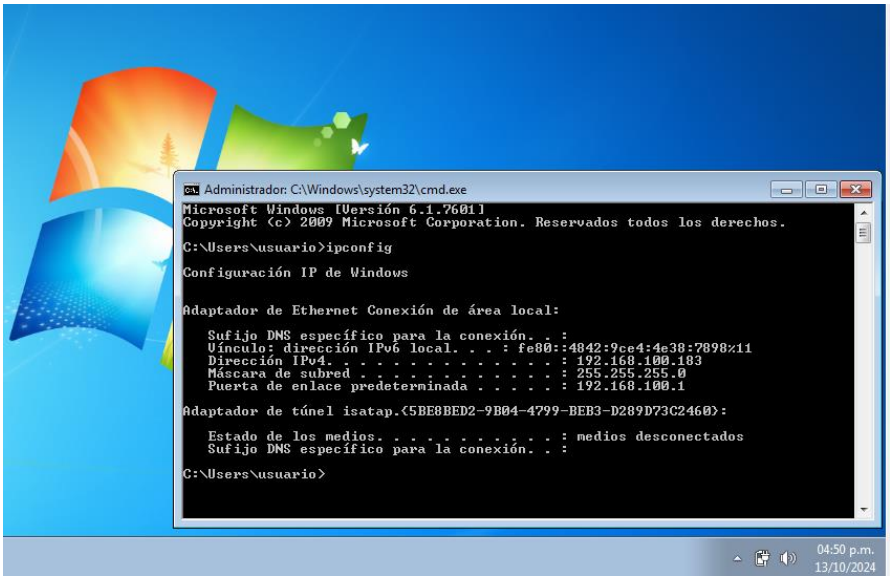
Para confirmar la conexión de red, comprobamos la dirección IP de la máquina virtual y la iniciamos para ver cómo funciona.

Tabla 2 Direcciones IP

Máquina Virtual	Dirección IP
Windows 7	192.168.100.183
Kali Linux	192.168.100.183

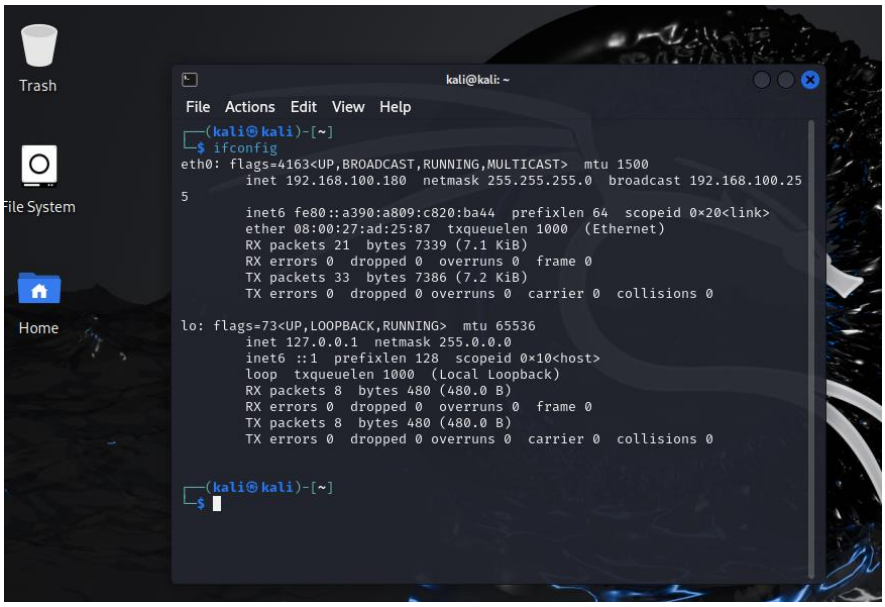
Fuente: Elaboración propia

Figura 8 Inicio Windows 7



Fuente: Elaboración propia

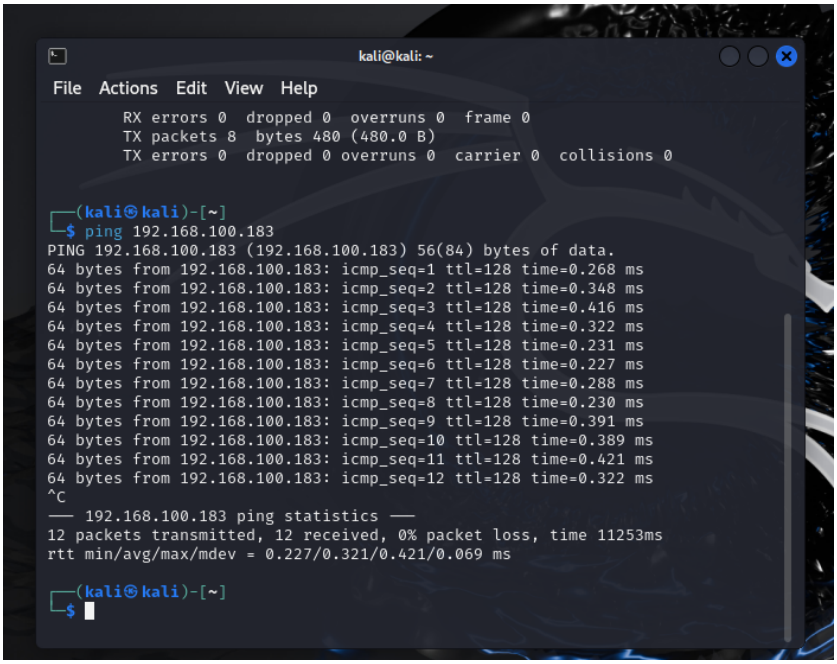
Figura 9 Inicio Kali Linux



Fuente: Elaboración propia

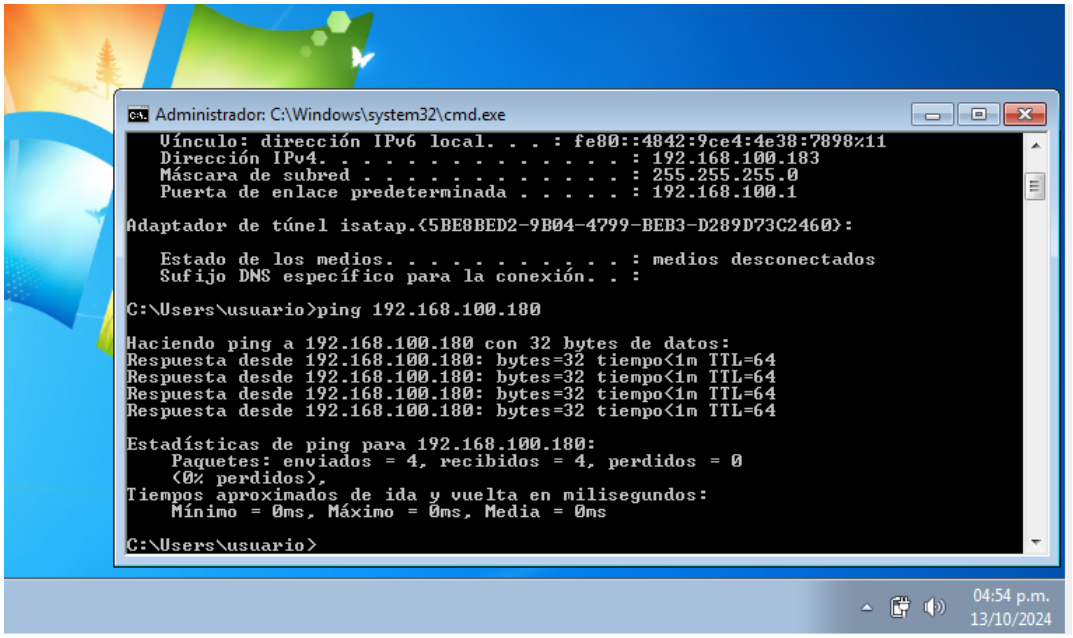
Seguidamente realizamos pruebas de ping desde Kali Linux al Windows 7 y viceversa con resultados exitosos como se evidencian en la imagen:

Figura 10 Comunicación entre Kali Linux y Windows



Fuente: Elaboración propia

Figura 11 Comunicación entre Windows y Kali Linux



Fuente: Elaboración propia

3 DESARROLLO DE TRABAJO – ETAPA 2

3.1 Conducta ética y cumplimiento legal

3.1.1 Análisis anexo 2 y anexo 3

3.1.1.1 Escenario 2

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Es fundamental que los contratos en las empresas sean preparados por un abogado activo dentro de la organización y con experiencia en el área de contratación. En este contexto, el contrato del escenario 2 fue elaborado por un abogado que ya no forma parte de la empresa y que fue despedido debido a su implicación en actividades sospechosas e ilegales. Esto revela una falta de supervisión por parte de la alta dirección, que debería garantizar la transparencia en el cumplimiento de las funciones, revisando minuciosamente la documentación generada por este abogado[13].

3.1.1.2 Acuerdo de confidencialidad

En relación con el anexo 3, que corresponde al acuerdo de confidencialidad, se identifican varias inconsistencias, descritas a continuación:

En la **primera cláusula**, se menciona: "se obliga a no divulgar directa o indirectamente la información confidencial ni sobre procesos ilegales dentro de CyberFort Technologies". Esto sugiere que la empresa restringe al profesional de informar sobre actos ilegales detectados, lo

[13] *¿Por qué es importante contar con un abogado para redactar o revisar un contrato? - Carlota Gonzàlez*. (2021, April 14). Carlota Gonzàlez. https://carlotagonzalez.com/abogado-redactar-revisar-contrato/

cual incumple con los principios éticos profesionales, ya que impide que actúe frente a situaciones ilícitas en la organización.

La no divulgación de material sin autorización previa se menciona en el punto 9 del mismo apartado. Esto debería dejar claro que si un organismo judicial solicita el material con fines de investigación, debe ser suministrado.

> **Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 – Acuerdo: acuerdo, deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.**

Tras la lectura de la **Ley 1273 de 2009**[14] y del acuerdo de confidencialidad, se pueden identificar las siguientes irregularidades:

En la **cláusula segunda**, se observa una posible vulneración del **Artículo 269A** sobre “acceso abusivo a un sistema informático". Esta cláusula define la información confidencial de forma amplia, incluyendo información societaria, técnica, jurídica, financiera, comercial, de mercado, entre otros datos secretos, tales como “datos de chuzadas, interceptación de información, y accesos abusivos a sistemas informáticos”.

Es claro que en el anexo 3 se viola el **Artículo 269B**, relativo a la "Obstaculización ilegítima de sistema informático", ya que impide al profesional divulgar procesos ilegales.Finalmente, se menciona la manipulación de la información en varias de sus cláusulas, lo cual podría constituir una infracción al **Artículo 269F**, referente a la "Violación de datos

[14] *Ley 1273 de 2009 - Gestor Normativo*. (2015, December). Funcionpublica.gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

personales". Manipular esta información en beneficio propio y sin denunciar actos ilegales puede contribuir a un manejo inadecuado de los datos.

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

Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros.

Como profesional en ingeniería de sistemas y experto en seguridad de la información, no sería conveniente aceptar o firmar dichas cláusulas en la revisión del contrato laboral, ya que el contrato es opaco y no se apega a la normatividad colombiana, lo cual representa un riesgo para el profesional y es antiético en varios aspectos. Después de revisar cada una de las cláusulas del contrato, se encuentra que la mayoría del Código de Ética del COPNIA no permite hacerlo.

3.1.2 Análisis anexo 7

Deberá analizar el caso problema "Ciber espionaje y Ética en CyberFort Technologies" (Anexo 7 - Escenario 2), redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar y dar respuesta los siguientes interrogantes:

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

Acceso a Información Sensible y Garantías contra el Abuso

Las empresas de ciberseguridad necesitan cierto grado de acceso a información sensible para realizar auditorías completas y efectivas, ya que solo así pueden identificar vulnerabilidades que los atacantes podrían explotar. Sin embargo, este acceso debe estar estrictamente regulado y limitado al alcance de la auditoría. Para prevenir abusos:

Contratos estrictos y acuerdos de confidencialidad: El contrato debe detallar el acceso permitido, con sanciones claras en caso de abuso.

Acceso segmentado y temporal: Limitar el acceso a datos únicamente mientras dure la auditoría, usando permisos específicos y revisables, además de eliminar el acceso una vez concluida la evaluación.

Tecnología de monitoreo y auditoría interna: Las herramientas de seguimiento pueden registrar la actividad de los auditores, detectando accesos indebidos en tiempo real.

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

Mecanismos de Supervisión y Control en Empresas de Ciberseguridad

Para evitar el uso no autorizado de herramientas avanzadas, las empresas de ciberseguridad deben implementar los siguientes mecanismos:

Políticas de ética estrictas y capacitación continua: Formar a los empleados sobre la responsabilidad ética en la manipulación de datos sensibles y reforzar la cultura ética en la organización.

Monitoreo en tiempo real y auditoría interna: Implementar herramientas que registren todas las actividades de los empleados mientras acceden a información sensible, con supervisión regular por un equipo de auditoría interna.

Autorización multinivel para uso de herramientas avanzadas: Restringir el uso de herramientas forenses a personal autorizado y requerir una validación por parte de supervisores para acciones sensibles.

Acceso basado en el principio de privilegio mínimo: Los empleados deben tener solo el acceso necesario para realizar su tarea específica.

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

Si se descubre que una empresa de ciberseguridad contratada ha participado en ciber espionaje, es crucial actuar para restaurar la confianza:

Investigación exhaustiva y acciones legales: Llevar a cabo una investigación rigurosa y, si corresponde, aplicar sanciones legales contra la empresa y los empleados implicados.

Exclusión de la empresa en futuras contrataciones: Considerar la posibilidad de prohibir la contratación de esta empresa para servicios sensibles en el futuro.

Implementación de nuevas salvaguardas en contratos futuros: Reforzar los acuerdos de confidencialidad y los controles de acceso en futuras contrataciones, exigiendo auditorías externas regulares.

Transparencia con el público y las partes interesadas: Informar sobre las medidas tomadas para prevenir incidentes similares y comprometerse a mejorar la seguridad.

Estas medidas, cuando se combinan, ayudan a fomentar una cultura ética dentro de las empresas de ciberseguridad y a proteger los intereses de los clientes.

4 DESARROLLO DE TRABAJO – ETAPA 3

4.1 Herramientas de Software

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

Fase de recolección de información: Se recibe la solicitud que describe lo sucedido, lo que da pie al análisis de la información proporcionada. Sé ha detectado una filtración de información originada desde uno de los dispositivos dentro de la organización.

Según la información a la que se tiene acceso actualmente, el ordenador hackeado está utilizando el sistema operativo Windows 7 de la víctima para lanzar una aplicación. Es importante señalar que Windows 7 dejó de admitir actualizaciones de seguridad a partir de enero de 2020. Microsoft fomentó el cambio a Windows 11 cuando dejó de dar soporte a este sistema operativo por considerarlo obsoleto.[15].

[15] Microsoft. (2023). *Hagamos una copia de seguridad de tu PC*. Windows. https://www.microsoft.com/es-co/windows/end-of-support?r=1#:~:text=Ha%20finalizado%20el%20soporte%20de,14%20de%20enero%20de%202020.

El uso continuo de Windows 7 incrementa los riesgos, ya que las vulnerabilidades nuevas descubiertas pueden ser explotadas, comprometiendo la seguridad de la información. Esto es particularmente crítico, ya que muchas empresas y usuarios aún no han actualizado sus sistemas operativos.

Fase de Búsqueda de vulnerabilidades

En los datos suministrados se valida una aplicación denominada Rejetto v. 2.3[16]. Este servidor web HTTP para compartir archivos fue creado como una utilidad práctica y libre de malware. Sin embargo, presenta un fallo que podría poner en peligro su seguridad. Tras el estudio de casos relacionados y la investigación en bases de datos de vulnerabilidades, se descubrieron dos vulnerabilidades para esta aplicación.

Existen advertencias sobre la vulnerabilidad actual en el programa Rejetto versión 2.3 y versiones anteriores dentro de las páginas procedentes de fuentes fiables:

[16] Arseniy Sharoglazov. (2023). *Rejetto HTTP File Server 2.3m Unauthenticated RCE*. Mohemiv.com. https://mohemiv.com/all/rejetto-http-file-server-2-3m-unauthenticated-rce/

Figura 12 Vulnerabilidad Rejetto

Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287)

Gravedad CVSS v3.1: CRÍTICA

Tipo: CWE-94 Control incorrecto de generación de código (Inyección de código)

Fecha de publicación: 07/10/2014

Última modificación: 26/02/2021

Descripción

La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (también conocido como HFS o HttpFileServer) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.

Impacto

Vector 3.x CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Puntuación base 3.x 9.80

Gravedad 3.x CRÍTICA

Vector 2.0 AV:N/AC:L/Au:N/C:C/I:C/A:C

Puntuación base 2.0 10.00

Gravedad 2.0 ALTA

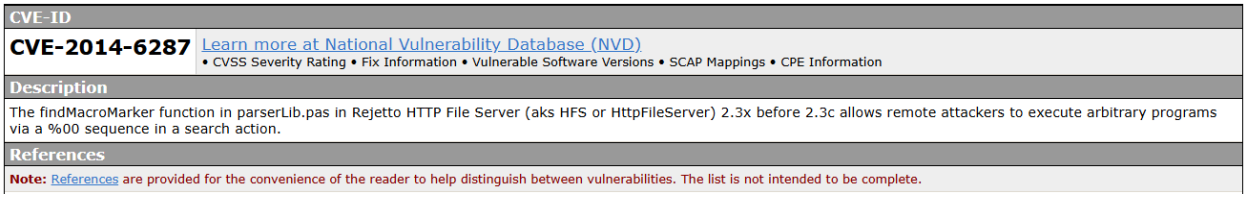
Productos y versiones vulnerables

CPE	Desde	Hasta
cpe:2.3:a:rejetto:http_file_server:*:*:*:*:*:*:*:*	**2.3** *(incluyendo)*	**2.3c** *(excluyendo)*

Fuente: *CVE-2014-6287 | INCIBE-CERT | INCIBE*. (2014). Incibe.es.

https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-6287

Figura 13 Vulnerabilidad 2014-6287



CVE-ID

CVE-2014-6287 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The findMacroMarker function in parserLib.pas in Rejetto HTTP File Server (aks HFS or HttpFileServer) 2.3x before 2.3c allows remote attackers to execute arbitrary programs via a %00 sequence in a search action.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Fuente: *CVE - CVE-2014-6287*. (2014). Mitre.org. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

En la versión 2.3x de Rejetto, anteriores a la 2.3c, se detectó una vulnerabilidad en la función *findMacroMarker* dentro del archivo *parserLib.pas*[17]. Esta falla ayuda a los atacantes controlar programas de manera brusca utilizando un patron denominado "*%00"* en una comprobación de búsqueda. Dicha vulnerabilidad podría ser aprovechada mediante un exploit que dé lugar a la ejecución de una shell reversa y a la apertura de Meterpreter.

Además, *Rejetto v. 2.3* y versiones previas contienen otras dos vulnerabilidades adicionales que están documentadas públicamente.

Figura 14 Vulnerabilidad Comment en Rejetto

Vulnerabilidad en la caracteristica File Comment en Rejetto HTTP File Server (CVE-2014-7226)

Gravedad CVSS v2.0: ALTA

Tipo: CWE-94 Control incorrecto de generación de código (inyección de código)

Fecha de publicación: 10/10/2014

Última modificación: 10/10/2014

Descripción

La caracteristica File Comment en Rejetto HTTP File Server (hfs) 2.3c y anteriores permite a atacantes remotos ejecutar código arbitrario mediante la subida de un fichero con ciertas secuencias inválidas de bytes UTF-8 que se interpretan como símbolos de macros ejecutables.

Impacto

Vector 2.0 AV:N/AC:L/Au:N/C:P/I:P/A:P

Puntuación base 2.0 7.50

Gravedad 2.0 ALTA

Productos y versiones vulnerables

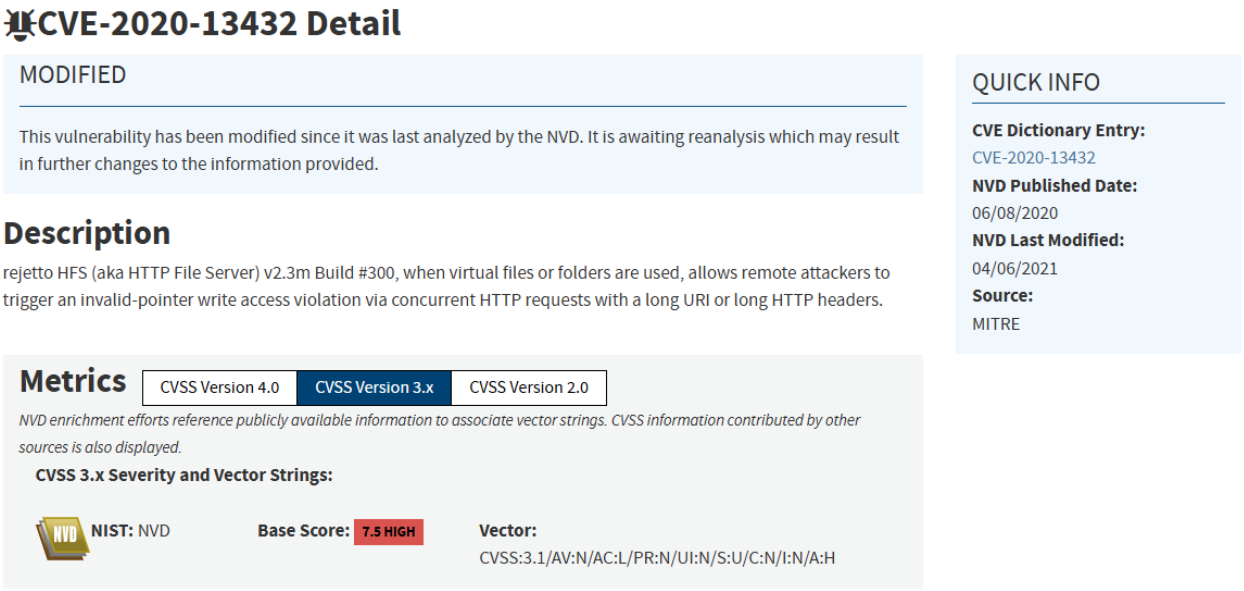
CPE	Desde	Hasta
cpe:2.3:a:rejetto:http_file_server:*:*:*:*:*:*:*:*		2.3c *(incluyendo)*

Fuente: *CVE-2014-7226 | INCIBE-CERT | INCIBE*. (2014). Incibe.es. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-7226

En *Rejetto 2.3*y versiones de antes, la función de comentarios de archivo es vulnerable porque un atacante puede aprovechar esta falla al manipular el archivo de manera que los bytes no válidos se conviertan en código que el sistema ejecuta. Esto podría permitir la ejecución de comandos arbitrarios en el sistema afectado, lo que representa un grave riesgo de seguridad. Esta vulnerabilidad podría ser explotada para ejecutar scripts maliciosos, inyectar código, o incluso tomar control del sistema de manera remota.

[17] *NotCVE - vendor:"Rejetto."* (2024). Notcve.org. https://notcve.org/search.php?page=1&query=vendor%3A%22Rejetto%22

Figura 15 Vulnerabilidad 2020-13432



Fuente: *NVD - CVE-2020-13432*. (2020). Nist.gov. https://nvd.nist.gov/vuln/detail/CVE-2020-13432

Esta vulnerabilidad relacionada con los archivos virtuales permite un acceso no autorizado a la memoria del sistema. Esto sucede cuando se envían solicitudes HTTP simultáneas que incluye un **URI largo**, lo que puede sobrescribir la memoria de manera no controlada. Este comportamiento genera un acceso por escritura en punteros no válidos, lo cual puede corromper la memoria o permitir que los atacantes ejecuten código arbitrario, alterando el funcionamiento normal del servidor.

Fase de Explotación de Vulnerabilidades:

En los datos suministrados se valida una aplicación denominada Rejetto v. 2.3. Este servidor web HTTP para compartir archivos fue creado como una utilidad práctica y libre de malware. Sin embargo, presenta un fallo que podría poner en peligro su seguridad.

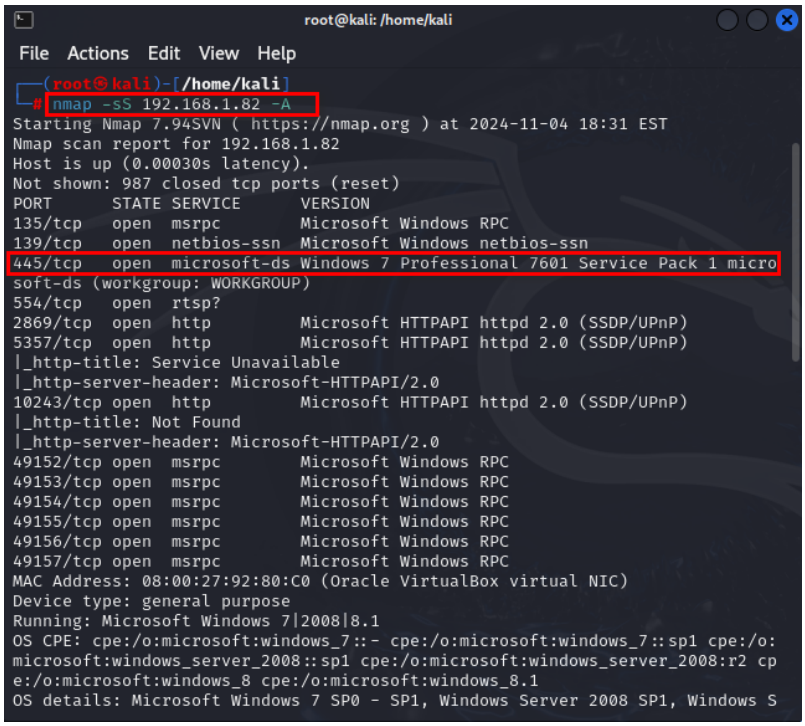
Existen advertencias sobre la vulnerabilidad actual en el programa Rejetto versión 2.3 y versiones anteriores dentro de las páginas procedentes de fuentes fiables:

Tabla 3 Lista Direcciones IP maquinas

Maquina	Dirección IP
Kali Linux	192.168.1.34
Windows 7	192.168.1.82

Fuente: Elaboración propia

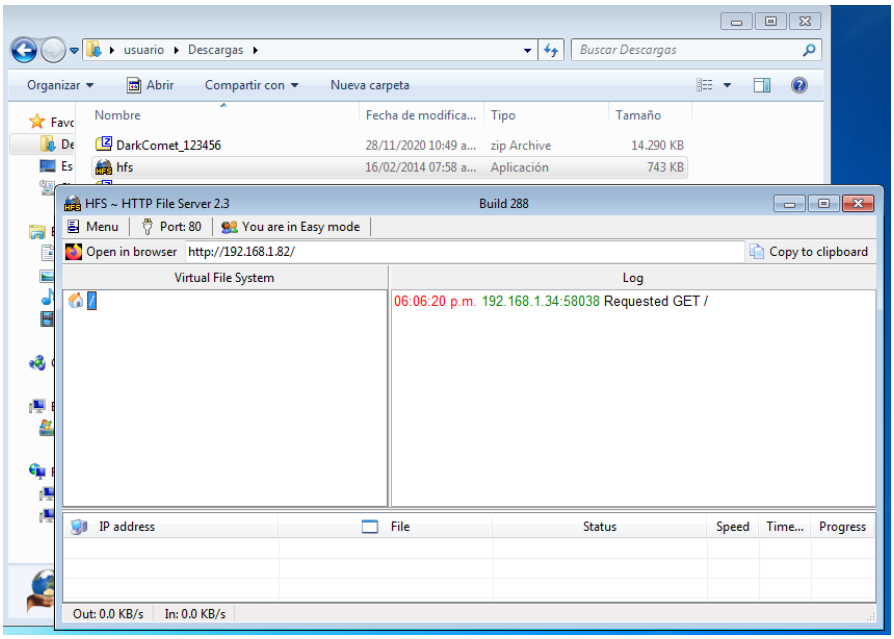
Figura 16 Escaneo puertos Windows 7



Fuente: Elaboración propia

Iniciamos con instalar la aplicación vulnerable en el sistema operativo Windows 7:

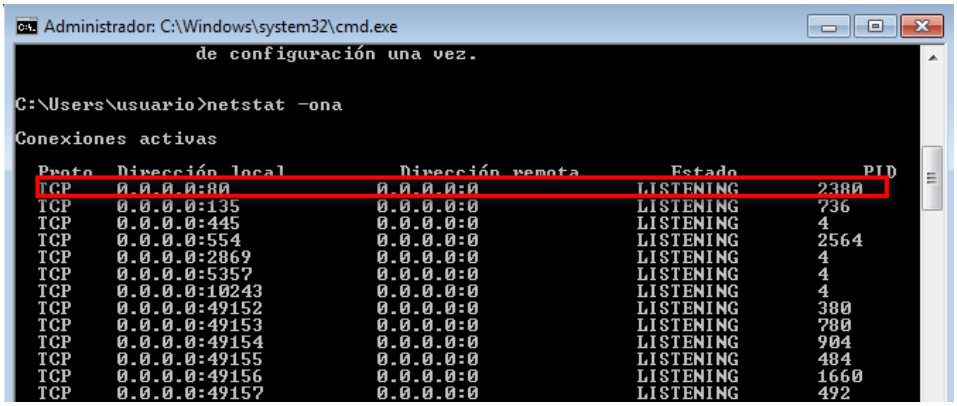
Figura 17 Instalación aplicación vulnerable



Fuente: Elaboración propia

Seguidamente vemos que puertos se están escuchando en la maquina victima y observamos que el puerto 80 esta abierto:

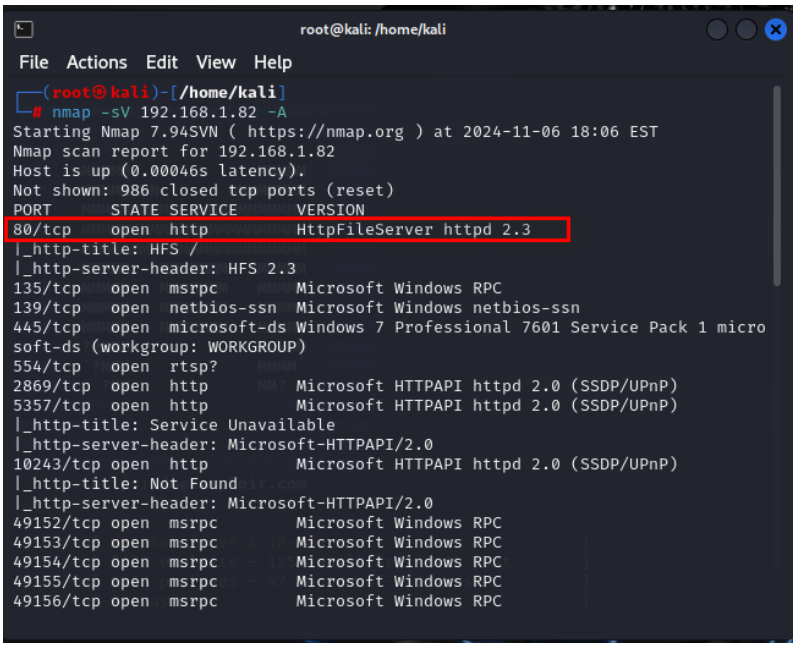
Figura 18 Uso netstat



Fuente: Elaboración propia

Luego de que ya la aplicación vulnerable (Http file server 2.3) este corriendo en el Windows, escaneamos nuevamente las vulnerabilidades para identificar que puertos están abierto y con que servicio:

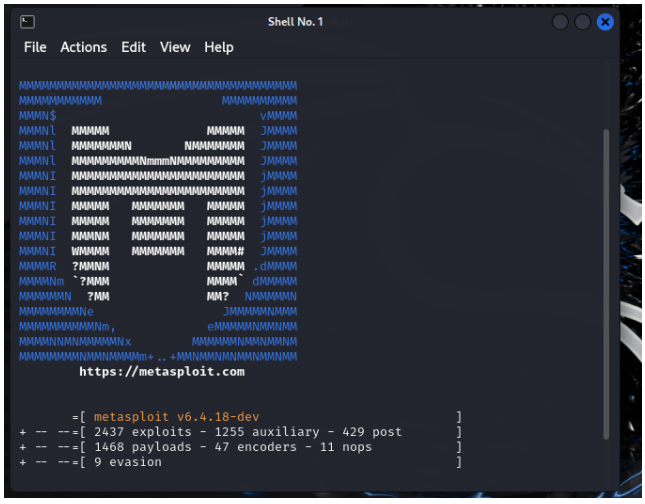
Figura 19 Escaneo de vulnerabilidades



Fuente: Elaboración propia

Comprobamos que mediante el puerto 80 está corriendo la aplicación vulnerable, lo cual empezamos con la explotación mediante la herramienta metasploit:

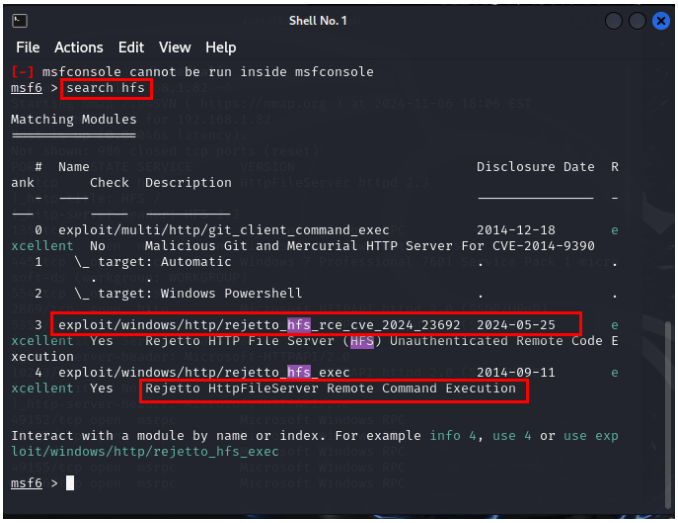
Figura 20 Uso metasploit



Fuente: Elaboración propia

Dentro del metasploit ingresar search hfs que se utiliza para buscar exploits, payloads o módulos relacionados con "hfs" (en este caso, HTTP File Server) dentro de la base de datos de Metasploit:

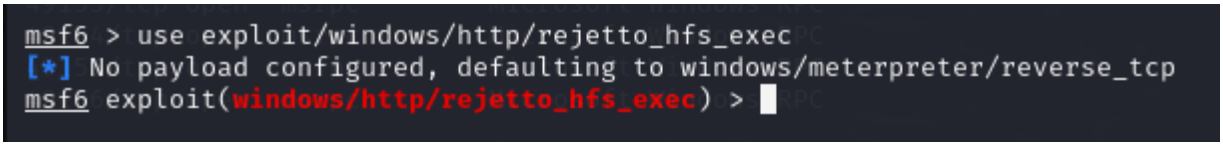
Figura 21 Búsqueda vulnerabilidad especifica



Fuente: Elaboración propia

Seguidamente escribimos para carga un módulo específico para explotar una vulnerabilidad en el software **HTTP File Server** (HFS) versión 2.3,y se evidencia que el módulo de exploit ha detectado que no se ha configurado un payload explícitamente, por lo que Metasploit está utilizando el payload predeterminado, que es windows/meterpreter/reverse_tcp:

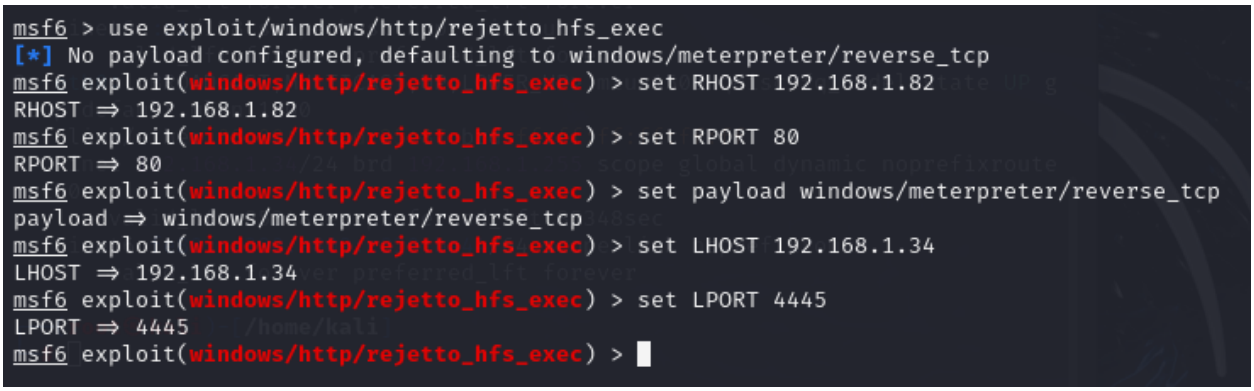
Figura 22 búsqueda payload



Fuente: Elaboración propia

Iniciamos Configurando el módulo con la dirección IP y el puerto de tu máquina Windows 7, la ip del Kali y el puerto que vamos a usar:

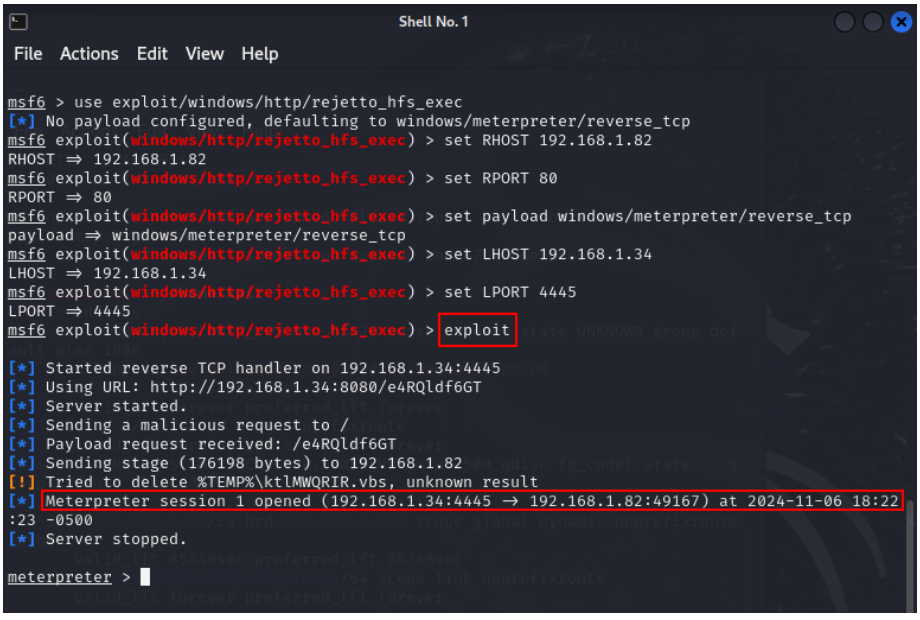
Figura 23 Configuración modulo



Fuente: Elaboración propia

Ejecutamos el módulo de explotación que hemos configurado previamente. Este paso es el proceso de explotación de una vulnerabilidad en la maquina(Windows 7) y se evidencia que hemos atacado exitosamente a la victima:

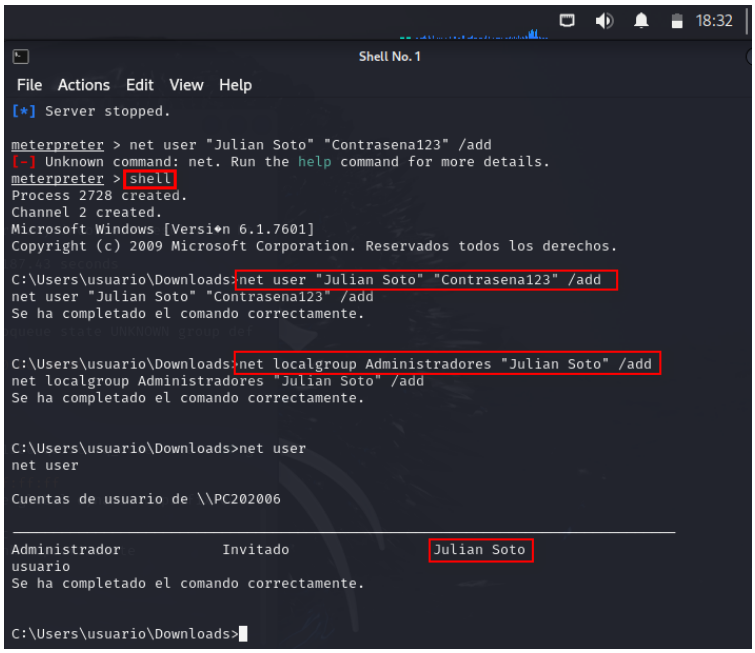
Figura 24 uso exploit



Fuente: Elaboración propia

Ya teniendo el ingreso a la maquina, podemos empezar a navegar sus archivos e incluso proceder con la creación de un usuario administrador:

Figura 25 Escalación de privilegios



Fuente: Elaboración propia

Fase Post-explotación:

En esta etapa, tras haber evidenciado el método y la forma en que se ejecuta el ataque y validada la fuga de información, se procede a analizar el alcance potencial de este acceso no autorizado. Se realizan pruebas para intentar acceder a archivos confidenciales, obtener credenciales de usuarios, elevar privilegios a nivel administrador, crear usuarios legítimos y llevar a cabo acciones como copiar, modificar o eliminar datos. Durante este proceso, se obtiene acceso al sistema comprometido como administrador, lo que posibilita la recopilación de toda la información almacenada en el dispositivo.

Figura 26 Comprobación escalación privilegios

Fuente: Elaboración propia

Fase de Informe:

Tras analizar la información inicial, investigar las vulnerabilidades potenciales y realizar pruebas en un entorno de laboratorio que simula la fase real, el resultado es claro: No se estaban implementando las políticas y controles adecuados para garantizar la protección de la información. Es crucial que las aplicaciones, especialmente aquellas que interactúan con información sensible, sean sometidas a un proceso riguroso de evaluación y prueba antes de ser implementadas. Esto implica no solo la revisión del código y las configuraciones de seguridad, sino también la realización de pruebas de penetración y auditorías de seguridad periódicas para identificar y corregir vulnerabilidades, lo hacía susceptible a vulnerabilidades y múltiples fallos de seguridad. Asimismo, carecía de mecanismos adicionales de protección, limitándose únicamente a las medidas básicas proporcionadas por el sistema operativo, el cual ya no recibe actualizaciones de seguridad por parte de su proveedor, en este caso Microsoft.

4.2 Datos E Información Del Anexo 4

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows

Se ha detectado una fuga de datos en la organización, proveniente de uno de los dispositivos de una de las áreas. De acuerdo con los informes preliminares, el equipo comprometido ejecuta la aplicación Rejetto v. 2.3 sobre un sistema operativo Windows 7. Rejetto v. 2.3 es un servidor web HTTP destinado al intercambio de archivos, con la intención de ser una herramienta confiable y libre de malware. Sin embargo, presenta varias vulnerabilidades graves que podrían ser explotadas.

La aplicación presenta varios fallos de seguridad que pueden ser aprovechados por atacantes, lo que podría resultar en la ejecución de una shell inversa o el acceso a una sesión de Meterpreter. En un acceso remoto típico, el usuario se conecta como cliente, y la máquina de destino actúa como servidor, escuchando las solicitudes entrantes. Sin embargo, es posible revertir este proceso, haciendo que la máquina comprometida inicie la conexión hacia el usuario, quien escucha en un puerto específico.

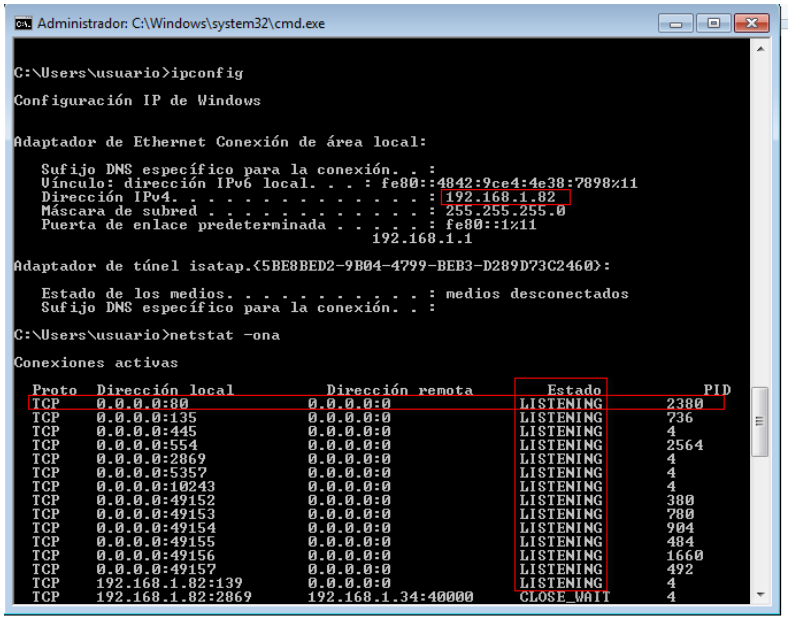
Dado que las configuraciones de cortafuegos normalmente sólo permiten conexiones a través de puertos designados, los atacantes recurren a las shell inversas. Por ejemplo, los servidores web suelen permitir conexiones en los puertos 80 y 443, lo que impide que el shell de un servidor comprometido se utilice para escuchar directamente. Es arriesgado dejar puertos abiertos o a la escucha, ya que esto deja sistemas y aplicaciones importantes -incluidos el correo electrónico, las bases de datos y el almacenamiento de datos- expuestos a los ataques de

herramientas de exploración como Metasploit, Nessus o Nmap. La seguridad de la información corre un grave riesgo cuando las políticas de puertos no se controlan adecuadamente.

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

El equipo cuenta un sistema antiguo y tiene funciones activas que permiten recibir conexiones externas, ya que la barrera de seguridad no las está bloqueando.

Figura 27 IPCONFIG

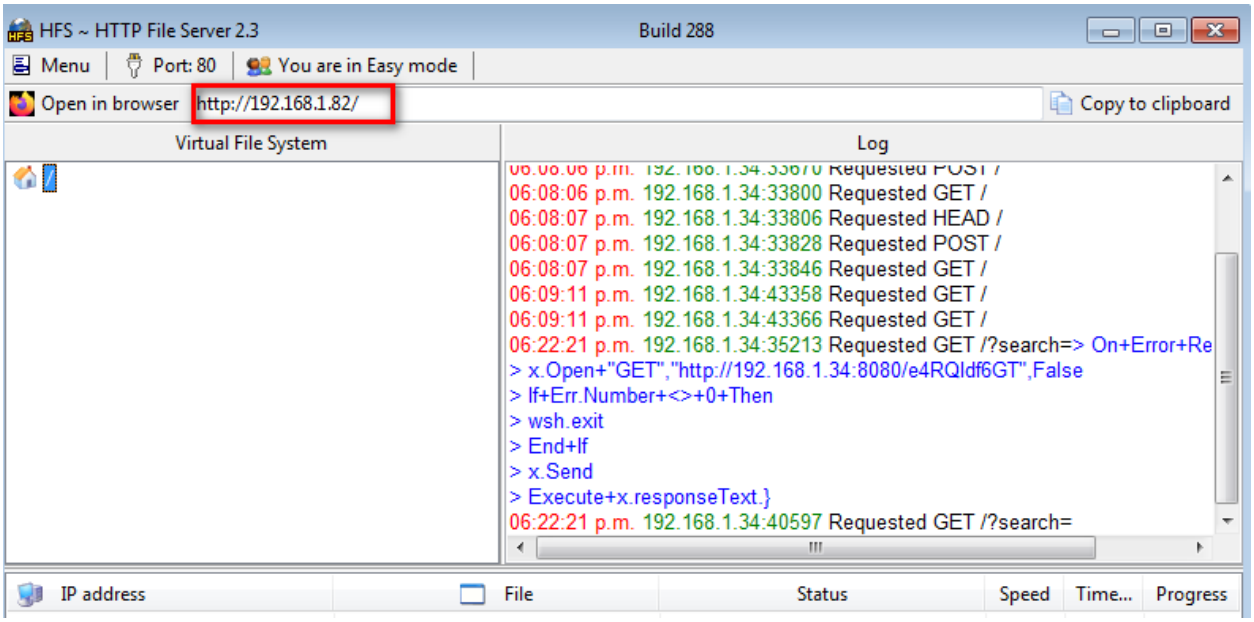


Fuente: Elaboración propia

Al ejecutar el comando **ipconfig**, se puede confirmar la dirección IP asignada a la máquina, en este caso **192.168.1.82**, lo que permite identificar la red en la que está ubicada la máquina. Posteriormente, con el uso del comando **netstat**, es posible analizar los puertos abiertos en el sistema y verificar aquellos que se encuentran en estado **LISTENING**, lo que indica que están esperando conexiones entrantes. Si el servidor expuesto está ejecutando una aplicación vulnerable, esta podría ser explotada para abrir puertos adicionales sin autorización. Este comportamiento puede ser detectado mediante **netstat**, que muestra la apertura de puertos como

el **80**, utilizado normalmente para tráfico web (HTTP). Esta situación implica un riesgo considerable, ya que la apertura de puertos no autorizados en el servidor expone la máquina a posibles ataques, permitiendo a los atacantes interactuar con el sistema a través de servicios no previstos. Identificar estos puertos es crucial para prevenir accesos no deseados y proteger la infraestructura de la red.

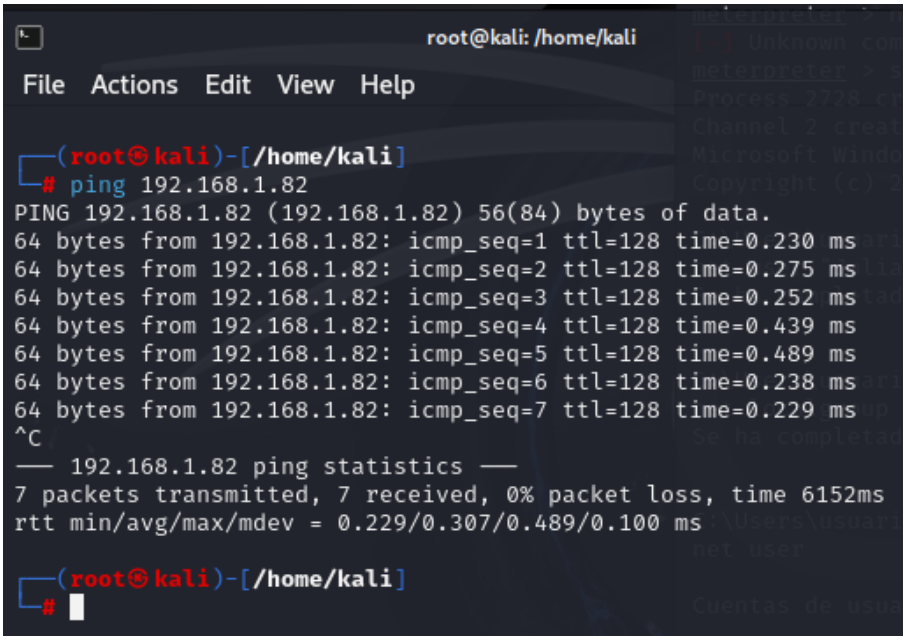
Figura 28 Aplicativo en ejecución



Fuente: Elaboración propia

En este escenario, un atacante quu use **Kali Linux** podría acceder a la máquina objetivo, dado que ambas están en la misma red, tal como se muestra en la imagen siguiente.

Figura 29 Comunicación maquinas



Fuente: Elaboración propia

Con la herramienta *Nmap*, un atacante puede identificar los puertos abiertos en el equipo y los servicios asociados que los tienen en ejecución

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

Un atacante puede buscar vulnerabilidades asociadas a una aplicación concreta si conoce la versión del software que está funcionando en un ordenador remoto. Es posible explotar esas vulnerabilidades si no han sido parcheadas. En este escenario de prueba se explotará una vulnerabilidad conocida que permite a un atacante ejecutar código arbitrario en el servidor que aloja la aplicación. El dispositivo con la dirección IP 192.168.1.82 es el objetivo. Al cargar archivos con secuencias de bytes UTF-8 incorrectas, que se interpretan como macros ejecutables, los atacantes pueden utilizar la funcionalidad de comentario de archivos en las versiones 2.3 y

posteriores de Rejetto HTTP File Server (HFS) para ejecutar código arbitrario, como se ve en la imagen siguiente.

Figura 30 Explicación explotación

Fuente: Elaboración propia

Explicación del Ataque

El ataque de reverse shell compromete la seguridad de una máquina Windows al establecer una conexión remota con el atacante, quien puede controlar el sistema de la víctima de manera invisible.El atacante, usando Kali Linux, configura un script o programa como FTP o Regetto para crear una conexión en espera (listener) que estará atenta a recibir una conexión desde la máquina Windows objetivo. El atacante envía un exploit o código malicioso que se ejecuta en la máquina Windows. Este código se conecta de vuelta al listener del atacante, abriendo una puerta de enlace (reverse Shell) que permite el acceso remoto. Una vez establecida la conexión, el atacante puede ejecutar comandos en la máquina Windows como si estuviera sentado frente a ella. Esto puede incluir el robo de información, la instalación de programas adicionales, la manipulación de archivos y escalación de usuarios, sin que el usuario lo detecte fácilmente.

Efecto del Ataque en la Máquina Windows

Pérdida de Control: El sistema Windows queda bajo el control del atacante. El usuario no se da cuenta de lo que está ocurriendo, pero el atacante puede realizar cualquier acción que un administrador del sistema podría llevar a cabo.

Riesgos de Seguridad: El atacante puede extraer información confidencial, modificar datos, instalar malware, o incluso dañar los componentes del sistema.

Invisibilidad: El ataque es sigiloso, ya que el código malicioso se ejecuta en segundo plano, y la conexión con el atacante no es evidente para el usuario común.

Representación Gráfica del Ataque

En el lado izquierdo, se muestra la máquina del atacante (Kali Linux), preparada con un listener para recibir la conexión. Una flecha señala hacia la máquina Windows (a la derecha), representando el envío del exploit.Una vez que el exploit se ejecuta, una segunda flecha conecta de vuelta la máquina Windows al atacante, indicando la apertura del reverse Shell.

Ilustración de Control Remoto:

La máquina Windows es representada con un símbolo de alerta, mostrando que el atacante tiene acceso a la línea de comandos.

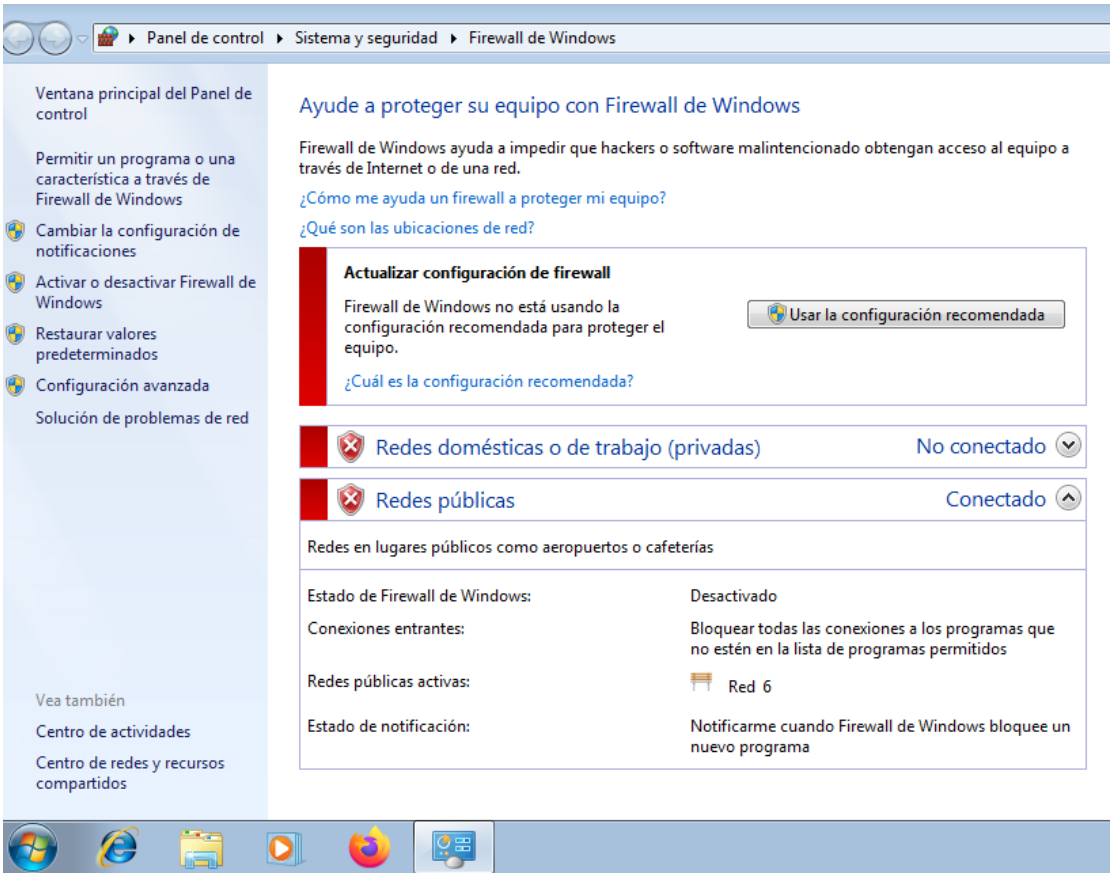
Se incluyen íconos de archivos y datos que el atacante podría manipular.

5 DESARROLLO DE TRABAJO – ETAPA 4

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

Primero, se debe identificar el tipo de ataque en curso y coordinar con el grupo de Red Team para confirmar las vulnerabilidades presentes en la infraestructura. Con base en su análisis, se detectaron múltiples fallas, destacando la desactivación de los firewalls y el antivirus.

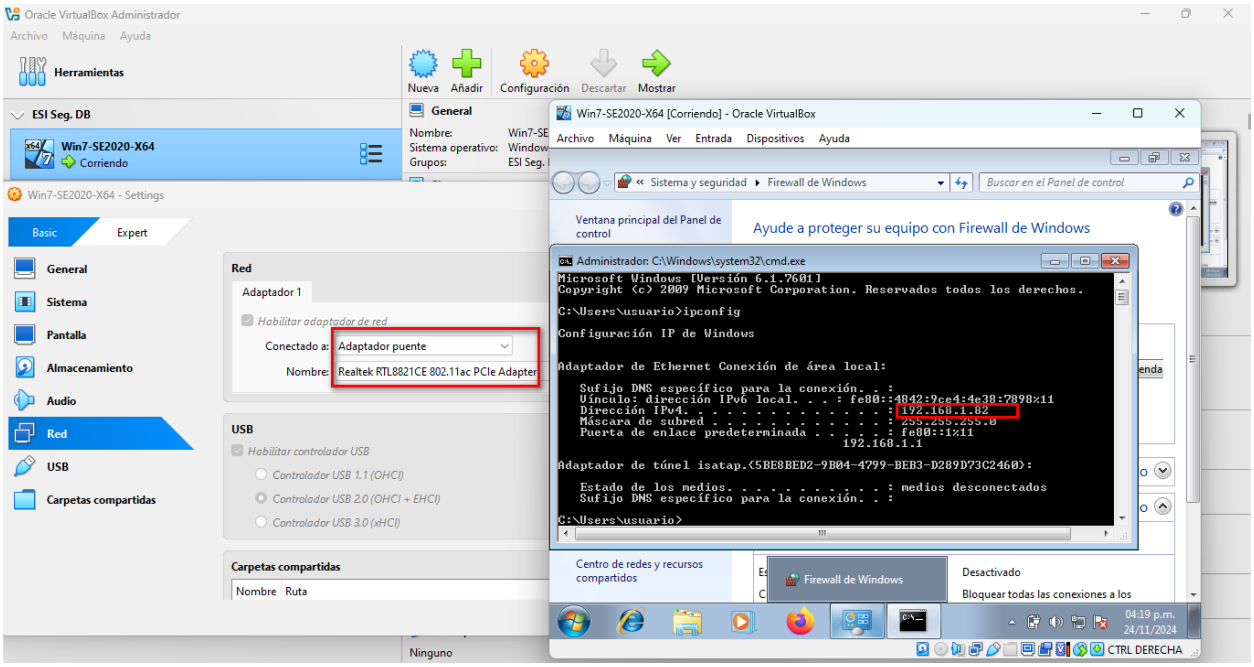
Figura 31 Verificación firewall Windows



Fuente: Elaboración propia

A continuación, se procede a coordinar con el grupo Red Team para verificar como están las conexiónes de red de cada máquina, enfocándose en validar la red de las máquinas con Windows 7, en particular la correspondiente a la dirección IP 192.168.1.82.

Figura 32 Validación conexión red maquina Windows



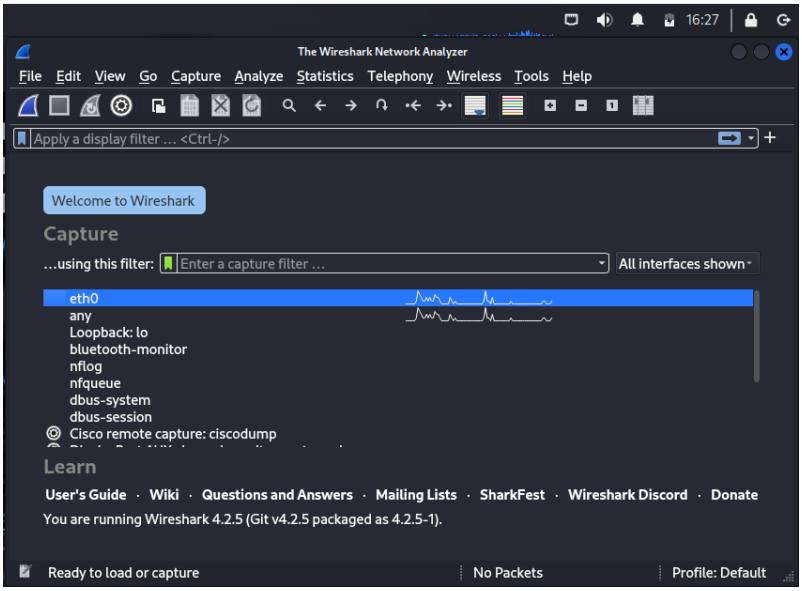
Fuente: Elaboración propia

Posteriormente, se ejecutaría un sniffer en cada computadora afectada con el fin de monitorear los datos que circulan en la red. Estas herramientas permiten trazar, decodificar y analizar los campos de uno o más paquetes, resultandos útiles para diagnosticar problemas de red, identificar intentos de explotación y monitorear sistemas comprometidos. Una opción recomendada es Wireshark[18], una herramienta ampliamente utilizada que permite un análisis detallado de la comunicación de red y la supervisión de paquetes tanto de entrada como de

[18] Luz, S. D. (2020, July 4). *Cómo usar Wireshark para capturar y analizar el tráfico de red*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/

salida. Desde mi estación Kali, podría utilizar esta herramienta para examinar el tráfico en tiempo real, con el objetivo de poder determinar el tipo de ataque y la información que se intentan extraer.

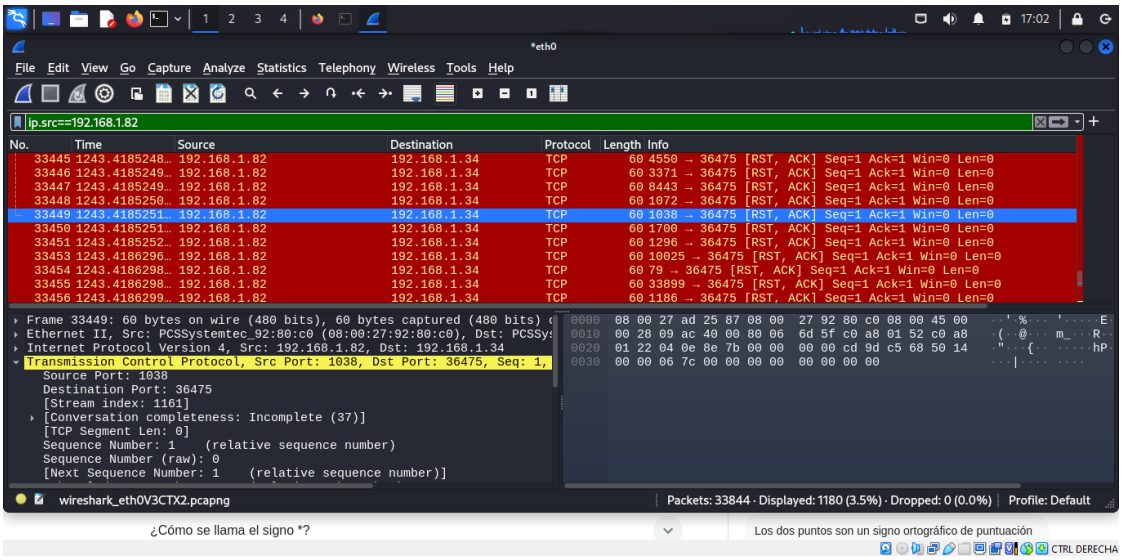
Figura 33 Herramienta Wireshark



Fuente: Elaboración propia

Aquí se muestra el sniffer en ejecución:

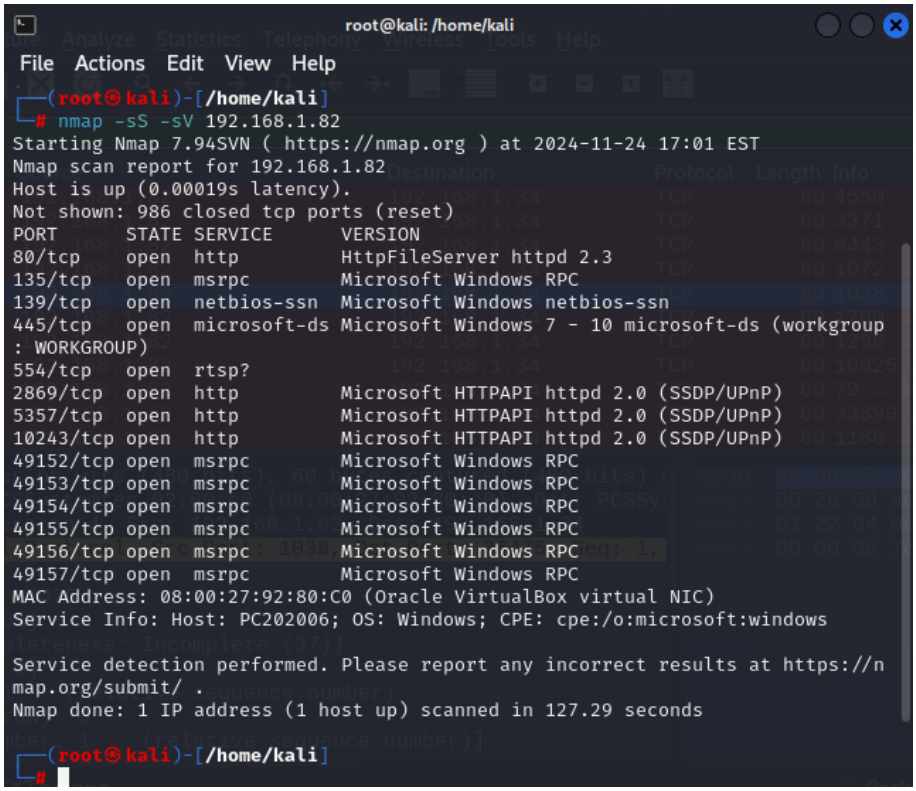
Figura 34 Wireshark capturando



Fuente: Elaboración propia

Por ello, como primera medida, sería necesario activar los firewalls[19] y el antivirus en cada máquina, además de actualizar el sistema operativo para mitigar las vulnerabilidades identificadas por el equipo Red Team. Posteriormente, con base en el informe de puertos vulnerables generado mediante Nmap, procedería a bloquear los puertos señalados en cada máquina con Windows 7, ajustándome a las vulnerabilidades detectadas.

Figura 35 Validación vulnerabilidades con NMAP



Fuente: Elaboración propia

[19] de, E. (2024, July 26). *Firewall: Qué es, cómo funciona y su importancia en la seguridad informática*. GoDaddy Resources - LATAM. https://www.godaddy.com/resources/latam/seguridad/firewall-que-es-como-protege-red

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

El primer paso sería garantizar que los sistemas operativos estén actualizados y tan pronto seria activar tanto el firewall como el antivirus en todas las PC. Adicionalmente, en cada sistema operativo Windows 7, implementaría medidas de **hardening**[20], tales como:

- ✓ **Realizar una instalación segura**: creando particiones primarias en la unidad con el fin de tener los archivos de datos en una unidad y las herramientas y software esenciales alojados en la partición del sistema operativo.
- ✓ **Establecer contraseñas robustas:** configurando políticas de vencimiento, bloqueo tras múltiples intentos fallidos y aplicándolas tanto para el acceso al sistema como para la protección de los archivos de datos.
- ✓ **Deshabilitar usuarios genéricos:** renombrar la cuenta de administrador, eliminar cuentas no utilizadas y limitar los privilegios de las cuentas activas.
- ✓ **Restringir carpetas compartidas:** Aumentar la seguridad de las contraseñas de acceso en red.
- ✓ **Implementar políticas de control de software**: Mediante listas blancas y negras, asegurando que solo se ejecuten aplicaciones permitidas y promoviendo buenas prácticas de uso.
- ✓ **Configuración**: Únicamente los puertos y servicios necesarios para cada máquina, cerrando aquellos no utilizados y reduciendo posibles puertas traseras.

[20] BBVA. (2024, September 3). *Técnicas de "hardening" para blindar tu empresa ante los ciberatacantes*. BBVA NOTICIAS. https://www.bbva.com/es/innovacion/tecnicas-de-hardening-para-blindar-tu-empresa-ante-los-ciberatacantes/

- ✓ **Deshabilitar**: El acceso remoto en equipos que no lo necesiten y, en caso de ser indispensable, habilitarlo únicamente a través de canales cifrados como SSH, restringiéndolo a usuarios específicos.
- ✓ **Realizar respaldos de información:** En dispositivos de almacenamiento físicos desconectados de la red para garantizar mayor seguridad.

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

Los equipos Blue Team[21] son grupos externos contratados por una empresa para analizar y mantener la ciberseguridad de sus sistemas desde una perspectiva externa. Su trabajo se basa en los hallazgos proporcionados por los equipos Red Team a través de sus pruebas y ataques controlados. Por otro lado, los equipos de respuesta a incidentes informáticos (SCIRT)[22] están formados principalmente por personal interno de la organización afectada. Estos equipos se encargan de identificar vulnerabilidades, contener incidentes y eliminar amenazas, llevando a cabo todo el proceso dentro de la misma unidad. Aunque su conocimiento interno les permite actuar con mayor rapidez y precisión, esta ventaja puede convertirse en un riesgo, ya que la posibilidad de filtraciones o manipulaciones por parte del personal interno representa una vulnerabilidad, a diferencia de los Blue Team, cuya independencia reduce la probabilidad de corrupción en el proceso.

[21] Lopez, V. (2024, March 13). *Blue team en ciberseguridad: definición, funciones y herramientas*. S2 Grupo. https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/

[22] *Equipo de respuesta ante incidentes | Cyberzaintza*. (2024). Ciberseguridad.eus. https://www.ciberseguridad.eus/ciberglosario/equipo-de-respuesta-ante-incidentes

Tabla 4 Diferencias entre equipos

Aspecto	Blue Team	Equipo de Respuesta a Incidentes Informáticos
Composición	Generalmente está compuesto por expertos externos contratados para evaluar y proteger los sistemas.	Compuesto por personal de la propia empresa, que tiene conocimiento directo de la infraestructura y los procesos internos.
Rol principal	Su función es prevenir ataques y mantener la seguridad de los sistemas a través de medidas proactivas, pruebas de penetración y vigilancia constante.	Se encarga de manejar los incidentes cuando ocurren, investigando, conteniendo y resolviendo las amenazas detectadas.
Enfoque	Enfoque preventivo, realizando auditorías y fortaleciendo las defensas antes de un posible ataque.	Enfoque reactivo, respondiendo rápidamente a los incidentes de seguridad para mitigar los daños.
Ventajas	Debido a su rol externo, se reduce el riesgo de corrupción interna y se aporta una visión objetiva.	Tiene la ventaja de tener acceso en tiempo real a la infraestructura interna, lo que permite una respuesta más rápida y personalizada.
Desventajas	Puede no tener el conocimiento profundo del entorno interno de la empresa, lo que puede limitar su capacidad de respuesta ante incidentes específicos.	Al ser parte de la misma empresa, el equipo puede ser susceptible a infiltraciones internas o filtraciones de información.

Fuente: Elaboración propia

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

Naturalmente, lo utilizaría como referencia para recordar las tareas y prioridades precisas en cada nivel del proceso de contención. Uno de los principios básicos de la ciberseguridad es la

reducción de costes y evitar la dependencia empresarial o económica, por lo que creo que es importante que el CIS sea una organización sin ánimo de lucro.

Además, los controles CIS[23] me permitirían elaborar un plan de acción detallado, utilizando sus recomendaciones sobre software y hardware para abordar áreas de desconocimiento y mejorar la seguridad. Esto se basa en la experiencia compartida de una comunidad que busca fortalecer la protección mediante el intercambio de ideas y soluciones colectivas.

Sin embargo, sería fundamental mantener el anonimato en la aplicación de estas herramientas, evitando exponer información confidencial de la empresa contratante del Blue Team. Implementar estas recomendaciones proporcionaría un conjunto estructurado de acciones, priorizadas cronológicamente, para garantizar una mejor protección de los sistemas, aprovechando el conocimiento colectivo de la comunidad cibernética.

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

Las herramientas SIEM unifican datos de riesgos en redes y sistemas, priorizan amenazas y detectan actividades inusuales para enfocar la seguridad en eventos sospechosos.

Ventajas de SIEM:

- ✓ Consolidación de la información relacionada con la seguridad.
- ✓ Automatización en la supervisión y respuesta ante incidentes.
- ✓ Respuesta ágil a amenazas y eventos críticos.

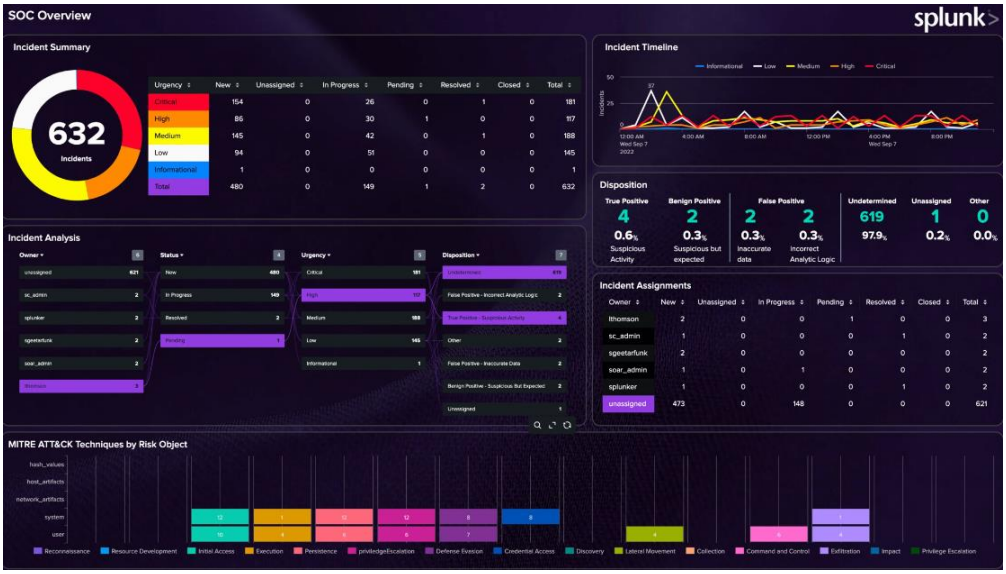
[23] ManageEngine. (2022). *¿Qué son y cómo implementar los Controles de CIS? | Definición de Controles CIS o CIS Controls (Cis Ciberseguridad) - ManageEngine*. Manageengine.com. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

- ✓ Disminución en el tiempo para identificar ataques.
- ✓ Análisis forense preciso y eficaz.
- ✓ Optimización de alertas y notificaciones.
- ✓ Correlación de registros en tiempo real.
- ✓ Mejor manejo de riesgos y análisis de vulnerabilidades.

Funciones principales de un SIEM:

- **Recopilación de datos:** recolecta registros de sistemas, usuarios y vulnerabilidades.
- **Clasificación y normalización:** unifica los formatos de datos y establece lo que es normal o anómalo.
- **Correlación:** analiza datos mediante algoritmos para identificar patrones y relaciones entre eventos.
- **Alertas y notificaciones:** genera avisos relevantes para administradores según la prioridad de los eventos.
- **Establecimiento de prioridades:** clasifica eventos críticos, emitiendo alarmas solo cuando es necesario.
- **Monitoreo en tiempo real:** permite observar eventos actuales y analizar datos históricos para fortalecer la seguridad.
- **Flujos de trabajo seguros:** facilitan la gestión de incidentes de forma automatizada o parcialmente automatizada, permitiendo además la apertura de nuevos casos o la ejecución de investigaciones relacionadas con incidentes.

Figura 36 Gestor de vulnerabilidades Splunk



Fuente: *Dashboard Studio Feature Highlights in Splunk Enterprise 9.2 | Splunk*. (2024). Splunk. https://www.splunk.com/en_us/blog/tips-and-tricks/dashboard-studio-feature-highlights-in-splunk-enterprise-9-2.html

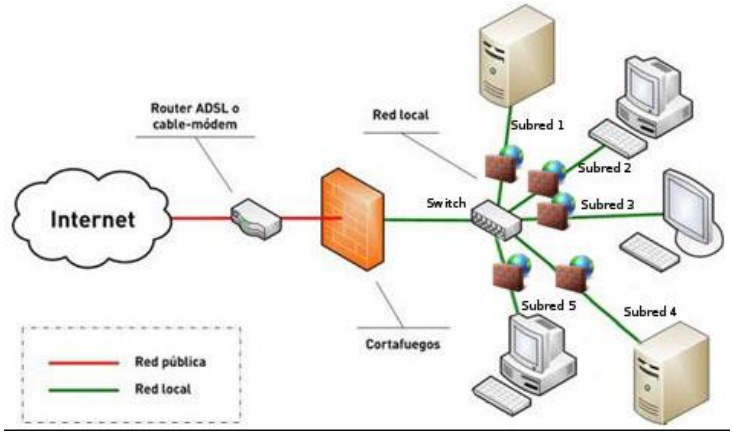
Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección

Firewall:

Dado que regulan la entrada y salida de paquetes de datos que no se ajustan a las normas de seguridad preestablecidas, los cortafuegos se consideran herramientas esenciales en la contención de amenazas. Según la configuración especificada, el cortafuegos aísla la máquina o la dirección IP y bloquea el puerto al recibir una solicitud inusual o sospechosa. Los cortafuegos de software imitan el funcionamiento de los cortafuegos físicos, mientras que los cortafuegos de hardware suelen montarse en routers controlables. Los cortafuegos por software, al igual que los

cortafuegos de Windows, suelen ser soluciones de software preconfiguradas que permiten al usuario ajustar el nivel de seguridad o protección según sus necesidades.

Figura 37 Herramienta contención Firewall



Fuente: *FIREWALL*. (2020, June). TecnolaboratorioSTI. https://tecnolaboratoriodeideas.wordpress.com/alcatel-omniswitch/

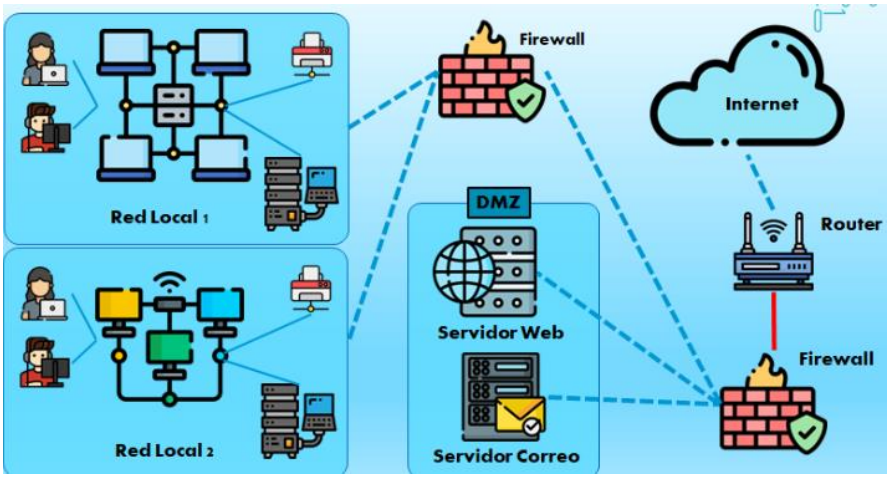
DMZ o zonas desmilitarizadas:

Las zonas desmilitarizadas (DMZ)[24] son redes aisladas dentro de la infraestructura interna de una organización, diseñadas para albergar servicios y recursos que necesitan estar accesibles desde Internet, como servidores de correo y servidores web. La principal característica de una DMZ es que impide las conexiones desde la DMZ hacia la red interna, pero permite conexiones tanto desde Internet como desde la red interna de la empresa, donde se encuentran los equipos de trabajo. Esta configuración tiene como objetivo proteger los servicios expuestos a Internet, que son más vulnerables a los ataques, redirigiendo los posibles intentos de intrusión

[24] *¿Qué es la Zona Desmilitarizada (DMZ) - Términos y Definiciones de Ciberseguridad?* (2024). Vpnunlimited.com. https://www.vpnunlimited.com/es/help/cybersecurity/dmz

hacia los servicios en la DMZ para evitar que afecten la red interna. Al igual que los firewalls, las DMZ pueden implementarse tanto mediante hardware como software.

Figura 38 Herramienta contención DMZ



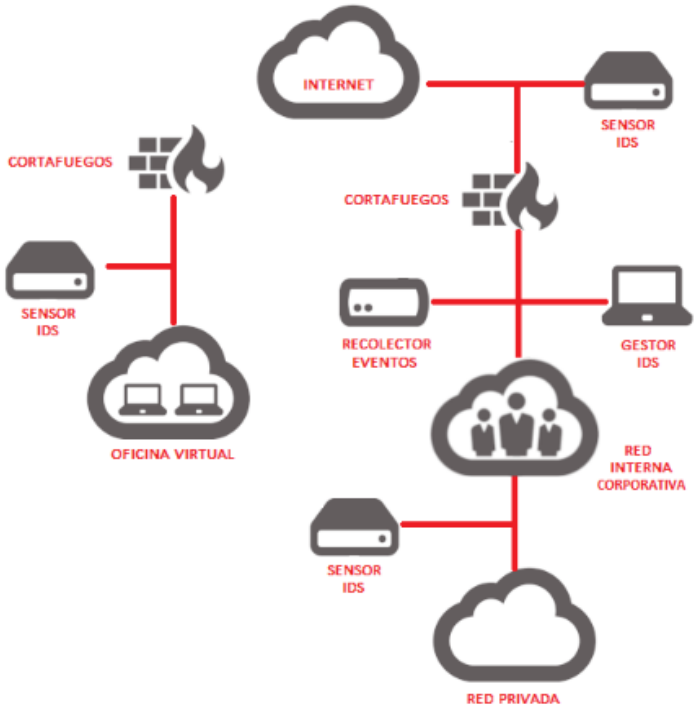
Fuente: Numbers, P. (2022, June 2). *Cortafuegos y zona desmilitarizada "DMZ" Para minimizar los riesgos derivados de un servidor con acceso desde Internet que pudiera comprometer la seguridad de la organización, se debe utilizar un cortafuegos o firewall y una red local denominada zona desmilitarizada o DMZ (por su traducción de*. Linkedin.com. https://es.linkedin.com/pulse/protege-tu-empresa-con-dmz-perfectnumbers

Snort:

Es un Sistema de Detección de Intrusos basado en red (IDSN)[25]. Un IDS es una red gratuita que detecta intrusiones mediante patrones conocidos y reglas configurables. Funciona como esniffer y permite analizar paquetes en tiempo real, registrando ataques para facilitar la respuesta.

[25] ciberseg1922. (2021, July 2). *Analizando Snort: sistema de detección de intrusiones*. Ciberseguridad. https://ciberseguridad.com/servicios/sistema-deteccion-intrusos-ids/snort/

Figura 39 Herramienta contención Snort



Fuente: *¿Qué son y para qué sirven los SIEM, IDS e IPS? | Empresas | INCIBE*. (2021). Incibe.es. https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips

6 CONCLUSIONES

Hay que poner en marcha una estrategia de defensa en profundidad para proteger a la empresa de los ataques en línea. Al implantar varias capas de seguridad, como sistemas de detección de intrusos, cortafuegos y cifrado de datos, los sistemas están protegidos en varios puntos, lo que dificulta a los piratas informáticos aprovecharse de los puntos débiles. Esta estrategia mejora enormemente la postura de seguridad de la organización al fortificar la infraestructura técnica y añadir una línea de defensa adicional contra accesos no deseados.

Para reducir el impacto de un ataque, la detección temprana de amenazas y una respuesta rápida son esenciales. Mediante la implantación de herramientas de supervisión en tiempo real, como los sistemas SIEM, es posible detectar tendencias extrañas y posibles peligros antes de que se conviertan en problemas importantes. Para controlar los ataques y detener su propagación, es esencial poder actuar con rapidez y eficacia, lo que subraya la importancia de una buena preparación.

El factor humano juega un papel fundamental en la seguridad cibernética, por lo que la capacitación continua del personal es indispensable. Educar a los empleados en buenas prácticas de seguridad, como identificar correos electrónicos fraudulentos o utilizar contraseñas seguras, ayuda a prevenir que sean víctimas de ataques como el phishing. Un personal bien capacitado se convierte en una primera línea de defensa crucial, contribuyendo a proteger los activos digitales de la organización y fomentando una cultura organizacional de seguridad.

La ciberseguridad es un proceso dinámico que debe ser evaluado y adaptado constantemente. Dado que las amenazas cibernéticas están en constante evolución, las estrategias de seguridad deben ser revisadas y actualizadas de forma regular para mantenerse efectivas. La

realización de auditorías periódicas, la actualización de las políticas de seguridad y la integración de nuevas tecnologías garantizan que la organización pueda enfrentar los desafíos emergentes y mantenerse protegida frente a los ataques, lo que resalta la necesidad de un enfoque continuo y flexible para la seguridad.

7 RECOMENDACIONES

Aplicar técnicas que se centren en identificar, mitigar y responder a las posibles vulnerabilidades, además de prevenir los ataques, es crucial para reforzar la seguridad dentro de una empresa. Esto se basa en identificar, abordar y minimizar los posibles riesgos. Sugerencias para crear planes que mejoren los aspectos de seguridad de una organización: Para reforzar la seguridad de una organización:

1.Utilizar una estrategia de defensa en profundidad

Se aconseja establecer varios niveles de seguridad para salvaguardar los sistemas y la red de la empresa. Para que las demás capas sigan protegiendo los activos vitales en caso de fallo, cada capa debe ofrecer protección en varios puntos de acceso (redes, apps, endpoints, etc.). recursos vitales de la organización.

Estrategia: La segmentación de la red, los sistemas de detección de intrusos (IDS), los firewalls, el software antivirus y el cifrado de datos en tránsito y en reposo son parte de esta estrategia.

2. Fortalecer el Control de Acceso y la Autenticación

Recomendación: Implementar controles de acceso robustos y autenticación multifactor (MFA) para todos los usuarios, especialmente los que tienen acceso a datos sensibles o sistemas críticos.

Estrategia: Asegurarse de que los usuarios sólo puedan acceder a los sistemas que necesitan para realizar su trabajo y que las contraseñas sean fuertes y cambiadas periódicamente. La implementación de MFA añade una capa adicional de seguridad frente a intentos de acceso no autorizado.

3. Realizar Pruebas Continuas de Seguridad con Red Team y Blue Team

Recomendación: Mantener un programa constante de pruebas de penetración y ejercicios de simulación de ataques con equipos Red Team (ataques simulados) y Blue Team (defensas).

Estrategia: Los ejercicios de Red Team y Blue Team ayudan a identificar vulnerabilidades no detectadas, probar la eficacia de las defensas y mejorar la coordinación entre equipos de seguridad. Además, deben realizarse simulaciones de incidentes para mejorar la capacidad de respuesta ante posibles ciberataques.

4. Actualizar y Parchar Regularmente los Sistemas

Recomendación: Establecer un proceso de gestión de parches efectivo que garantice la actualización continua de sistemas operativos, aplicaciones y hardware.

Estrategia: Los parches de seguridad deben ser aplicados de manera oportuna para corregir vulnerabilidades conocidas. Esto reduce la superficie de ataque y protege contra exploits comunes utilizados por los atacantes.

5. Desarrollar un Plan de Respuesta ante Incidentes

Recomendación: Crear y probar regularmente un plan de respuesta ante incidentes que defina los pasos a seguir en caso de una brecha de seguridad.

Estrategia: Este plan debe incluir protocolos de comunicación, roles y responsabilidades claras, y herramientas de recuperación que permitan minimizar el daño y la interrupción de las operaciones. La capacitación periódica de los empleados y la realización de simulacros de incidentes son cruciales.

6. Educar y Capacitar al Personal de Forma Continua

Recomendación: Implementar programas de concienciación sobre seguridad cibernética para todo el personal, especialmente para aquellos que tienen acceso a sistemas sensibles.

Estrategia: Los empleados deben ser entrenados regularmente sobre las mejores prácticas de seguridad, cómo detectar phishing, y las políticas de la empresa en cuanto a la protección de datos y la gestión de contraseñas.

7. Implementar Controles de Seguridad en la Nube

Recomendación: Si la organización utiliza servicios en la nube, es esencial implementar controles de seguridad adicionales en estas plataformas.

Estrategia: garantizar que los servicios estén configurados de forma segura en la nube, incluida la autenticación multifactor, la segmentación de la red y la protección de datos en tránsito y almacenamiento. La nube debe ser un componente esencial de la estrategia de seguridad.

8. Asegurar las Comunicaciones y los Dispositivos Móviles

Recomendación: Implementar políticas de seguridad estrictas para los dispositivos móviles y las comunicaciones cifradas.

Estrategia: Esto incluye la gestión de dispositivos móviles (MDM), cifrado de correo electrónico, y políticas de uso seguro de dispositivos personales en la red corporativa (BYOD).

9. Revisar y Auditar Continuamente las Políticas de Seguridad

Recomendación: Realizar auditorías regulares de seguridad para evaluar el cumplimiento de las políticas establecidas y detectar posibles fallas en los controles de seguridad.

Estrategia: Estas auditorías deben incluir revisiones de configuraciones, acceso a datos y registros de actividad, y deben ser realizadas por equipos internos o externos para garantizar una evaluación imparcial.

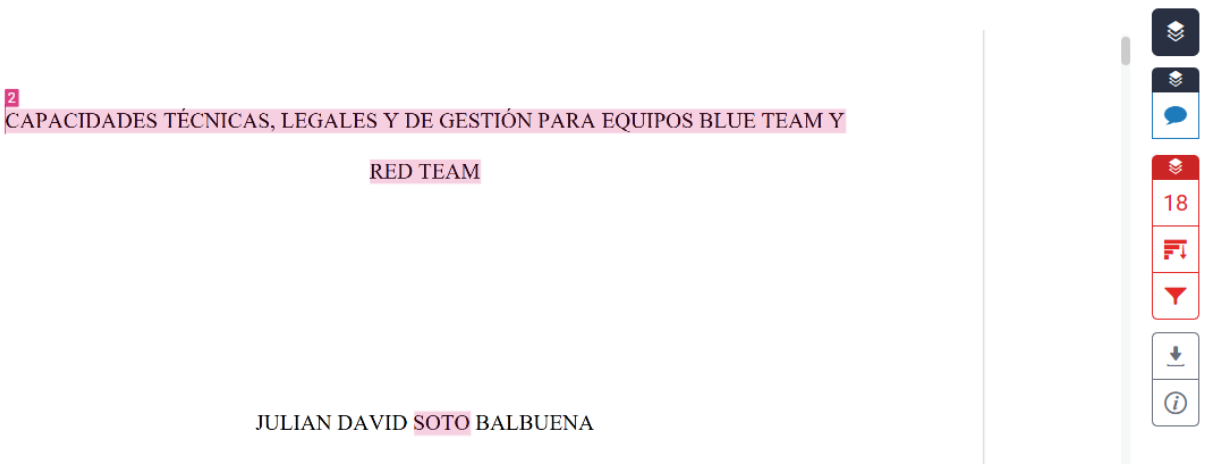
8 ANEXOS

Enlace video sustentación:

https://www.youtube.com/watch?v=_iAcs0aspIM

Reporte similitud:

Figura 40 Reporte similitud turnitin



Fuente: Elaboración propia

9 BIBLIOGRAFIA

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26)Abrir este documento utilizando ReadSpeaker docReader .https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

Congreso Colombia. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

GeeksforGeeks. (2024, February 29). *How To Turn Off Firewall On Kali Linux?* GeeksforGeeks. https://www.geeksforgeeks.org/how-to-turn-off-firewall-on-kali-linux/

How to use a reverse shell in Metasploit. (2017). Metasploit Documentation Penetration Testing Software, Pen Testing Security. https://adfoster-r7.github.io/metasploit-framework/docs/using-metasploit/basics/how-to-use-a-reverse-shell-in-metasploit.html

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Kali Linux Nmap | How to Use Nmap in Kali Linux with Examples? (2021, August 8). EDUCBA. https://www.educba.com/kali-linux-nmap/

Kinzie, K. (2022, August 19). *How to Use Wireshark: Comprehensive Tutorial + Tips*. Varonis.com; Varonis. https://www.varonis.com/blog/how-to-use-wireshark

Ley 1273 de 2009 - Gestor Normativo. (2015, December). Funcionpublica.gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 842 de 2003 | Copnia. (2016). Copnia.gov.co. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Linux, K. (2024, March). *Metasploit Framework | Kali Linux Documentation*. Kali Linux; Metasploit Framework | Kali Linux Documentation. https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/

MINTIC. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63)Abrir este documento utilizando ReadSpeakerdocReader . http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26)Abrir este documento utilizando ReadSpeaker docReader . https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa

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

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285-288. https://doi.org/10.1109/ICCD.2011.6081410

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Zambrano Hernández, Peña Hidalgo, H. J., & Cardenas Corral. (2024). Guía Para la Gestión y Clasificación de Incidentes de CiberseguridadAbrir este documento utilizando ReadSpeaker docReader . Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf