CAPACIDADES TECNICAS LEGALES Y DE GESTION PARA EQUIPOS BLUE TEAM Y RED TEAM

YEINY PAOLA BONILLA RIOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PEREIRA
2022

CAPACIDADES TECNICAS LEGALES Y DE GESTION PARA EQUIPOS BLUE TEAM Y RED TEAM

YEINY PAOLA BONILLA RIOS

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
Luis Fernando Zambrano Hernández
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PEREIRA
2022

CONTENIDO

Pág.

LISTA DE FIGURAS

GLOSARIO

Lista de palabras o expresiones organizadas alfabéticamente en mayúscula sostenida, que se encuentran enmarcadas sobre el tema o contenido del trabajo de grado y es un complemento para la comprensión del documento.

ATAQUE: Es un intento de espiar, robar, desestabilizar, eliminar, obtener acceso a un sistema, sin estar autorizado y valiéndose de maniobras o software malicioso.

CAJA BLANCA: Es un tipo de pentesting, donde quien o quienes lo realizan, tienen un conocimiento previo de la estructura.

CAJA NEGRA: Es un tipo de pentesting, donde quien lo realiza, no tiene información relacionada con el objetivo sobre el cual se va ha realizar y parte desde cero, para obtener la información.

CODIGO ABIERTO: Es una modalidad de desarrollo, donde se permite la colaboración y modificación. En algunas ocasiones es gratuito.

CHUZADAS: Termino coloquial, dado a las interceptaciones a llamadas que se han realizado de forma ilegal en Colombia.

EXPLOIT: Es un software informático, una parte de código o comandos que aprovechan la vulnerabilidad de un sistema, ejecutando una tarea especial.

HACKING: Son técnica, a través de las cuales se puede acceder a un sistema, vulnerando sus condiciones de seguridad.

HOST: Se refiere a dispositivos conectados a una red, como computadores, servidores, tabletas, que ofrecen servicios.

METASPLOIT: Es un software, de gran uso en pentesting, que facilita una gran cantidad de herramientas para ejecutar exploits y también permite su desarrollo.

NETBIOS: Es una interfaz de comunicación entre el hardware y la red.

PENTESTING: Es una práctica, que se realiza con el fin de evaluar o determinar niveles de seguridad de un sistema informático

RESUMEN

Ante el avance tecnológico acelerado que se ha presentado en los últimos años, donde miles de nuevos servicios se han virtualizado, maneras más fáciles y ágiles de hacer trámites, hacen parte de nuestra vida cotidiana, la información digital, los activos digitales, hoy en día cobran gran importancia. De la forma como crecen los beneficios, también crecen los ataques a todas estas plataformas y no solo a nivel de grandes empresas, si no de cada persona, últimamente los ataques que antes se pensaba que solo afectaría una gran organización, se hacen más cercanos a los usuarios finales.

Desde hace varios años se ha visto la necesidad de proteger la información, sin embargo, a hoy es un tema imperante, que no puede pasarse por alto. Para lograrlo se han desarrollado estándares, manuales, que relacionan una serie de buenas prácticas y de actividades que se deben realizar, para mantener un nivel de protección. También se cuenta con hardware y software de seguridad, acorde a las necesidades específicas de cada organización.

Luego, viene el recurso humano que realiza la integración de las políticas el Hardware y el Software, para brindar confianza, disminuir el riesgo, disminuir el impacto, para prepararse ante una situación de ataque, que cada vez parece más inminente.

Entre las muchas estrategias que existen para elevar los niveles de seguridad, está la de blue team y red team, que es una de las más completas, dado que tiene en cuenta aspectos de lado y lado, es decir tanto del lado atacante, como del lado de la defensa, por eso este documento elabora un informe técnico en el que se determina cual es la estrategia de los equipos blue team y red team, para aumentar la seguridad en las organizaciones.

ABSTRACT

Given the accelerated technological progress that has occurred in recent years, where thousands of new services have been virtualized, easier and more agile ways to carry out procedures, are part of our daily lives, digital information, digital assets, today are of great importance. In the way that profits grow, attacks on all these platforms also grow and not only at the level of large companies, but of each person, lately the attacks that were previously thought would only affect a large organization, have become closer to end users.

For several years the need to protect information has been seen, however, today it is a prevailing issue that cannot be ignored. To achieve this, standards and manuals have been developed that relate a series of good practices and activities that must be carried out to maintain a level of protection. There is also security hardware and software, according to the specific needs of each organization.

Then comes the human resource that performs the integration of the Hardware and Software policies, to provide confidence, reduce the risk, reduce the impact, to prepare for an attack situation, which seems more and more imminent.

Among the many strategies that exist to raise security levels, there is that of blue team and red team, which is one of the most complete, since it takes into account aspects from both sides, that is, both from the attacking side and from the attacking side. defense side, that is why this document prepares a technical report in which the strategy of the blue team and red team is determined, to increase security in organizations.

INTRODUCCIÓN

La Seguridad de la Información es un tema de gran calado hoy en día, es por esto por lo que las empresas en caminan sus esfuerzos a disminuir el riesgo al nivel más bajo posible, siendo la estrategia blue team y red team, una de las mejores, dado que tiene dos componentes, uno de ataque y otro de defensa, generando una visión más global y real de la situación de la organización al mismo tiempo que la prepara para responder ante un incidente real.

Para conocer específicamente de que se trata esta estrategia de seguridad, en este documento genera un informe técnico, en el que se tratan algunos conceptos básicos que guardan una estrecha relación con el trabajado desempeñado por estos dos equipos, además de la normatividad que se debe tener en cuenta, en caso de que este trabajo sea realizado sin autorización de la parte a la que se aplican las pruebas o pasando por alto prohibiciones que se encuentran en la legislación de cada país.

También se documentan las fases para llevar a cabo un pentesting, describiendo las herramientas de uso más frecuentes, así como también las herramientas de contención que, de acuerdo con los casos analizados en el documento, pueden ser de utilidad para frenar el ataca o disminuir su impacto.

1 DEFINICIÓN DEL PROBLEMA

Los sistemas informáticos son fundamentales para las organizaciones, hoy en día se tiene una dependencia muy alta de todos los servicios y facilidades que se obtienen al usarlos, sin embargo, estos sistemas están siendo muy vulnerables debido al crecimiento acelerado.
Estas vulnerabilidades son una oportunidad para los hackers, para personas que quieren realizar un daño, obtener dinero a partir de estafar, extorsionar, se han convertido también en una oportunidad para realizar instigaciones políticas, entre muchas otras situaciones que generan un gran número de impactos negativos entre quienes son blanco de los ataques.
Las consecuencias de ser blanco de ataques se ven en un abanico muy amplio, pues pueden ir desde el impacto económico, reputacional, recibir demandas, por mencionar solo lo más general.
Todo lo anterior, bien merece brindar soluciones, que generen confianza entre las organizaciones y los usuarios de todos estos sistemas.
La implementación de estrategias de gobierno, de las organizaciones para dar respuesta a estos ataques, es un tema al que no se puede ser ajeno y que se debe enfrentar.

1.1 ANTECEDENTES DEL PROBLEMA

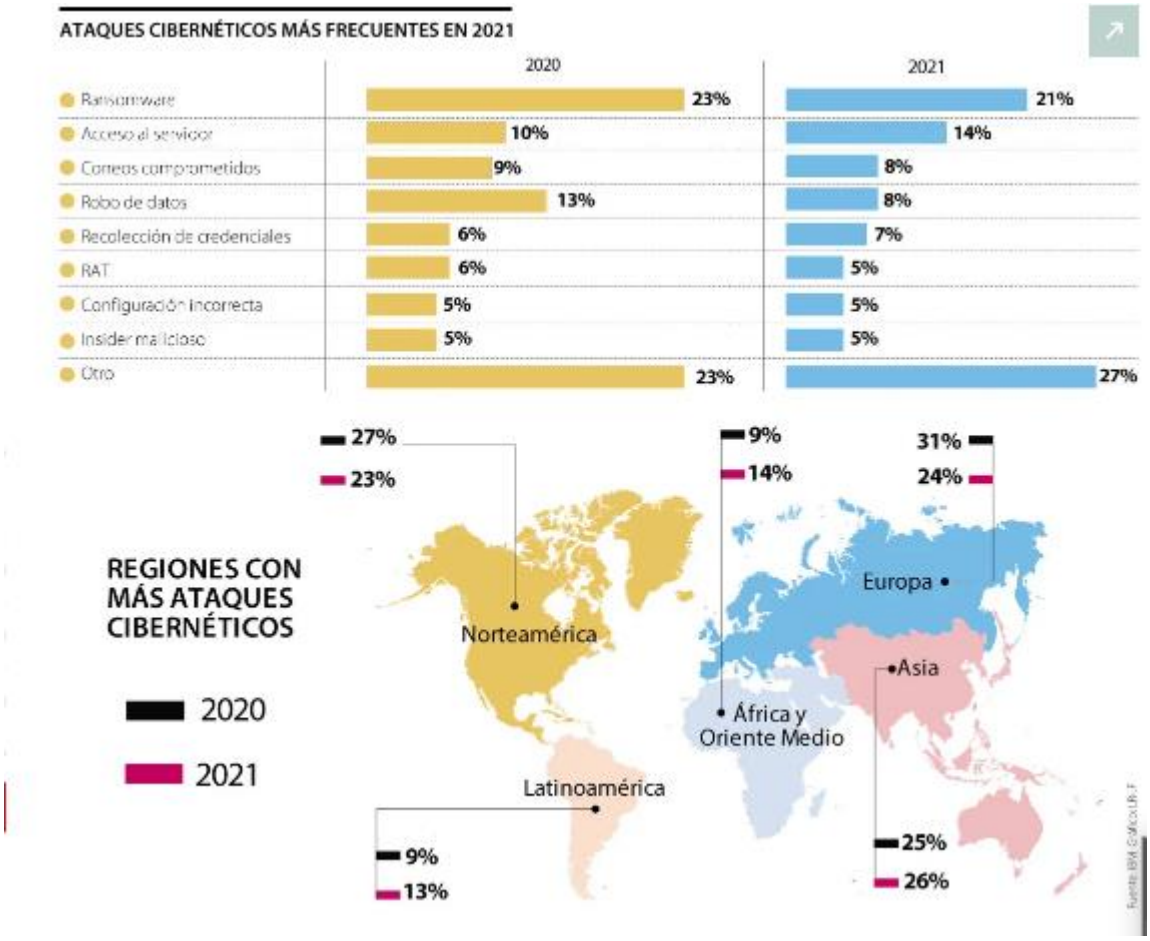
De acuerdo con un artículo del periódico La República, del 19 de marzo de 2022, se registró un incremento en los ataques durante el año 2021 en los países de América Latina, en comparación con el año anterior, esta información fue entregada por el índice de inteligencia de Amenazas X-Force de IBM Security, donde se informó que los países más atacados fueron Brasil, México y Perú[1]

En la siguiente gráfica, tomada del artículo, se evidencia que los ataques más frecuentes son el ramsonware, que es el secuestro de los datos, por el que generalmente se solicita un rescate económico, el acceso al servidor, donde un delincuente obtiene acceso a un sistema sin permiso, y el robo de datos, que en su metodología más frecuente se encuentra el uso del correo electrónico corporativo (BEC por sus siglas en inglés), para hacer caer a las víctimas.

Los ciberdelincuentes buscan ganar dinero, obtener poder, por eso las organizaciones no pueden seguir actuando bajo el supuesto de tener parchadas todas las vulnerabilidades y deben contar con estrategias que vayan mas delante de lo que debería ser obvio.

[1] https://www.larepublica.co/globoeconomia/cantidad-de-ciberataques-aumentaron-4-en-america-latina-durante-el-ano-pasado-3326053

Figura 1. Ataques cibernéticos mas frecuentes en el 2021



Fuente: https://www.larepublica.co/globoeconomia/cantidad-de-ciberataques-aumentaron-4-en-america-latina-durante-el-ano-pasado-3326053

1.2 FORMULACIÓN DEL PROBLEMA

¿Como las estrategias de los equipos de blue team y red team, pueden contribuir a hacer frente a los actuales problemas de seguridad cibernética y disminuir el impacto negativo generado por los ciberataques?

2. JUSTIFICACION

La ciberdelincuencia siempre ha existido, sin embargo, cada vez las plataformas de ataque son mas extensas y vulnerables, los esfuerzos de las organizaciones para proteger su información no siempre son suficientes y siempre siguen quedando muchos baches de seguridad en todo el ecosistema.
Se hace necesario estudiar, analizar, buscar métodos, estrategias para que se pueda proteger la información, las infraestructuras, la seguridad de las personas y muchos otros aspectos de la vida, donde estos sistemas se encuentran inmersos.

Debido a lo anterior es necesario, comprender como los equipos de blue team y red team, diseñan su estrategia y contribuyen a aumentar los niveles de seguridad en las organizaciones y a disminuir el impacto negativo que generan los ciberataques.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Construir un informe técnico que permita determinar la estrategia usada por los equipos de blue team y red team, para identificar las vulnerabilidades en una organización.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar y definir la normativa existente relacionada con los delitos informáticos.
- Definir conceptos de pentesting, fases y herramientas que pueden ser utilizadas en cada una de ellas.
- Definir las herramientas de contención que pueda usar el equipo blue team, a fin de minimizar el impacto generado por el ataque.

4. DESARROLLO DEL TRABAJO

4.1 MARGEN LEGAL DE COLOMBIA SOBRE DELITOS INFORMATICOS

Ley 527 de 1999.
Esta ley que se conforma de 40 artículos, y es la que le da vida Jurídica a los mensajes de datos electrónicos, las firmas digitales, las empresas certificadoras, el intercambio electrónico y establece los fines para los que pueden ser usados, las características que deben cumplir para tener la validez mencionada.

La ley 1273 de 2009, es la ley que creó un nuevo bien jurídico, llamado: "de la protección de la información y los datos" y adicionó al código penal un nuevo título que contiene dos capítulos en los cuales se describen las penas, castigos o sanciones que se presentan al infringir esta ley[2]. A continuación, se describen en el capítulo I, los siguientes:

Artículo 269ª: Trata del acceso a un sistema o permanencia en un sistema informático, sin tener autorización o sin tener las facultades para hacerlo. En este caso se incurre en cárcel de 48 a 96 meses y sanciones económicas que están entre 100 y 1000 SMLMV.

Articulo 269B: Este caso trata de la obstaculización ilegitima del sistema informático o red de telecomunicaciones. Se considera que aquí puede entrar por ejemplo una denegación de servicio y tiene la misma sanción que el artículo 269ª.

Articulo 269C: Trata de la interceptación de datos informáticos, en un sistema o en una red de telecomunicaciones, en cualquiera de sus fases, inicio, transmisión o tránsito de los datos. Por ejemplo, las chuzadas a las llamadas o interceptación de correos electrónicos. Para este caso la penalización es de 36 a 72 meses de prisión.

Articulo 269D: En este artículo se trata el Daño Informático, que puede ser la destruir, alterar, deterior, dañar, suprimir, borrar datos de un sistema de información. La penalización es de 48 a 96 meses de prisión y entre 100 y 1000 SMLMV de multa.

[2] COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (5, enero,2009). Por medio de la cual "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En Diario Oficial. Enero, 2009. Nro.47223. p. 1.

Articulo 269E: El uso de software malicioso, la producción, el tráfico, la adquisición, venta, envío, introducción o extracción de Colombia, puede acarrear de 48 a 96 meses de prisión y entre 100 y 1000 SMLMV.

Articulo 269F: Se trata la violación de datos personales, con provecho propio o para un tercero. Si se obtiene, compila, sustrae, ofrece, comercializara, intercambia, si se envía, divulga, se modifica o emplean códigos o datos personales, contenidos en ficheros, archivos, BD o medios semejantes también se sanciona con 48 a 96 meses de prisión y entre 100 y 1000 SMLMV.

Articulo 269G: La suplantación de sitios Web para captura de datos personales, la creación, desarrollo, programación, trafico, ejecución, venta, envío, de enlaces, páginas electrónicas, ventanas emergentes, puede tener una sanción de 48 a 96 meses de prisión y entre 100 y 1000 SMLMV.
En este artículo también se incluyen la modificación de nombres de dominio, que envíen el usuario a una IP diferentes, con el agravante de que si la cadena de delito reclutó victima (Ejemplo, ataques DdoS con Zombis).

Articulo 269H: Esta articulo relaciona una lista de situaciones que pueden aumentar las penas de la mitad a unas tres cuartas partes cuando, se cometen contra servicios estatales, oficiales, del sector financiero nacional o extranjero.
También se son ejecutadas por un servidor público en ejercicio de sus funciones, o aprovechando la confianza dada por ser un empleado o la depositada por el poseedor de la información.

En el capítulo II, se tratan los atentados informáticos y otras infracciones:

Articulo 269I: Cuando se comete hurto, hurto calificado (art 239 y 240 del código Penal), por medios informáticos, con herramientas que superan las medidas de seguridad, en las que se manipule un sistema, una red, se suplante un usuario, se sancionará de acuerdo con el artículo 240 del código penal.

Articulo 269J: La transferencia de activos sin permiso o sin consentimiento, a través del uso de herramientas informáticas y siempre que no constituya un delito más grave, se penaliza con, entre 48 y 120 meses de prisión y multa de 200 a 1500 SMLMV.

CONPES 3701
Este documento genera una serie de lineamientos a seguir en cuanto a las políticas de ciberseguridad y ciberdefensa, con el fin de que pueda desarrollarse una estrategia a nivel nacional, para contrarrestar el número creciente de ataques que

se presentaban en esa fecha, tarea en la que se involucraba a las entidades que debían desarrollar las bases dadas, para garantizar la seguridad de la información[3].

El CONPES, tomó como referencia, otras normas internacionales, de forma que pudiera obtener un producto completo y que se adaptara a las condiciones del país.

4.2 ETAPAS DE UN PENTESTING

Existe diversidad de metodologías para para la realización de pentesting, que sirven de apoyo al hacking ético, algunas son de código abierto, otras tienen un enfoque más específico, frente a otras que abarcan un tema en general, algunas son desarrolladas por grandes instituciones o grupos que las mantienen en constante actualización, lo cual es una ventaja, teniendo en cuenta la velocidad de los cambios y avances tecnológicos[4].

Cada metodología tiene una estructura diferente, usa nombres diferentes para definir las fases o etapas en las que se desarrolla, sin embargo, por las actividades realizadas podría decirse que hay una fase de planeación, otra de escaneo, otra de penetración y otra en la que se mantiene el acceso y se despliegan los ataques. A continuación, se definen.

Fase de reconocimiento: Esta es una de las fases que más tiempo demanda en toda la metodología, dado que, de acuerdo con el tipo de ataque, si es de caja negra, gris o blanca, se trata de recopilar la mayor parte de información del objetivo, nombres de empleados, direcciones de correos electrónicos, actividad de la empresa, dominios, entre otros.

En esta fase, se usan herramientas como redes sociales, internet, whois, buscadores especiales, entre otras.

Fase de Escaneo: De acuerdo con la información recopilada en la fase anterior, se realiza un escaneo a la red, a fin de identificar host, sistemas operativos, servicios, puertos y demás para buscar vulnerabilidades y definir un vector de ataque.

---

[3] Departamento nacional de planeacion. CONPES 3701. [Sitio web]. Colaboración.dnp.gov.co. [Consultada: 9 de septiembre de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

[4] Welivesecurity. Penetración Test, ¿En qué consiste? [Sitio web]. kWelivesecurity.com. [Consultada: 1 de septiembre de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

En esta fase, se puede hacer uso de Nmap, Nessus, Nexpose, que son herramientas que mediante comandos ejecutados sobre un dominio o sobre direcciones IP, devuelven información valiosa de los servicios y software en ejecución.
Otras herramientas utilizadas para encontrar vulnerabilidades es CVE, la cual es una base de datos que contiene datos sobre las vulnerabilidades conocidas.

Fase de enumeración: En esta fase, se debe realizar la identificación de usuarios, host, servicios y se debe establecer una conexión que permita la ejecución de consultas dentro del mismo sistema.
El escaneo genera una serie de datos que informan sobre lo que se encuentra al interior, lo que puede llegar a ser vulnerable. Es muy importante porque permite la correlación de información, se generan ideas acerca de la ruta que se puede seguir para realizar el ataque.

Fase de acceso: En esta fase, se aprovechan las vulnerabilidades que se han reconocido en fases anteriores.
A partir de obtener el número de equipos, las direcciones IP, los sistemas Operativos, los puertos y servicios, se intenta una o varias formas de acceder.
Una de las herramientas que puede usarse es Metasploit.

Fase de mantenimiento de acceso: Aquí como su nombre lo indica se trata de permanecer dentro del sistema sin ser detectado. Metasploit, es un programa con herramientas que pueden ser útiles en esta etapa.

Aunque generalmente estas son las fases definidas, siempre se debe realizar un informe de los resultados, socializarse y entregar recomendaciones.

4.3 DEFINICION Y EXPLICACION DE LAS SIGUIENTES HERRAMIENTAS:

- **Metasploit**

Es un software, generalmente usado para hacer pruebas de seguridad en sistemas informáticos, está dotado de muchas herramientas, que son pequeños programas, la mayoría de ellos han sido desarrollados bajo el conocimiento de vulnerabilidades identificadas, y tiene otro conjunto de herramientas llamadas payloads, que son los que explotan las vulnerabilidades; el otro grupo de herramientas son los encoders, cuya función es a través de cifrado, evadir los antivirus o los sistemas se seguridad perimetral.
También es posible escribir código y ejecutarlo, es decir crear sus propias herramientas, además que también interactúa con otras herramientas como Nmap.

- **Nmap**

Es una de las herramientas más potentes y utilizadas para realizar un escaneo de puertos, servicios, host, sistemas operativos, en una red, teniendo un rango de direcciones o en una dirección especifica. Nmap, tienen muchas variaciones del comando, lo que posibilita aún más la diversidad en la información devuelta.

• OpenVas

Es un escáner potente de vulnerabilidades, posee una interfaz gráfica, fue desarrollado a partir del escáner de Nessus y tiene una licencia de pago, se habla de que tienen más de 50 mil test y que está en permanente actualización. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad[5]

Servicios en línea:

• ExploitDB

Un exploit es un programa construido para explotar una vulnerabilidad de un sistema y puede ser usado por hackers de sombrero blanco o negro. Existen de varios tipos, como los conocidos, que trabajan sobre vulnerabilidades que ya han sido identificadas, los de día cero que son los más peligrosos y desconocidos, exploits de servicios, que tiene un enfoque especifico en esta materia y exploits para acceder a privilegios de root.
ExploitDB, es un proyecto no lucrativo, que fue desarrollado por la empresa Offensive Security, quienes también son creadores de Kali Linux. Consiste en una aplicación web que reúne información de bases de datos públicas, con información de exploits, los cuales pueden ser consultadas, descargados y usados por pentesting de todo el mundo, con la finalidad de ayudar en las auditorias[6].

• CVE

Es un sitio web, con una lista de vulnerabilidades identificadas, donde cada una de ellas es referenciada con un número, además entrega información de la fecha en la que se encontró la vulnerabilidad, los sistemas afectados, si existe o no solución conocida para la vulnerabilidad, y referencias a blogs o paginas donde se encuentra información de la vulnerabilidad.

---

[5] Greenbone open vas. OpenVas. [Sitio web]. Openvas.org. [Consultada: 29 de agosto de 2022]. Disponible en:https://www.openvas.org/

[6] Keepcoding. Que es exploitDB. [Sitio web]. Keepcoding.io. [Consultada: 29 de agosto de 2022]. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/

4.4 RECONOCIMEINTO ANALISIS Y CONFIGURACION DEL BANCO DE TRABAJO.

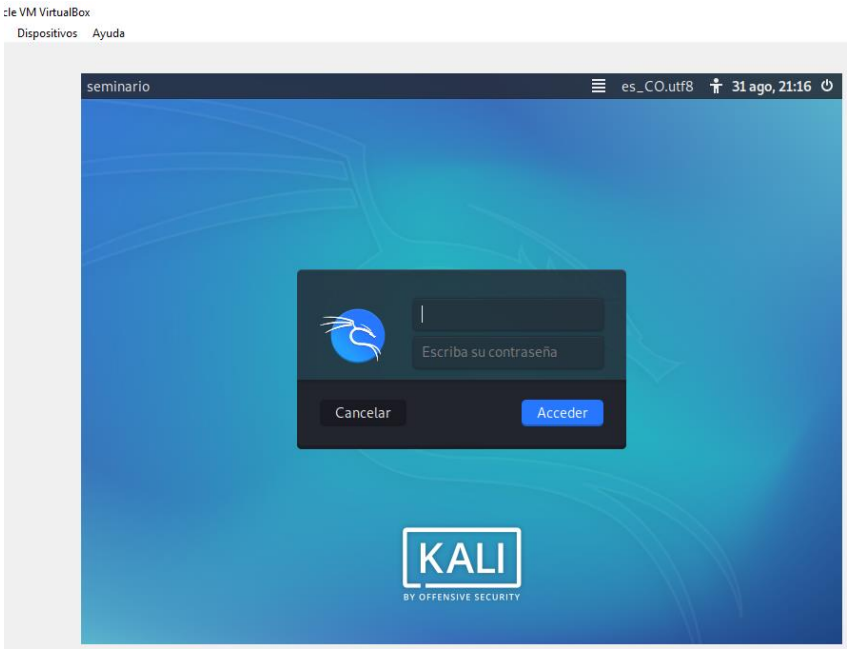
Como punto inicial se realizó la descarga de la herramienta virtual box, quedando instalada la versión 6.1.36. Posteriormente se realizó la descarga de las maquinas Windows y Kali Linux y se procedió a la importación de cada una de las OVAS.

En la imagen 1, se puede apreciar que se encuentra instalada la máquina de Kali Linux, a la que posteriormente se ingresa con las credenciales suministradas.

El anfitrión es una maquina con sistema operativo Windows 10 64 bits, 8 GB de RAM, procesador Core i5, 4200M – 2.50 GHZ.

La máquina Kali Linux, tiene 2 GB de RAM, disco dinámico y el mismo procesador del anfitrión

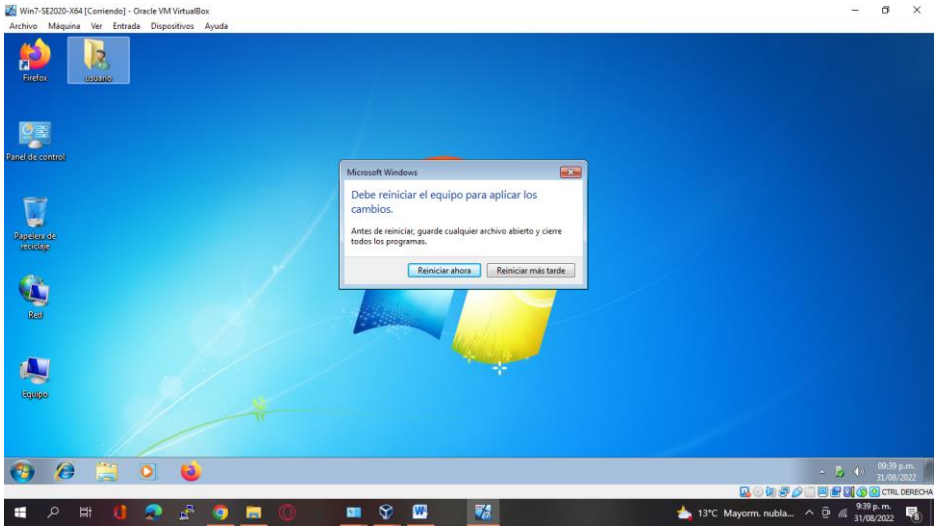
Figura 2. Interfaz inicio de sesión Kali Linux



Fuente: Autor.

En la imagen 2, se puede observar la instalación de la maquina Windows 7 de 64 bits. Se realizó una asignación de 2 Gb de memoria, disco dinámico, adaptador de red puente.

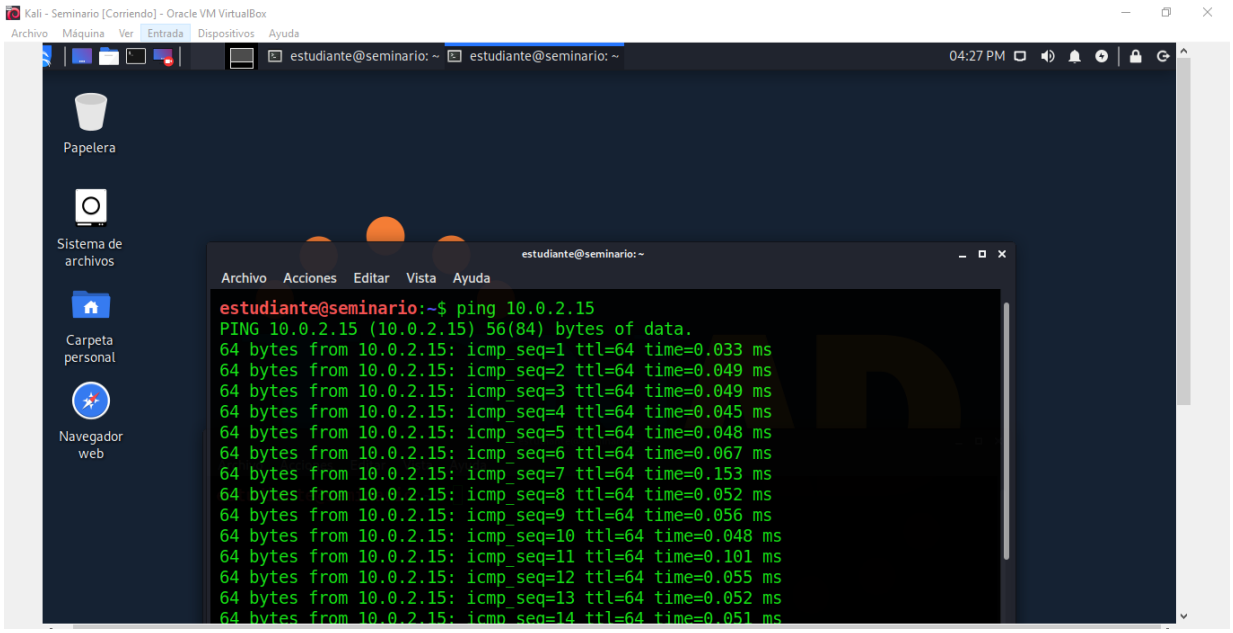
Figura 3. Windows 7 - Instalado



Fuente: Autor.

En la imagen número 3, se evidencia la comunicación entre las maquinas Kali y Windows.

Figura 4. Verificación de comunicación entre las maquinas.



Fuente: Autor.

4.5 EVIDENCIAS DE PROCESOS ILEGALES Y NO ÉTICOS ESTIPULADOS EN EL ACUERDO Y ARGUMENTACIÓN DE LAS RESPUESTAS

.

De acuerdo con las lecturas y la interpretación, efectivamente se encuentran muchos párrafos con una redacción que da lugar a interpretar que la organización comete delitos y que el acuerdo de confidencialidad pretende hacer cómplice y responsable a la parte receptora de todas las malas prácticas realizadas.
A continuación, se relacionan los puntos donde se encuentran irregularidades y la interpretación dada en relación con la ley 1273 de 2009, cuando aplica.

Clausula Primera.

Objeto: *en virtud del presente* ***acuerdo de confidencialidad,*** *la* ***parte receptora****, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la* ***información confidencial*** *o sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados.*

Interpretación: La organización está dando por hecho que realiza procesos ilegales, y estos no deben ser denunciados por la parte receptora.

Clausula segunda. Numeral 2.

Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

De acuerdo con la redacción del párrafo, la organización está dando por hecho que ha realizado chuzadas, interceptación de información y acceso abusivos a sistemas informáticos, que esta es su información confidencial y que no puede ser divulgada. Partiendo de esa premisa, estas serían algunas de las actividades que tendría que desarrollar el equipo de blue team y red team del cual se haría parte.

De acuerdo con la ley 1273 del 2009, en el artículo 269C, que trata de la interceptación de datos informáticos, la organización Hackers Security estaría cometiendo un delito y lo estaría enmascarando detrás de una fachada de ser una organización que asesora en temas de seguridad de la información.

Clausula cuarta. Numeral 1, en las obligaciones del contratista:

Mantener la ***información confidencial*** *segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de esta*

o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

*"Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él",* en esta oración al referirse a él, se da a entender, que la parte receptora, puede hacer uso de esa información en su beneficio.

Clausula dos. numeral 2, en las obligaciones del contratista:

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

"Restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla", en esta frase, se entiende que las únicas personas que no tienen acceso a esa información son las que más lo necesitan.

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

En este punto se haría cómplice de un delito, al darse cuenta de la práctica de conductas no éticas y no realizar ninguna denuncia. Aunque la ley 1273 no relaciona este hecho.

Clausula dos. numeral 4, en las obligaciones del contratista:

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

Nuevamente la organización reconoce en el numeral anterior, que realiza actividades ilegales y pide no denunciarlas ni hacerlas públicas.

Clausula dos. numeral 5, en las obligaciones del contratista:

Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

En el párrafo anterior, el uso de la información confidencial entregada queda supeditada a la orden que reciba en ese momento.

Clausula dos. numeral 6, en las obligaciones del contratista:

Responder por el mal uso que le den sus representantes a la ***información confidencial.***

En el párrafo anterior, hace responsable al contratante o parte receptora por las actividades que realicen los representantes y de antemano relaciona el mal uso de la información.

Clausula dos. numeral 8, en las obligaciones del contratista:

Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

En el numeral anterior se solicita asumir la responsabilidad por de delitos, partiendo de la premisa de que las actividades de la organización son ilegales.

Clausula sexta.

la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

En el párrafo anterior, se hace responsable a la parte que contraviene, de los perjuicios causados por la inobservancia del mismo documento, lo cual estaría en contravía de los derechos y deberes de las partes.

Clausula octava.

Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Hackers Security.

El punto octavo, tiene un párrafo en el que la parte receptora, se hace responsable ante cualquier delito y debe liberar de toda responsabilidad la organización. Esta es una conducta falta de ética, dado que la parte receptora, está realizando un trabajo para organización que es quien contrata y paga.

4.6 PROCESOS ILEGALES EN EL ANEXO 3 CONFORME A LA LEY 1273

Conforme a lo descrito en el anexo 3, documento que corresponde a un acuerdo de confidencialidad entre la organización y la parte receptora, se evidencian algunos párrafos en los que la organización da por hecho que realiza chuzadas, realiza acceso a sistemas informáticos sin permiso, e intercepta información.

El Artículo 269ª, se refiere al Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.[7]

De acuerdo con lo anterior, si la organización realiza o a realizado este tipo de prácticas, estaría violando el artículo 269A de la ley 1273 de 2009, dado que esto equivale a un acceso abusivo a un sistema informático.

También puede ser penalizado con base en el artículo 269C, de la misma ley, en este caso, por la realización de las chuzadas, pues ellas constituyen una interceptación de datos en su origen, o destino.

El articulo 269H, corresponde a la agravación punitiva, cuando una organización o persona, se aprovecha de la confianza depositada por el poseedor de la información, que en este caso puede ser una empresa contratante de asesoría o de prestación del servicio y donde se utiliza como fachada, para encubrir otras acciones que son delito.

4.7 APLICACIÓN AL TRABAJO DE HACKERS SECURITY

De acuerdo con la información presentada en el acuerdo de confidencialidad, con sus definiciones y clausulas, queda en evidencia, que es un acuerdo de impunidad, donde se va a conocer información de delitos, posiblemente se le solicite que sea participe de alguno de ellos y conforme al código de ética del COPNIA, uno de los deberes es la denuncia de delitos de los que se tenga conocimiento, con todas las pruebas que se puedan aportar.
El código de ética tiene en sus prohibiciones, permitir o tolerar la realización ilegal de la profesión. Con base en lo anterior, se estaría violando este código y se estaría expuesto a las sanciones de este.

---

[7] COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (5, enero,2009). Por medio de la cual "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen
las tecnologías de la información y las comunicaciones, entre otras disposiciones. En Diario Oficial. Enero, 2009. Nro.47223. p. 1.

Por este motivo, bajo ese acuerdo, no aplicaría a este trabajo.

4.8 CASO OPERACIÓN ANDRÓMEDA

De acuerdo con la información consultada[8], la operación Andrómeda, consistió en un grupo de personas del ejercito que se concentró en interceptar correos y llamadas, inicialmente a miembros del grupo de las FARC, luego creo un lugar fachada de hacking ético, dotado con equipos y redes de última tecnología, donde personas que se vieran atraídas por este tipo de actividades pudieran asistir libremente, tanto para aprender, como para enseñar. Estos conocimientos eran aprovechados por las personas a cargo del lugar, al parecer para extralimitarse en sus funciones, hasta llegar al punto de interceptar correos, conversaciones de WhatsApp, vender información sustraída, entre otras.

Al respecto considero que el ejército dentro de sus funciones de inteligencia debe poder interceptar llamadas, correos, mensajería de un grupo que se encuentra al margen de la ley, para lo cual debe disponer de un recurso humano, calificado, ético, supervisado y controlado.
En el momento de extender estas interceptaciones a otras personas que no hacen parte del grupo al margen de la ley, y de usar los recursos del estado tanto económicos, tecnológicos, humanos, de tiempo, se está extralimitando en sus funciones y aparte de esto está cometiendo un delito, dado que como se relaciona en la ley 1273 de 2009, en el artículo 269c, es necesario contar con una orden judicial para poder llevar a cabo este tipo de actividades.

Sin este el único delito, la sustracción de información, la venta o intercambio de esta, también se encuentra penalizado.

La penalización aumenta, dado que estas personas son funcionarios públicos, se aprovechan de personas que no tienen conocimiento de los fines reales de las actividades realizadas, lo anterior acorde con los artículos 269F y el 269H.

La profesión de los ingenieros que trabajan en este proyecto o que son cómplices, también se ve comprometida, teniendo en cuenta que el deber relacionado en el literal F, relaciona lo siguiente: “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”[9]

---

[8] El país. Esta es la cronología de como se ha desarrollado el caso Andrómeda. [Sitio web]. Elpais.com. [Consultada: 9 de septiembre de 2022]. Disponible en: https://www.elpais.com.co/colombia/esta-es-la-cronologia-de-como-se-ha-desarrollado-el-caso-andromeda.html

[9] COPNIA. Código de ética. [Sitio web]. Copnia.gov.co. [Consultada: 8 de septiembre de 2022]. Disponible en:

4.9 DESCRIPCION DE LAS HERRAMIENTAS DE SOFTWARE UTILIZADAS PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3

El anexo 4, entrega información acerca del uso de unos equipos con Windows 7, los cuales se usan en la actualidad debido a que se requiere el uso de un servicio llamado SMB v1. Tomando como base esta información se hace uso de las siguientes herramientas.

VirtualBox: Esta herramienta que permite la virtualización de diferentes maquinas, para este caso Kali Linux y la máquina de Windows 7 – 64 bits, a través de protocolos de red propiciados por la herramienta, se logra generar comunicación entre ellas, para generar el ambiente del ejercicio.

NMAP: Es una herramienta de código abierto, que permite hacer escaneo de red y auditoría, cuenta con muchas opciones para generar información, de puestos, servicios, sistemas operativos, versiones, entre otras. Por medio de esta herramienta se realiza un escaneo a la máquina, con el fin de identificar los puertos y servicios en uso.
Esta herramienta además permite la identificación de las vulnerabilidades presentadas en la máquina, contrastando la información con bases de datos previamente alimentadas con vulnerabilidades conocidas. Es así como entrega información de base, para continuar con la consulta.

CVE: Esta es una base de datos, donde se codifican las vulnerabilidades, se documenta información que describe la vulnerabilidad, la forma de superarla, los sistemas afectados con sus versiones, entre otras características. Esta también es una herramienta de consulta para ubicar vulnerabilidades de sistemas por diferentes versiones. Es así, como para el caso del anexo 4, se consultó allí la vulnerabilidad encontrada con la herramienta NMAP, que referencia CVE2017-0143.

Kali Linux: Este potente software, está dotado de herramientas. Inicialmente se ejecuta nmap, con las variantes necesarias para encontrar las vulnerabilidades. Seguido a esto, se puede realizar una búsqueda del exploit, el cual está estructurado y requiere la asignación de algunos valores a variables, para posteriormente aprovechar la vulnerabilidad.

---

https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

4.10 LISTA Y DESCRIPCION DE LOS DATOS EN EL ANEXO 4 – ESCENARIO 3, QUE SIRVEN COMO BASE PARA IDENTIFICAR EL FALLO DE SEGURIDAD.

- El anexo menciona que hay una serie de fuga de información. Esto puede ser interpretado, como que la información se está desapareciendo, o que se localiza en manos de otras personas, donde no debería estar.
- Los equipos de los cuales se sospecha cuentan con un sistema operativo que a la fecha no tiene soporte y es Windows 7, el cual finalizó el 14 de enero de 2020.
- La última vez que se actualizaron los equipos, fue el 5 de febrero de 2017. De acuerdo con esta fecha, los equipos no cuentan con el parche creado por Microsoft para contrarrestar las fallas de seguridad presentadas por SMBv1.
- Estos equipos cuentan con un servicio, usado para compartir impresoras y archivos en la red. SMBv1. En este punto relaciona un protocolo que tiempo atrás, se conoce que tiene grandes fallas de seguridad y que Microsoft, recomienda encarecidamente no usar.
- Los equipos no tienen instalada la actualización que corregía la vulnerabilidad de MS17-010.

4.11 HERRAMIENTA UTILIZADA PARA ENCONTRAR FALLOS DE SEGURIDAD

Se utilizó el escáner de NMAP, primero para realizar la identificación de los puertos y servicios, se encuentran 11 puertos abiertos.

```
nmap 192.168.20.96
```

Posteriormente se ejecuta el comando

```
Nmap 192.168.20.96 –script vuln
```

Con el anterior comando, se encuentra una vulnerabilidad en Microsoft SMBv1, nombrada como ms17-010 e identificada con CVE: CVE-2017- 0143.

Esta es una vulnerabilidad que presenta un riesgo alto para cualquier sistema donde se encuentre.

El mismo escáner, ofrece accesos a sitios web, donde se pueden encontrar referencias de la vulnerabilidad encontrada.

4.12 ¿COMO AFECTA EL ATAQUE A LA MAQUINA WINDOWS 7?

SMB – Server Message Block, es un protocolo desarrollado por IBM, en el año 1983, Microsoft Windows, para compartir archivos e impresoras en una red, para poder compartir los archivos usa el puerto 445 y el protocolo de red TCP.

Cuando se lanza el ataque, se aprovecha el puerto 445 y logra que se abra una sesión del Shell en la maquina atacante, de esta forma el atacante administra la máquina, gana accesos, finaliza e inicia servicios, es decir tiene el control total.

4.13 DOCUMENTACION DE LOS PASOS EJECUTADOS PARA EXPLOTAR LA VULNERABILIDAD.

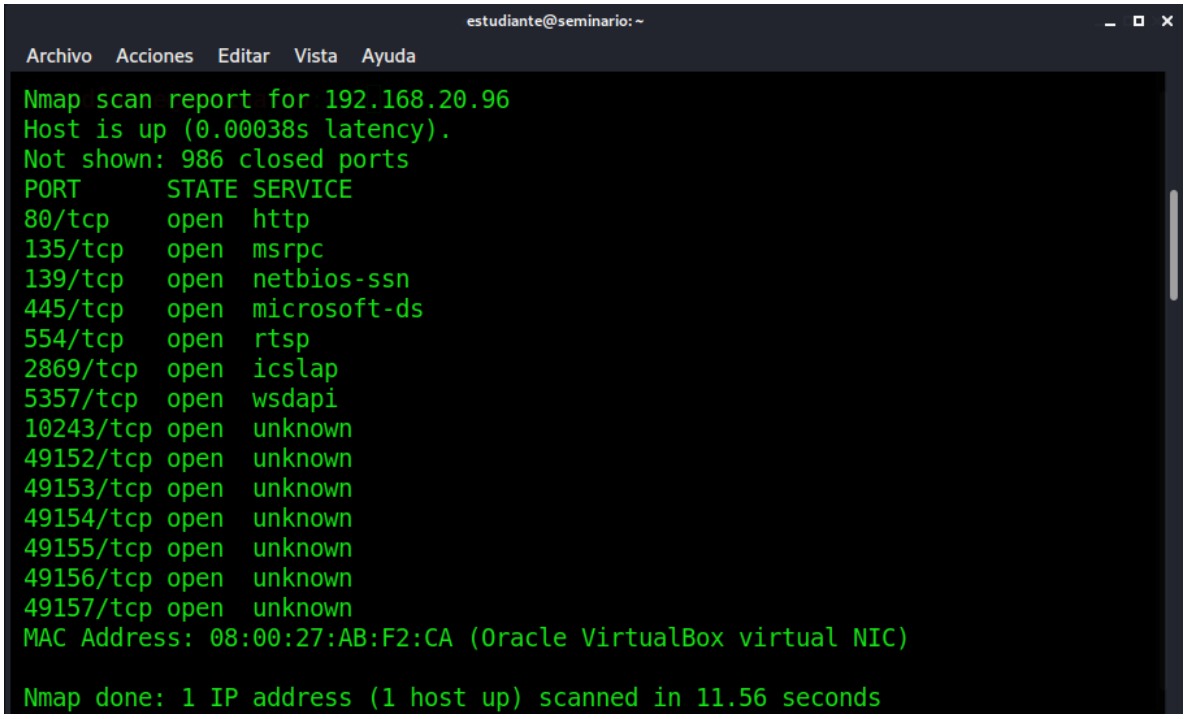
Inicialmente, se configuraron las maquinas Windows 7 y Kali Linux en red, a través de la herramienta adaptador puente.
La dirección de la máquina Windows: 192.168.20.96 y la dirección de la máquina atacante, con Kali Linux: 192.168.20.95.

Una vez conocida la IP de la máquina Windows 7, se dispone a realizar el escaneo con la herramienta NMAP, con el siguiente comando:

Nmap 192.168.20.96

Arrojando los resultados de puertos abiertos y servicios funcionando en cada puerto, de acuerdo con la información mostrada en la siguiente imagen.

Figura 5. Escaneo con NMAP



Fuente: Elaboración propia.

Entre los puertos abiertos, se encuentra el puerto 445, el cual generalmente sirve como para acceso directo a redes que no requieren el uso de la capa NetBIOS, y en el caso de la organización, es el puerto mediante el cual se comparte la impresora.

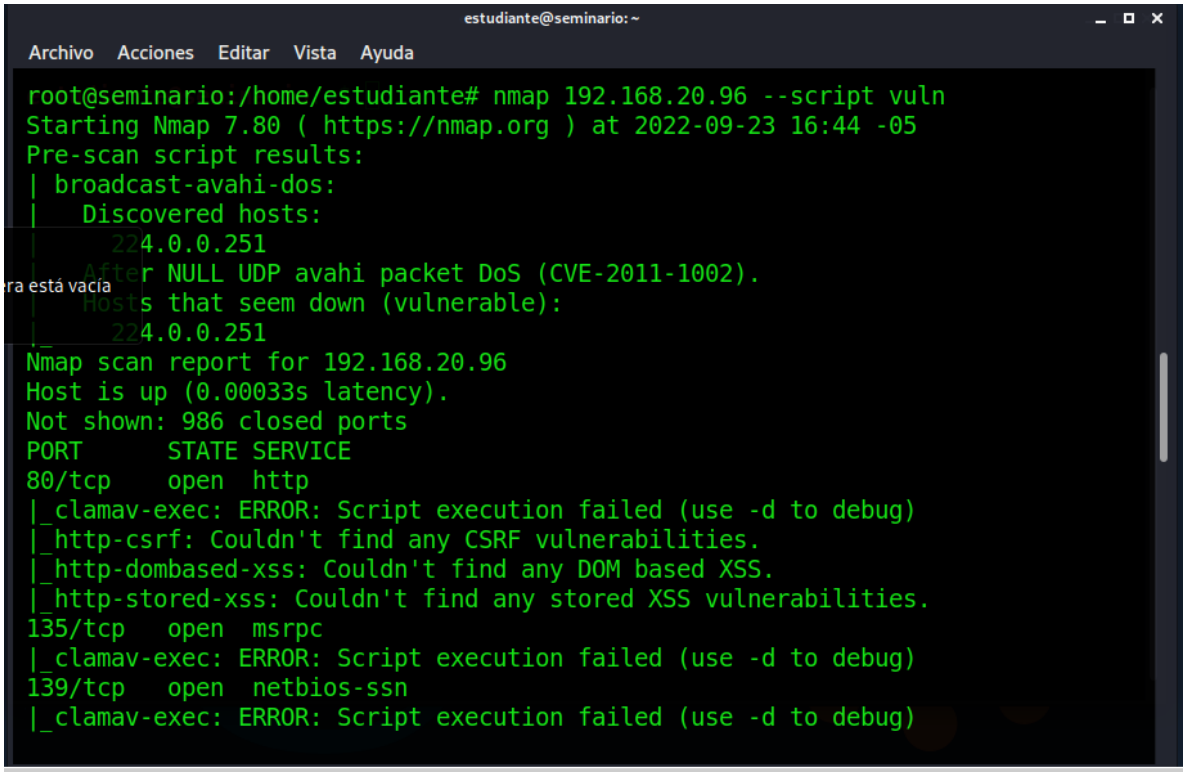
Como segundo paso, se ejecuta el siguiente comando, que muestra las vulnerabilidades encontradas en la maquina con Windows 7.

Nmap 192.168.20.96 – script vuln

Este comando permite encontrar las vulnerabilidades de acuerdo con el escaneo previo de puertos.
En la mayoría de los casos, no se presentan vulnerabilidades, sin embargo, en este aparece una relacionada justamente con la aplicación que tiene instalada la organización en los equipos Win 7.

En la imagen se aprecia que se realiza un escaneo, puerto por puerto de los 14 que se encontraron. Como resultado, algunos puertos arrojan resultados indicando que no se pudo realizar ningún hallazgo como se observan en las siguientes imágenes.

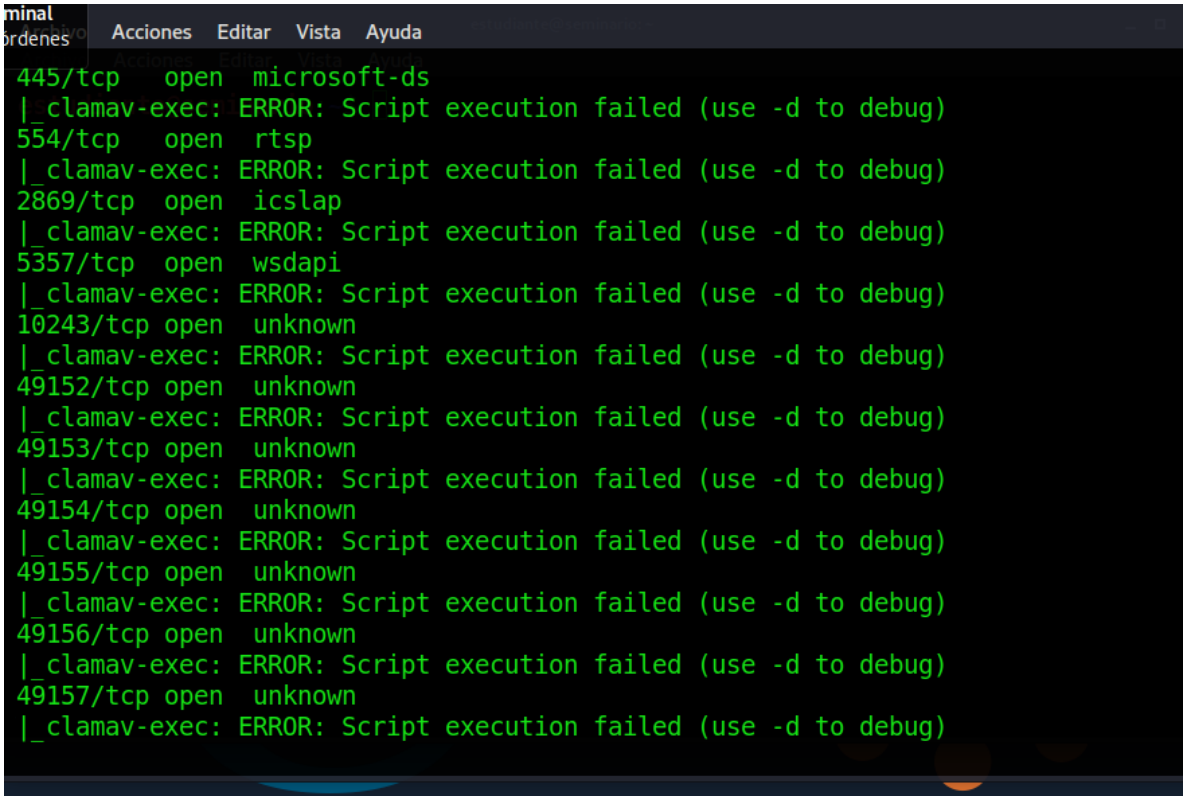
Figura 6. Escaneo de vulnerabilidades



Fuente: Elaboración propia.

Del puerto 135 al 49157, el sistema y muestra que hay una falla en la ejecución del script, y que para hacer una depuración puede usar la opción –d.

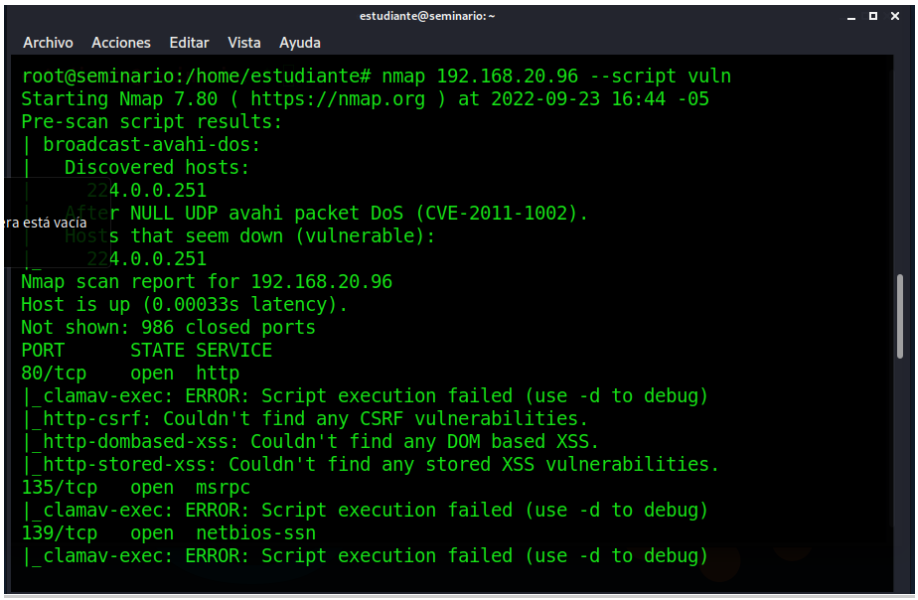
Figura 7. Escaneo de vulnerabilidades imagen 2



Fuente: Elaboración propia.

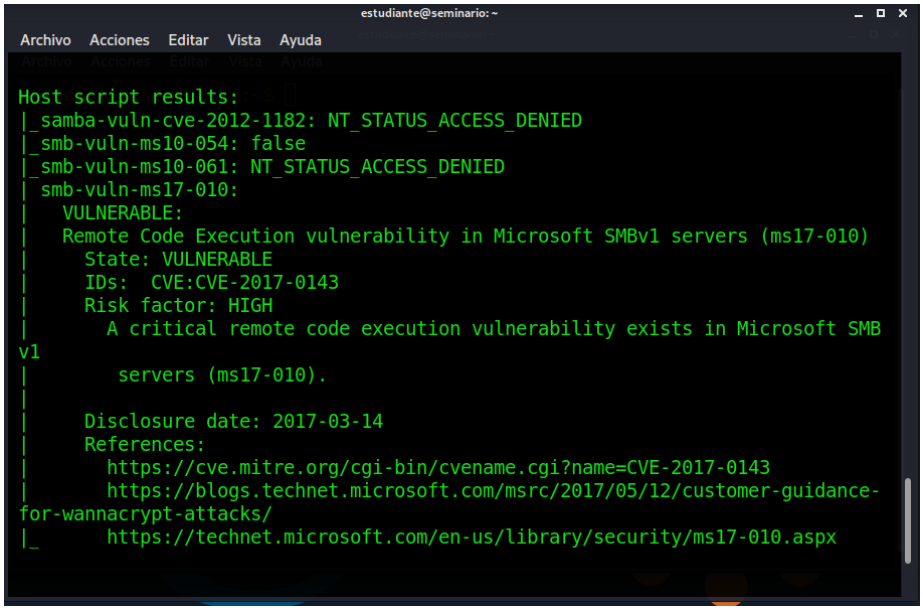
La imagen 3 y 4, corresponden a la ejecución del **script vuln** con relación al host, mostrando la vulnerabilidad CVE-2012-1182: NT_SATATUS_ACCESS_DENIED. Es la vulnerabilidad de SAMBA, la cual permite ejecutar una Shell en un equipo, desde un equipo remoto y con usuarios root.
Además, muestra que hay una vulnerabilidad en Microsoft SMBv1 servers (ms17-010), identificada con el número CVE-2017-0143, con un factor de riesgo alto y descrita como una vulnerabilidad que permite la ejecución de código remoto, descubierta en marzo del año 2017 y entrega referencias al CVE Mitre.

Figura 8. Escaneo de vulnerabilidades 3



Fuente: Elaboración propia.

Figura 9. Resultado de escaneo

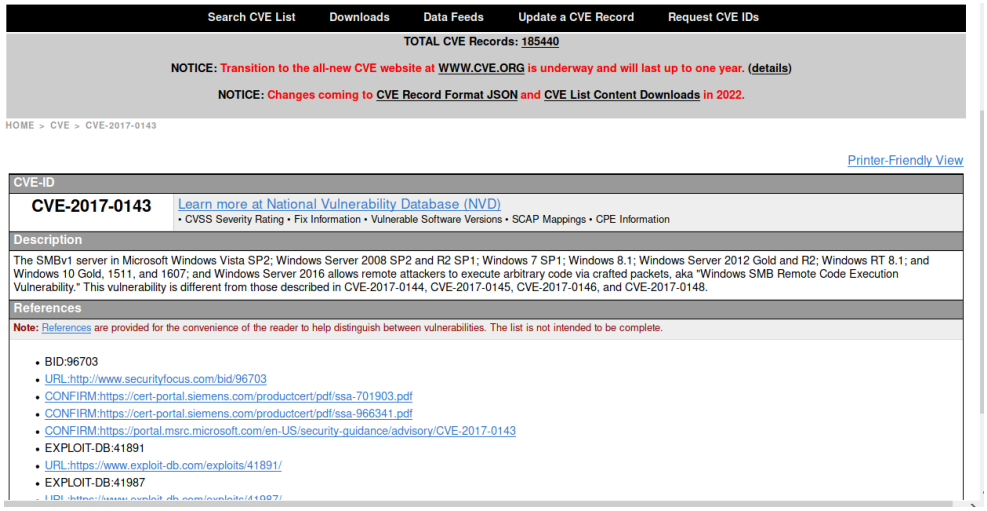


Fuente: Elaboración propia.

Después de conocer el código CVE de la vulnerabilidad, se procede a la búsqueda de información relacionada en la base de datos CVE, donde se encuentra la información que indica el servicio que posee la vulnerabilidad y los sistemas

operativos afectados con sus respectivas versiones, además de presentar los exploits con los que se puede vulnerar.

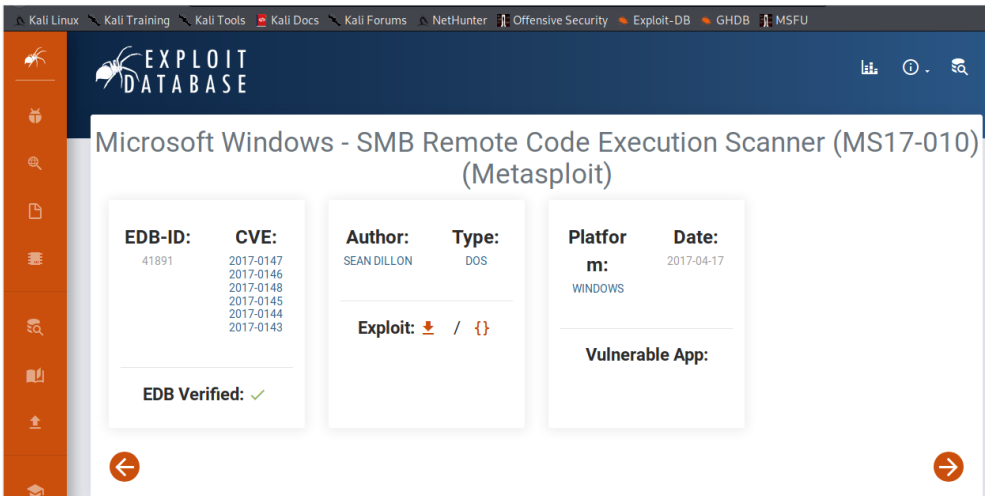
Figura 10. Consulta en CVE



Fuente: Elaboración propia

Se realiza la consulta en la página de exploit, donde se encuentran otros CVE que son afectados con el mismo exploit.

Figura 11. Base de datos de exploit



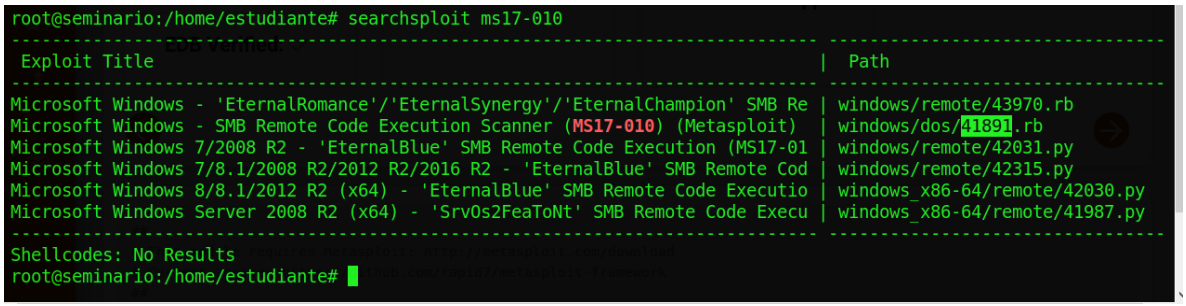
Fuente: elaboración propia.

Luego de identificar plenamente la vulnerabilidad, y con los datos obtenidos, se continua con la herramienta NMAP, en la búsqueda del exploit, a través del uso del siguiente comando:

Searchsploit ms17-010

El valor MS17-010, arroja una lista de resultados, como se observa en la siguiente imagen, al lado izquierdo, el nombre del exploit y al lado izquierdo la ruta donde se encuentra. No siempre se encontrarán los exploit en la base de datos, aunque es muy completa, algunas veces pueden ser creados o descargados de otros sitios web.

Figura 12. Busqueda del exploit



Fuente: Elaboración propia.

De acuerdo con la imagen anterior, se encuentra el exploit, indicando que a través de la herramienta metasploit puede ser penetrado y se identifica con el código 41891.

Para continuar y tomando en cuenta la información anterior, se procede a iniciar la consola de metasploit, ejecutando el siguiente comando:

Msfconsole

En la siguiente imagen, se muestra el inicio de la consola. Metasploit es un software, equipado con herramientas que ayudan a explotar las vulnerabilidades más conocidas, a través de Payloads que son los códigos que realizan el trabajo.

Metasploit también dispone de otros módulos que funcionan como auxiliares, encoders que sirven para evadir antivirus o sistemas de seguridad.

Para continuar con el proceso de explotación, se hace uso del siguiente comando, el cual devuelve los módulos que están relacionados con la búsqueda.

Search 2017-0143

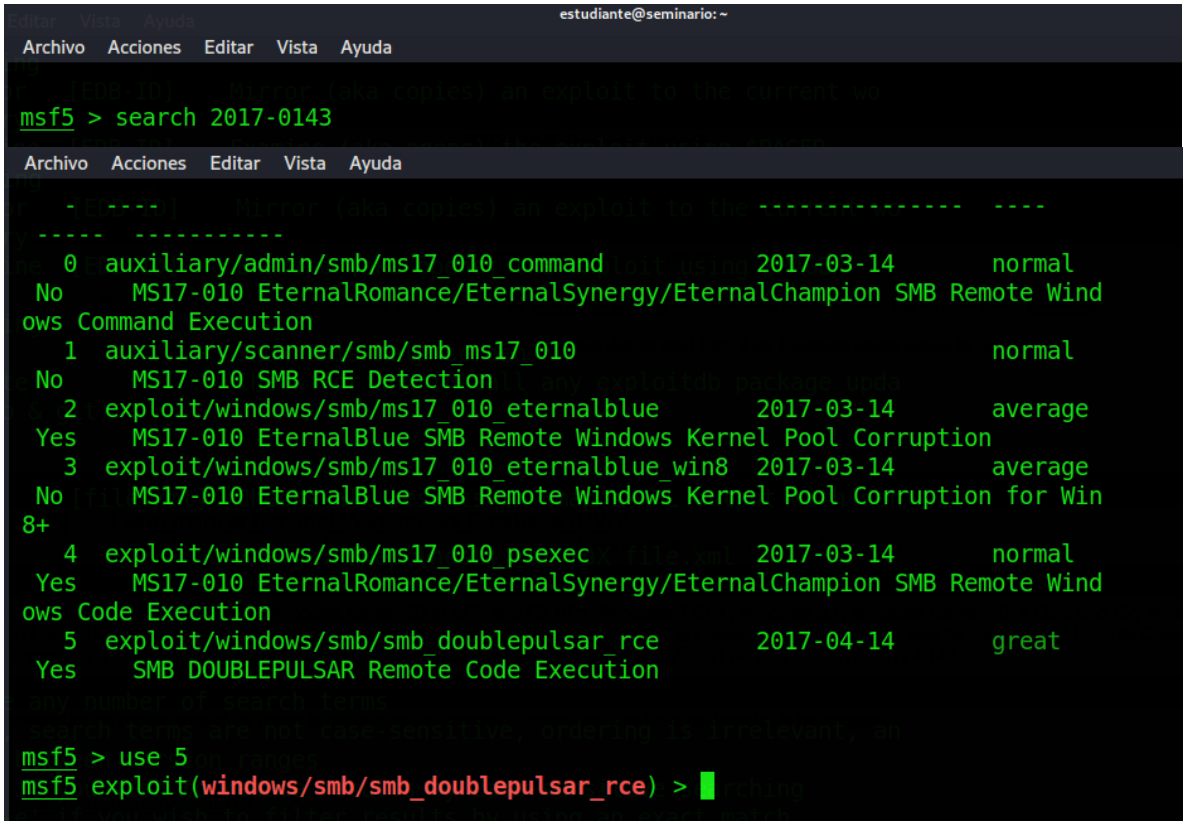
En la imagen 8, se encuentran 6 opciones, de las cuales 4 corresponden a exploit y puede ser configurado para realizar el ataque, a fin de confirmar que esta fue la forma en la que se estaba produciendo la fuga de información.

En la misma imagen, se hace uso del comando:

Option 3

opción para elegir el exploit o el script que se desea trabajar.

Figura 13. Búsqueda del exploit 2



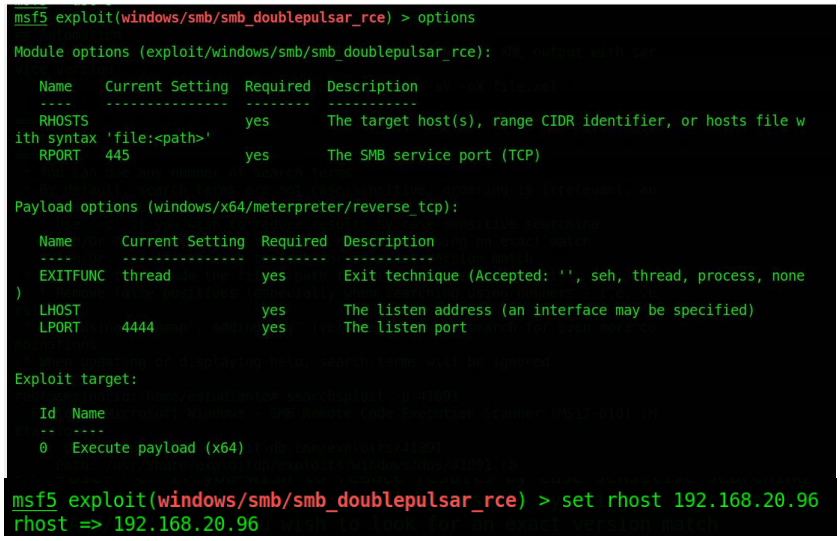
Fuente: propia.

Al ejecutar options para visualizar la configuración dentro de ese modulo, se usa el comando set, para cambiar los valores de las variables, como esa muestra en la siguiente imagen.

Options

Set rhosts 192.168.20.96

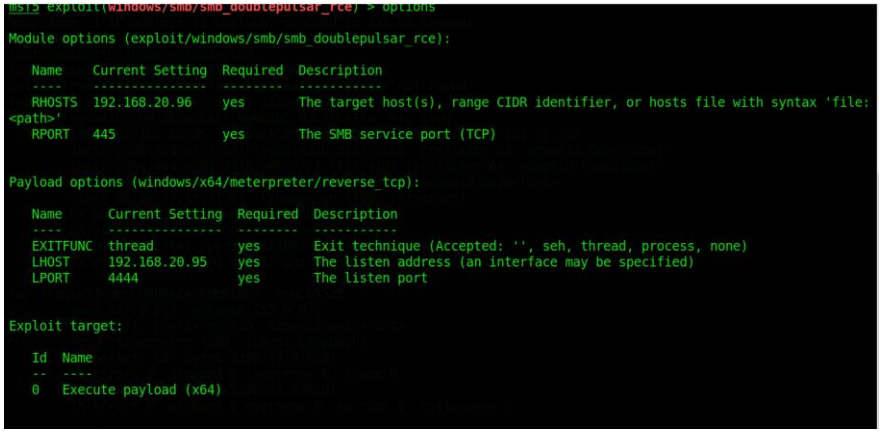
Figura 14. Comando Options y Set



Fuente: Propia

después de configurar el host remoto y el host local, queda como se muestra en la imagen.

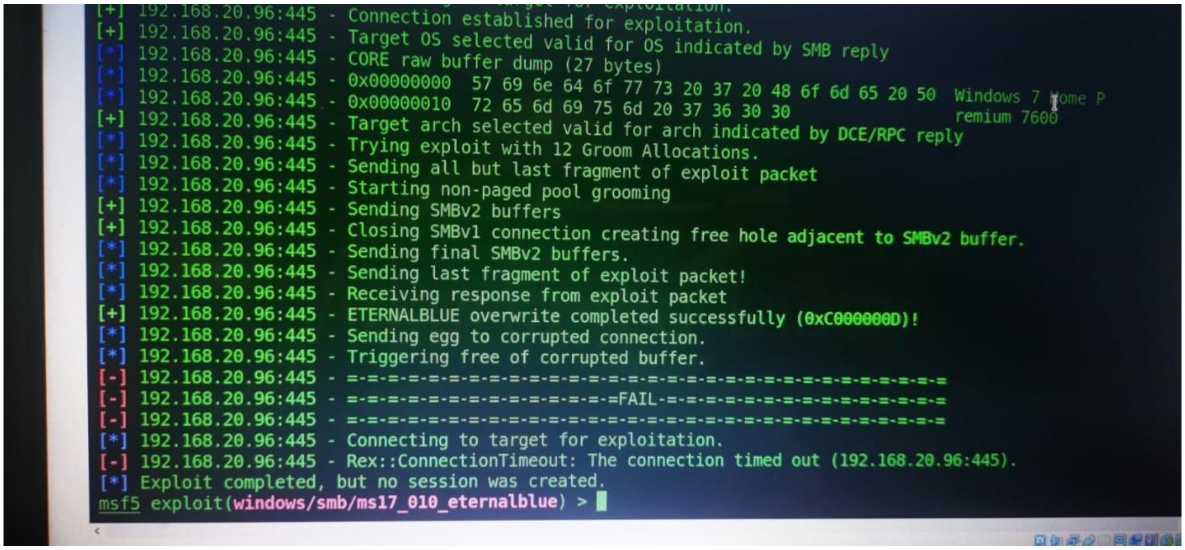
Figura 15. Configuración lista



Fuente: Propia

El siguiente paso es la ejecución del exploit, que crea la sesión del Shell y lo devuelve para que sea ejecutado desde la maquina atacante, donde se tiene la posibilidad de acceder a la maquina víctima.

Figura 16. Ejecución del exploit



Fuente: Propia

4.14 PRIMEROS PASOS ANTE UN ATAQUE

Considero que una de las primeras preguntas, sería, cuáles son los servicios afectados, con el fin de determinar el impacto inicial que está teniendo el ataque y además porque, puede dar indicios del tipo de incidente presentado.
Seguidamente, realizar revisión de los logs, herramientas de monitoreo, firewalls, consolas de antivirus.

De acuerdo con la documentación consultada, una organización debe tener un plan de contingencia que le permita tomar una decisión en el momento de presentarse un ataque, que evite la propagación del daño realizado.
Por lo anterior, debe existir una estrategia de contención, acorde al tipo de incidente, debe estar adecuadamente documentada, de modo que se puedan tomar decisiones en forma rápida.

Un ejemplo, se presenta en la siguiente imagen, tomada del documento de gestión de incidentes de MinTIC.

Figura 17. Ejemplo de estrategia para atención de incidentes

Incidente	Ejemplo	Estrategia de erradicación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web
Intrusión	Instalación de un rootkit	Reinstalación del equipo y recuperación de datos

Fuente: Documento de gestión de incidentes MinTIC

Otra acción para realizar en primera instancia es dar aviso al Cai Virtual de la policía Nacional, quienes también brindan asesoría y judicializan posteriormente.

4.15 MEDIDAS DE JARDENIZACION PARA EVITAR LA PRODUCCION DEL MISMO ATAQUE

- Actualizar a un sistema operativo con Soporte, y en caso de no ser posible, realizar las actualizaciones necesarias al sistema operativo Windows 7 y la consulta de sus vulnerabilidades en bases de datos, para subsanarlas.
- Realizar la actualización del protocolo SMBv1.
- Deshabilitar los puertos y servicios que no son necesarios.
- Implementar alternativas al uso compartido de impresoras, que no pongan en riesgo la seguridad del sistema.
- Implementar un sistema de monitoreo IDS IPS, con el fin de realizar seguimientos a los escaneos de puertos o tráfico malicioso.
- Configurar un firewall adecuado para las necesidades de la organización.
- Capacitar a los usuarios en temas de ciberseguridad.

4.16 DIFERENCIAS ENTRE UN EQUIPO BLUE TEAM Y UN EQUIPO DE RESPUESTAS A INCIDENTES INFORMATICOS

Un equipo blue team, tiene un enfoque general de fortalecimiento de la seguridad, debe crear estrategias de defensa, retroalimentarse de los hallazgos realizados por el equipo red.
El equipo de respuesta a incidentes tiene un enfoque más específico, debe responder en caso de presentarse un incidente, por lo que su actuación tiene espacio en los momentos específicos de los ataques.

4.17 ¿SI DENTRO DE UN EQUIPO BLUETEAM LE INDICAN QUE DEBE TRABAJAR CON CIS "CENTER FOR INTERNET SECURITY" USTED LO UTILIZARÍA PARA QUE FIN?

Tomando en cuenta que CIS, es una comunidad global de profesionales de TI, que se han agrupado con el fin de generar estándares de buenas prácticas en seguridad alrededor de la prevención, protección, respuesta y recuperación de incidentes informáticos; cuando dentro de un equipo azul solicitan trabajar con CIS, se usaría para aplicar sus recomendaciones de buenas prácticas, enfocadas en la protección, según sea el caso. De esta forma obtener un nivel de protección, basados en los análisis realizados por un equipo de profesionales que basan sus recomendaciones, en sus experiencias y en estudios de personas con grandes conocimientos en la materia[10].

4.18 EXPLIQUE Y REDACTE LA FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LOS QUE ES UN SIEM.

Security Information and event Management.SIEM, es un software diseñado y capacitado para detectar, responder y detener amenazas informáticas.
El SIEM, centraliza todos los registros de los logs de todos los sistemas, de esta forma el administrador tiene la posibilidad de contar con un conglomerado de información, que para el caso de grandes empresas o industrias es una carga menos, dado que está ahorrando un esfuerzo que le permite realizar análisis y correlacionar eventos en tiempo real[11].

Funciones:

UEBA: Tomando como base el comportamiento anómalo de usuarios y equipos, se genera una analítica, de especial relevancia a la hora de detectar intrusiones.

SOAR: Son sistemas con los que el SIEM, ofrece una respuesta a incidentes.

---

[10] CIS. Center for Internet Security. Sobre nosotros. [Sitio web]. Elpais.com. [Consultada: 30 de septiembre de 2022]. Disponible en: https://www.cisecurity.org/abou1t-us

[11] NSIT. ¿Qué es SIEM en seguridad informática? Alcance e implementación. [Sitio web]. Nsit.com.co. [Consultada: 30 de septiembre de 2022]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

BIGDATA Y ANALYTICS: Para estar a la vanguardia con los tipos de ataques actuales, una solución SIEM, debe tener la capacidad de generar aprendizajes de máquina para detectar lo desconocido.

FUENTES PROPIAS DE INTELIGENCIA: A través del registro de indicadores de compromiso IoC e Indicadores de ataque IoA.

CUMPLIMIENTO: Esta relacionado con la identificación de estar alineado con las normas, leyes que proponen controles como HIPPA (Seguridad de información del sector Salud), PIC-DSS (Protección de datos de tarjetahabientes), GDPR (Protección de datos personales), NIST (Controles de seguridad y privacidad para las agencias del gobierno)

Centralización de la información de seguridad: El SIEM, reúne información de seguridad de todos los sistemas, como correo electrónico, ERP, Mainframes, entre otros. para que los eventos puedan ser correlacionados y analizados.

Automatización de las tareas: Permite la creación de tareas acorde con las necesidades de análisis que se tengan.

Respuesta automática a incidentes considerados como maliciosos. Por su naturaleza y la información que centraliza, es posible la configuración acorde a eventos específicos.

Aumento de eficiencia en el tiempo de respuesta a ataques. Esta función, asociada al punto anterior, dado que tiene información que se convierte en variables que pueden ser activadoras de alguna acción especifica en respuesta a un ataque.

Funcionalidades técnicas:

- Mitre Attack: Incluye etiquetas de las tácticas, y formas de ataque, con esto se reduce la fatiga de alertas.

- Tener la capacidad de procesar otras fuentes de inteligencia como TAXII o STIX.

- Integrar servicios en la nube a través de APIS.

- Capacidad de desarrollar un ecosistema de protección basado en aplicaciones desarrolladas por los fabricantes.

4.19 ALGUNAS HERRAMIENTAS DE CONTENCION DE ATAQUES INFORMATICOS

Existen muchas herramientas con fines de protección de la información, tanto de hardware como de software, entre ellas se pueden mencionar las siguientes:

Firewall: Esta herramienta puede ser de tipo software o hardware. Por el nombre se infiere que actúa como un muro o una pared, impidiendo que al sistema detrás de ella, ingrese información que no tiene permiso.
Es una herramienta de uso imprescindible en la protección de redes privadas o de algunos sistemas, sin embargo, su efectividad está muy relacionada con la configuración que se realice.
Aunque este tipo de herramientas en muchas ocasiones pueden ser evadidas por los atacantes, si logran dificultar el ingreso y un análisis adecuado y oportuno podría dar luces de algún intento de ataque.

Existen Firewall, con propósitos específicos, como por ejemplo la protección a bases de datos, otros que incluyen funciones adicionales a las comunes de filtrado del tráfico, ofreciendo una amplia gama de opciones de contención.

Endpoint en modo de contención de ataques: es un sistema que realiza un monitoreo de los intentos de conexión a los computadores de una red, a través del servicio RDP. Cuando se detectan estos intentos fallidos, el sistema genera un ataque de fuerza bruta contra RDP, generando de esta forma una contención.

Esta herramienta actúa en diferentes etapas del ataque, en una de sus etapas, puede llegar a bloquear puertos, y detectar cuando se ha finalizado el ataque.
Ofrece un tablero de control que muestra diferentes etapas en las que trabaja la herramienta, realizando la contención.

Software antivirus: Esta herramienta, aunque parece de mínimo impacto, tiene una importante función al momento de bloquear archivos de malware, que pueden ser la parte inicial de un ataque y de este modo logran ofrecer protección a los sistemas y a la información.

Los antivirus también han evolucionado en cuanto a las formas de detección del programa maligno, dado que mantener sus sistemas tradicionales los haría inviables. Han orientado sus programas al análisis del comportamiento del usuario, usando técnicas de inteligencia con sus bases en Data Minig y Big Data, logrando impedir la ejecución de procesos sospechosos o peligrosos.

5. CONCLUSIONES

- Con la realización del informe, se concluyó que para el desarrollo del trabajo realizado por los equipos blue team y red team, es necesario como primera medida tener conocimiento de la normatividad que legisla en cada país, contar siempre con la autorización del cliente y apoyarse en las fases del pentesting.

- Los equipos blue team y red team, son una buena estrategia en el fortalecimiento de la seguridad de las organizaciones, aunque un alto porcentaje de ellas no cuenta con los recursos para sostener su funcionamiento y reciben asesorías que tratan de disminuir la brecha de seguridad con herramientas de contención, sin embargo, no se realizan pruebas para evaluarlo.

- Uno de los aspectos importantes para disminuir la cantidad de delitos que se cometen a través del uso de herramientas informáticas, o para realizar daños a la información o infraestructura críticas, es el contar con una legislación fuerte, actualizada, que debe ser complementada con sus respectivas denuncias por parte de los afectados y una investigación oportuna por parte de las autoridades.

- Las herramientas para contención de ataques pueden llegar a ser muy efectivos, sin embargo, el factor humano siempre va a jugar un papel importante, en la configuración que es lo que realmente determina su funcionamiento.

- De la misma forma sucede con las herramientas SIEM, es necesario contar con un recurso humano calificado que pueda analizar la correlación de información de diferentes fuentes de esta forma atienda oportunamente las alertas que tales sistemas producen.

- También se concluyó que existen numerosas herramientas gratuitas que ofrecen documentación relacionada con buenas prácticas que deben seguir en las industrias, para lograr mejorar los niveles de seguridad, lo que indica que hay mucho por hacer en las organizaciones, sin que eso represente un alto costo, solo es necesario la voluntad, involucrar la gobernanza de la organización para tomar acciones que disminuyan la brecha.

6. RECOMENDACIONES

Seguir e implementar hasta donde sea posible, los estándares de seguridad, como la ISO 27001, el CIS, recomendaciones del Ministerio de las TIC, entre otros, son acciones base para disminuir las brechas de seguridad en los sistemas de cualquier organización.

Es indispensable conocer el inventario de activos que se tiene en la organización y gestionarlo, es decir, conocer cuáles son las vulnerabilidades de cada equipo, software, conocer la versión en funcionamiento y las vulnerabilidades de esa versión, mantener este software debidamente actualizado y parchado.

Aparte de asegurar los sistemas de información, de configurar barreras de contención o de protección, es necesario realizar pruebas, para determinar hasta que nivel se logra la confiabilidad en ellas.

Todos los aspectos anteriores son necesarios, sin embargo, la correlación entre ellos, el análisis de la información generada por esas herramientas, los resultados de las pruebas de seguridad generan una cantidad de datos que bien vale la pena analizar y así, obtener comportamientos normales y anormales del funcionamiento de los sistemas y poder identificar de forma oportuna cuando está sucediendo un ataque.

7. VIDEO DE SUSTENTACION

https://youtu.be/lUmROcg7YIY

BIBLIOGRAFÍA

CIS. Center for Internet Security. Sobre nosotros. [Sitio web]. Elpais.com. [Consultada: 30 de septiembre de 2022]. Disponible en: https://www.cisecurity.org/abou1t-us

Computadoras. Para que sirve y como se deshabilita el puerto 445. [Sitio web]. Clasesordenador.com. [Consultada: 9 de septiembre de 2022]. Disponible en: https://www.clasesordenador.com/para-que-sirve-y-como-deshabilitar-este-puerto-tcp-445/

Departamento nacional de planeacion. CONPES 3701. [Sitio web]. Colaboración.dnp.gov.co. [Consultada: 9 de septiembre de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (5, enero,2009). Por medio de la cual “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En Diario Oficial. Enero, 2009. Nro.47223. p. 1.

COPNIA. Código de ética. [Sitio web]. Copnia.gov.co. [Consultada: 8 de septiembre de 2022]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

El país. Esta es la cronología de como se ha desarrollado el caso Andrómeda. [Sitio web]. Elpais.com. [Consultada: 9 de septiembre de 2022]. Disponible en: https://www.elpais.com.co/colombia/esta-es-la-cronologia-de-como-se-ha-desarrollado-el-caso-andromeda.html

Enter.co. La historia oculta detrás de la fachada de Andrómeda. [Sitio web]. Enter.co. [Consultada: 9 de septiembre de 2022]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Greenbone open vas. OpenVas. [Sitio web]. Openvas.org. [Consultada: 29 de agosto de 2022]. Disponible en:https://www.openvas.org/

Hackplayers. CVE-2012-1182: Ejecución de código remoto en Samba. [Sitio web]. Techcommunity.microsoft.com. [Consultada: 23 de septiembre de 2022]. Disponible en: https://www.hackplayers.com/2012/11/cve-2012-1182-samba-vulnerability.html

Keepcoding. Que es exploitDB. [Sitio web]. Keepcoding.io. [Consultada: 29 de agosto de 2022]. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/

Microsoft. Dejar de usar SMB1. [Sitio web]. Techcommunity.microsoft.com. [Consultada: 23 de septiembre de 2022]. Disponible en: https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

MINTIC. Normograma. [Sitio web]. Mintic.gov.co. [Consultada: 9 de septiembre de 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

Nmap.org. Guía de referencia de Nmap. [Sitio web]. Nmap.org. [Consultada: 29 de agosto de 2022]. Disponible en: https://nmap.org/man/es/index.html

NSIT.Que es SIEM en seguridad informática? Alcance e implementación. [Sitio web]. Nsit.com.co. [Consultada: 30 de septiembre de 2022]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

Openwebinars. ¿Qué es metasploit framework?. [Sitio web]. Larepublica.co. [Consultada: 23 de septiembre de 2022]. Disponible en: https://openwebinars.net/blog/que-es-metasploit/

Periódico La república. La información se ha convertido en el “oro” para las empresas en la era de los datos. [Sitio web]. Larepublica.co. [Consultada: 23 de septiembre de 2022]. Disponible en: https://www.larepublica.co/internet-economy/la-informacion-se-ha-convertido-en-el-oro-para-las-empresas-en-la-era-de-los-datos-3391144#:~:text=%E2%80%9CEn%202021%2C%20en%20Colombia%20el,y%20bloque%C3%B3%20150.000%20eventos%20maliciosos%E2%80%9D.

Periódico La república. Cantidad de ciberataques aumentaron 4% en América Latina durante el año pasado. [Sitio web]. Larepublica.co. [Consultada: 3 de octubre de 2022]. Disponible en: https://www.larepublica.co/globoeconomia/cantidad-de-ciberataques-aumentaron-4-en-america-latina-durante-el-ano-pasado-3326053

Semana. El informe que sacudió el caso de la fachada Andrómeda. [Sitio web]. Semana.com [Consultada: 9 de septiembre de 2022]. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

WatchGuard. Modo de conteción de ataques RDP. [Sitio web]. watchguard. [Consultada: 30 de septiembre de 2022]. Disponible en: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Endpoint-Security/monitor-threats/IOAs/rdp-attack-containment-mode.html

Welivesecurity. Penetración Test, ¿En qué consiste? [Sitio web]. kWelivesecurity.com. [Consultada: 1 de septiembre de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/