CONTROL O MITIGACION DE VULNERABILIDADES EN EL AREA DE TECNOLOGIAS DE LA EMPRESA WHITEHOUSE SECURITY E IMPLICACIONES ETICAS Y LEGALES DE LA SEGURIDAD INFORMATICA.

MEDARDO MARCELINO PEREZ RENTERIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CEAD-QUIBDO - 2020-II

CONTROL O MITIGACION DE VULNERABILIDADES EN EL AREA DE TECNOLOGIAS DE LA EMPRESA WHITEHOUSE SECURITY E IMPLICACIONES ETICAS Y LEGALES DE LA SEGURIDAD INFORMATICA.

SEMINARIO ESPECIALIZADO EQUIPOS ESTRATEGICOS

BLUE TEAM & RED TEAM

ETAPA 5 – SOCIALIZACION DEL INFORME TECNICO

PROFESOR
JHON FREDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CEAD-QUIBDO - 2020-II

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Quibdó, 09, 11, 2020

Dedico este informe técnico a mis hijas y a mi mujer por darme fortaleza y apoyo para avanzar con esta especialización.

Agradecimientos

Agradecimientos para el equipo de docentes de la universidad y en especial al **Ingeniero John Fredy Quintero** por su apoyo y asesoramiento oportuno.

Contenido

Lista de tablas

Lista de figuras

Glosario

RedTeam: En muchos entornos profesionales lo definen como un test de intrusión, en el cual se pueden ver vulnerabilidades y fallos en la estructura tecnológica de una organización.

BlueTeam: (seguridad defensiva): es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva (Bruno, 2020).

CIS o Center for Internet Security: organización sin fines de lucro impulsada por la comunidad, responsable de CIS Controls ® y CIS Benchmarks ™, las mejores prácticas reconocidas a nivel mundial para proteger los sistemas y datos de TI (Microsoft, 2020).

Access Rights Manager: es una herramienta ligera de AD y Azure AD- optimiza la incorporación de usuarios y facilita una rápida respuesta a las solicitudes de eliminación de cuentas.

SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management): es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estand de datos y priorización de amenazas (People, 2020).

Servidor Proxy: Un proxy es un equipo informático que hace de interm entre las conexiones de un cliente y un servidor de destino (Barboza, 2020).

Hardening: En informática, el hardening o endurecimiento es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuanto más funciones desempeñan (Innovación, 2020).

CIS o Center for Internet Security: es una entidad sin fines de lucro cuya misión es 'identificar, desarrollar, validar, promover y mantener soluciones de mejores prácticas para la ciberdefensa'.

Resumen

Con el aumento de los ataques cibernéticos de hoy en día, es importante para las empresas e instituciones evaluar el nivel de protección que tienen sus sistemas informáticos. Para realizar esta evaluación se requiere realizar un test de penetración altamente técnico y especializado. Esta evaluación debe ser comprensible para poder priorizar y diseñar una correcta estrategia de mitigación.

En el presente documento se hace una descripción de la empresa Whitehouse Security, la cual requiere previamente una instalación de un banco de trabajo, el cual hace necesario la aplicabilidad de las strategias Red Team & Blue Team, 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 The WhiteHouse Security., realizar pruebas de penetración, la metodología empleada, fases y resultados de cada una de estas, así como las conclusiones y recomend para mitigar las vulnerabilidades encontradas.

1. Introducción

Atraves del desarrollo del curso seminartio especializado se pretende utilizar estrategias Red Team & BlueTeam, con el fin de responder a los interogantes planteamientos en las diferentes etapas estrategicas, presen en los eccenarios propuesto por la empresa casa Whitehouse Security, y asi poner en marcha plan para detectar y exploatar vulnerabilidades encontradas, de igual forma echar un vistazo a las implicaciones éticas y legales, teniendo como producto final un informe técnico determinante que permita presentar los detalles de seguridad informatica en la empresa.

2. Objetivos

2.1 Objetivo general

Realizar metodos de control de contención o mitigacion en vulnerabilidades presentes en el area de tecnologias de la empresa Whitehouse Security y conocer temas relacionados con implicaciones eticas y legales de la seguridad informatica.

2.2 Objetivos específicos

- Comprobar los procesos de los equipos de los Red Team & Blue Team de la empresa y tener presente los aspectos éticos y legales
- Identificar vulnerabilidades del escenario propuesto
- Posibles soluciones para mitigar las vulnerabildad encontradas
- Realizar informe Tecnico

3. *Desarrollo de la actividad*

Mediante los avances de las difentes etapas del seminario especializado se examinaron diversos ambitos prácticos y teóricos, atraves de varias fases dando como producto final un informe técnico ralacionando las actividades de las cinco faces. Se llevo acabo un analisis con varios programas teniendo encuenta las faces del pentesting.

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias, para el desarrollo de la práctica utilizamos las siguientes herramientas recomendadas por al empresa WHITEHOUSE SECURITY.

3.1 Metasploit

Metasploit framework es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad y equipos Red Team y Blue Team. Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda entests de penetración «Pentesting» y el desarrollo de firmas para sistemas de detección de intrusos. , utiliza una línea de comandos msfconsole y cuenta con una interfaz gráfica puede ejecutarse tanto en Windows como en Linux. Es una herramienta desarrollada mayormente en Perl y Ruby con posibilidad de integrar otro tipo de script en diferentes lenguajes ya sea Python, Perl, etc (Rizaldos, 2018).

Cuenta con una gran lista de exploits con la posibilidad de interactuar con herramientas externas como Nessus, Nmap,etc.

3.2 Nmap

Nmap es el programa gratuito por excelencia para descubrir todos los hosts que hay en una o varias redes**,** así como qué puertos tiene abiertos un determinado host. Abreviatura de Network Mapper, es una herramienta gratuita de código abierto para la exploración de vulnerabilidades y la detección de redes. Los administradores de red utilizan Nmap para identificar qué dispositivos se están ejecutando en sus sistemas, descubrir los hosts disponibles y los servicios que ofrecen, encontrar puertos abiertos y detectar riesgos de seguridad (Luz, 2019).

3.3 OpenVas

un escáner de vulnerabilidades de uso libre utilizado para la identificación y corrección de fallas de seguridad. Un escáner de vulnerabilidades de uso libre utilizado para la identificación y corrección de fallas de seguridad. Se trata de un framework que tiene como base servicios y herramentas para la evaluación de vulnerabilidades y puede utilizarse de forma individual o como parte del conjunto de herramientas de seguridad incluidas en OSSIM (Open Security Information Management) (welivesecurity, 2014).

3.4 Explotad

Un exploit es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware. (base de datos de exploits o brechas de seguridad) es un directorio web donde muchos hackers cuelgan vulnerabilidades de aplicaciones y cómo aprovecharse de ellas, con instrucciones especificas (Copyright, 2020).

Cada día aparecen nuevas y es un lugar donde se puede aprender mucho, pero también se puede hacer daño a terceros si hacemos un mal uso de sus instrucciones y lo hacemos con fines malévolos.

CVE: Los puntos vulnerables y las exposiciones comunes (CVE) conforman una lista de fallas de seguridad informática que se encuentra disponible al público. Por lo general, cuando alguien habla de un CVE, se refiere al número de identificación de CVE que se le asigna a una falla de seguridad (hat, 2020).

Los CVE permiten que los especialistas en TI coordinen sus esfuerzos para priorizar y solucionar estos puntos vulnerables y mejorar la seg-dad de los sistemas informáticos.

3.5 Banco de Trabajo

Un **banco de trabajo** es una mesa especialmente adaptada o acondicionada a una tarea específica. El banco suele ser robusto y puede tener tanto una práctica en su diseño como complejas especificaciones técnicas que le otorguen el nivel de herramienta.

En nuestro caso crearemos un banco de trabajo con las siguientes herramientas o software informático: Virtualbox, Kali Linux, Win7-SE2020, Win7-SE2020-X64

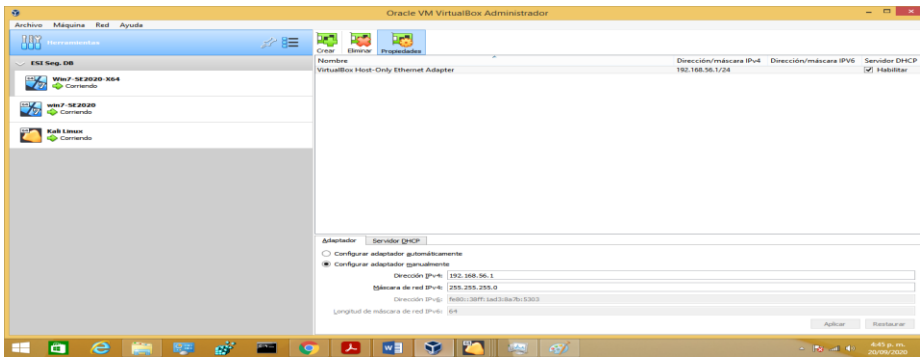
3.5.1 Virtualización

La virtualización crea un entorno informático simulado, o virtual, en lugar de un entorno físico. A menudo, incluye versiones de hardware, sistemas operativos, dispositivos de almacenamiento, etc., generadas por un equipo. Esto permite a las organizaciones particionar un equipo o servidor físico en varias máquinas virtuales. Cada máquina virtual puede interactuar de forma independiente y ejecutar sistemas operativos o aplicaciones diferentes mientras comparten los recursos de una sola máquina host.

Para crear el laboratorio o banco de trabajo utilizamos el virtualizador Virtualbox

VirtualBox: es una aplicación que sirve para hacer máquinas virtuales con instalaciones de sistemas operativos. Esto quiere decir que si tienes un ordenador con Windows, GNU/Linux o incluso Mac OS, puedes crear una máquina virtual con cualquier otro sistema operativo para utilizarlo dentro del que estés usando (Fernández, 2020).

Figura 1: Imagen Virtualbox



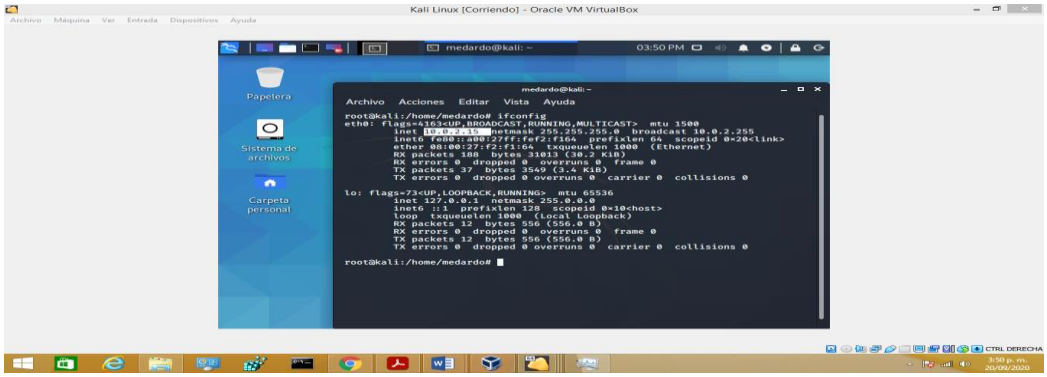
Fuente: Medardo Perez Rentería

3.5.2 Kali Linux

Kali Linux es una distribución la cual contiene su propia colección de cientos de herramientas de software, especialmente hechas a medida para los usuarios; como profesionales en pruebas de penetración y otros profesionales de seguridad. También viene con un programa de instalación para completamente configurar Kali Linux como el sistema operativo principal en cualquier computadora.

Es muy parecido a todas las otras distribuciones Linux existentes, pero existen otras características las cuales diferencian a Kali Linux, muchas de las cuales se adaptan a necesidades específicas de los profesionales en pruebas de penetración. A continuación se exponen algunas de estas (Singh, 2019, pág. 27).

Figura 2: Máquina virtual Kali Linux



Fuente: Medardo Perez Rentería

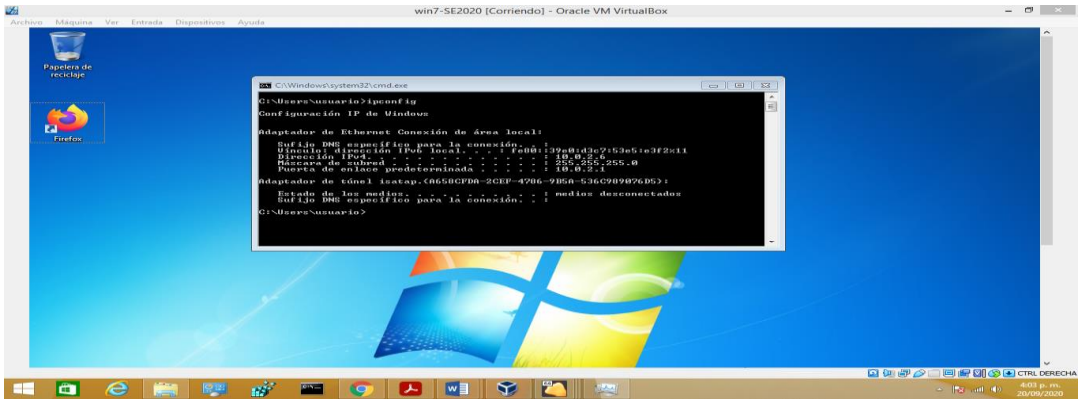
3.5.3 Win7-SE2020 - X32

Es un sistema operativo creado por Microsoft. Consiste en un conjunto de programas que permiten la ejecución de los recursos que tiene un ordenador. El significado del término (windows, ventanas) hace alusión a su interfaz gráfica, que presenta un modelo basado en tareas y compartimentos independientes, con sus propios menús y controles.

Una CPU de 32 bits puede procesar 4 bytes de datos en un ciclo de CPU ya que 8 bits son iguales a 1 byte. Entonces, si el tamaño de los datos a procesar es mayor a 4 bytes, requeriría que la CPU vaya a otro ciclo para procesar los datos restantes.

Hoy en día, los procesadores de 32 bits se han vuelto casi obsoletos. Incluso un ordenador de 10 o 12 años de edad seguramente esté ejecutando un procesador de 64 bits (Calvo, 2015).

Figura 3: Máquina virtual Win7-SE2020 – X32



Fuente: Medardo Perez Rentería

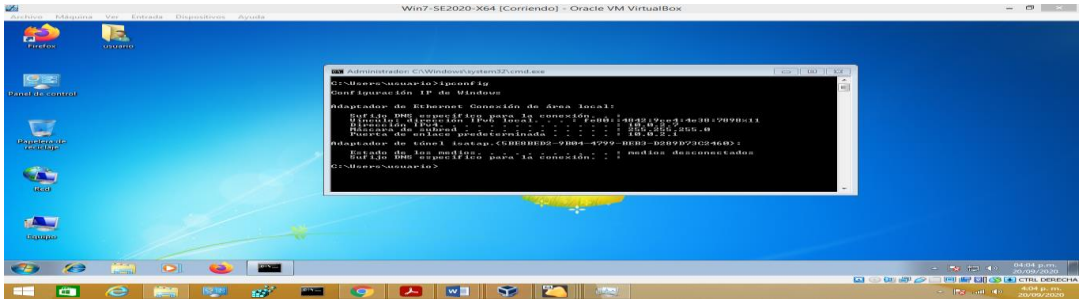
3.5.4 Win7-SE2020-X64

Es un sistema operativo creado por Microsoft. Consiste en un conjunto de programas que permiten la ejecución de los recursos que tiene un ordenador. El significado del término (windows, ventanas) hace alusión a su interfaz gráfica, que presenta un modelo basado en tareas y compartimentos independientes, con sus propios menús y controles.

En el caso de 64 bits, el registro puede almacenar 2 ^ 64 valores que pueden vincularse a 16EB (exabytes) de RAM. Una gran cifra en comparación con la memoria de 4 GB a la que se podía acceder con su contraparte anterior de 32 bits.

En el caso de una CPU de 64 bits, los datos completos, si tienen menos de 8 bytes, podrían procesarse de una sola vez. Incluso si los datos son más de 8 bytes, el procesador de **64 bits requerirá menos tiempo** que el otro. No notaremos mucha diferencia en el uso diario, excepto a quien le guste realizar múltiples tareas entre aplicaciones grandes.

Figura 4: Máquina virtual Win7-SE2020-X64



Fuente: Medardo Perez Rentería

Se evaluaron las diferentes acciones de los equipos Red Team & Blue Team de la organización en el marco de los criterios éticos y legales; En la parte jurídica para los delitos informáticos, en Colombia se cuenta con varios recursos, sin embargo, uno de los más significativos es la ley 1273 de 2009, la cual complementa el Código Penal Colombiano con base en el concepto de la protección de la información y de los datos, con el cual se busca preservar los sistemas que utilicen tecnologías da la información y las comunicaciones en Colombia.

La ley 1273 de 2009 no es más que el mecanismo mediante el cual se definen los tipos penales que tienen relación con delitos informáticos, la protección de la información y los datos de todos los colombianos.
En dicha ley se tipifican los diferentes delitos informáticos, y las diferentes penas aplicables a quienes incurran en cualquiera de ellos.

Otro punto importante es la actuación ética y legal del contrato y el personal que laboraba realizando los contratos del nuevo personal equipos estratégicos en ciberseguridad: red team & blue team y de la operación “OPERACIÓN ANDRÓMEDA BUGGLY” en la ciudad de Bogotá, En el acuerdo se evidencia un acto ilegal en el Cuarto punto.
Obligaciones de la parte receptora: Se obliga al receptor a guardar silencio si encuentra procesos ilegales a no dar aviso a las autoridades, también se le hace responsable si los representantes hacen mal uso de la información confidencial si al momento de algún allanamiento tiene información y la más grave de todas lo hacen responsable ante las autoridades de la información que tenga en su poder.

Pero lo más grave es que, según la Ley de Protección de Datos 1273 de la Constitución Política de Colombia se infringieron varios artículos como:

Utilizar software malicioso para captar información de terceros, Hurto por medios informáticos y semejantes y venderla al mejor postor cometiendo delitos.

Considero que todo lo que se realizó estuvo mal hecho por parte de las personas que dirigían la operación, porque no llevaron un registro de las cosas que allí se realizaban ni del personal que entraba en las instalaciones menos de lo que realizaban con toda esta tecnología.

La firma de un contrato con la organización que al momento de analizarlo se encuentran muchas anomalías como ocultar, suplantar o asumir respon.

De otras personas y en un apartado del acuerdo menciona textualmente:
No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros; se puede ver involucrado en problemas legales.

Ya pasando al marco de las vulnerabilidades en el sistema informático de la organización Whitehouse Security a partir del uso de metodologías y técnicas de intrusión. Realizando el análisis al escenario 3 se encontraron diferentes falencias:

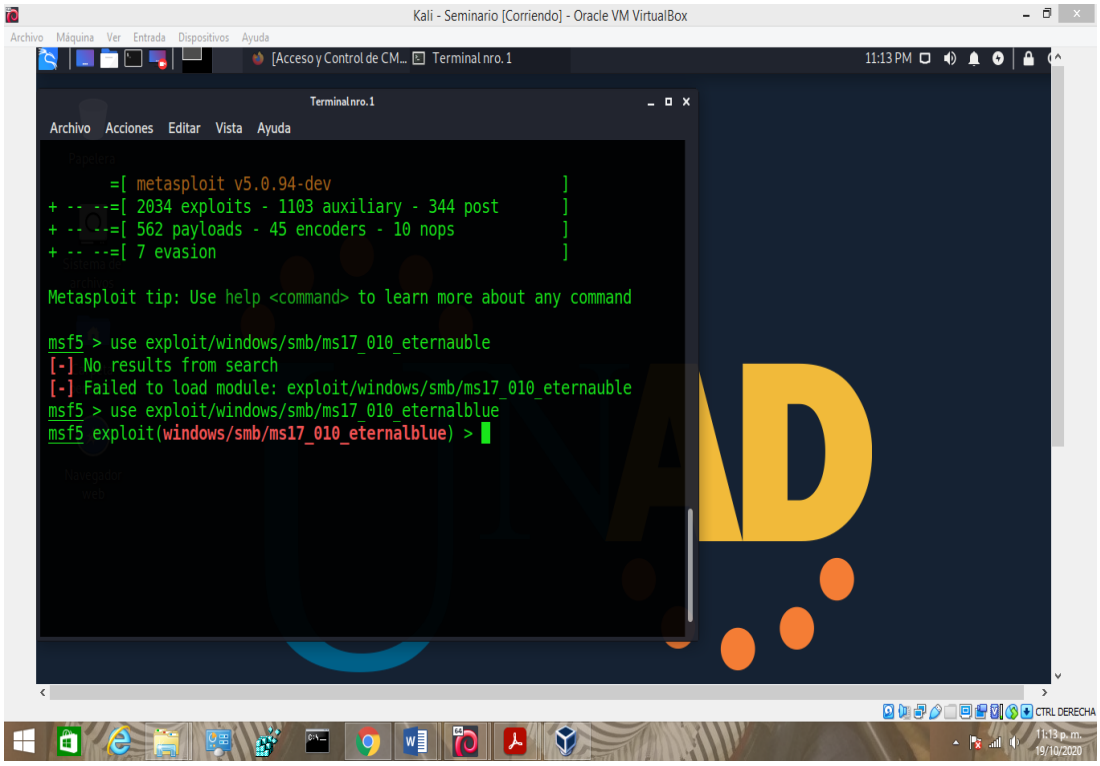
Tabla 1: Vulnerabilidades escenario 3

VILNERABILIDADES ENCONTRADAS EN EL ESCENARIO 3	
1	Fuga de información la cual se presenta al interior de la organizacion. dos de sus equipos de cómputo en la dependencia.
2	Equipos de cómputo sospecha cuentan con Windows 7 X86 y X64 y tienen un sistema operativo antiguo
3	Fuga de información (10 de junio de 2020) los S.O. no se encontraban actualizados.
4	Fallo de seguridad con identificador CVE-2017-0144.
5	No tienen instalada la actualización MS17-010.

Fuente: Medardo Perez Rentería

Se realizó un ataque con EXPLOIT a las máquinas virtuales buscando las “vulnerabilidad en la implementación del protocolo del Bloque de Mensaje de Servidor (SMB, por sus siglas en inglés) de Microsoft, a través del puerto 445” esto con la falla que presentan los dos sistemas operativos que se encuentran sin una actualización nueva lo cual los vuelve vulnerables a este ataque.

Figura 5: Exploit/windows/smb/ms17_010_eternalblue



Fuente: Medardo Perez Rentería

Para contener estos ataques informáticos se formuló estrategias de contención de riesgos y vulnerabilidades en la infraestructura TI de la organización que se encontraron en la fase anterior:

- Actualizar los sistemas operativos de las máquinas.
- Eliminaría el SMBv1 el cuan es protocolo que permite acceder y modificar a archivos de un servidor remoto, así como a otros recursos, la última actualización fue en el 216
- Recomiendo instalar el parche MS17-010 para eliminar la vulnerabilidad que presenta la falla de seguridad con identificador CVE-2017-0144.
- Crear un equipo de respuesta a incidentes, responsabilidades.
- Crear procedimientos de recuperación y restauración de sistemas SIN eliminación de posibles evidencias del ataque.
- Monitorear periódicamente a toda la red para identificar posibles fallas.

Al momento de revisar todas las vulnerabilidades, se recomienda instalar el SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas.

Las funciones principales del sistema es recopilar información de registros para verificar el cumplimiento de ciertas normas de seguridad en las compañías detención y bloqueo de actividades sospechosas.

Una de las características y la más importante es que podemos monitorear en tiempo real todo el tráfico de información de nuestra compañía y activar las alertas de posibles ataques (Brokers, 2018).

Link para ver video: **https://youtu.be/HeGLvncHF48**

4. Conclusiones

Se implementaron varias técnicas de control a partir de un análisis de vulnerabilidades en la informática de la empresa WhiteHouse Security.

A partir de un ámbito legal se efectuó una evaluación de los procesos de los equipos estratégicos Red Team & Blue Team, obteniendo un informe técnico con las sugerencias y técnicas a seguir, con el objetivo de implementar las mejoras y optimizar la seguridad del sistema.

Atraves de la implementación de varios sofware se pudo verificar las fallas y vulnerabilidades en un entorno de simulación, la empresa usando estrategias, procesos técnicos de entremetimiento, mostrando como resultado un informe técnico evidenciando fallas relevantes y las probables soluciones.

5. Recomendaciones

Partiendo de los resultados que se evidencian de la empresa Whitehouse Security, equipos actualizados, se recomienda utilizar el Manual de funciones que tenga la organización en funciones y políticas de privacidad que se necesite para proteger la información.

El SMBv1 se debe actualizar, ya que este es un protocolo antiguo y ya nos se utiliza, pues este otorga acceso a un servidor remoto y permite actualizar a archivos y diferentes recursos del sistema.

De antemano se aconseja instalar el parche MS17-010 ya que este suprime la vulnerabilidad que ocasiona el defecto de seguridad con identificador CVE-2017-0144, atraves de estos protocolos se fortalece la seguridad en la empresa.

Verificando la capacidad de conocimiento que tengan los encargados de la seguridad informática, se aconseja implementar una estrategia para preparar al personal en el tema de la seguridad informática y en cuanto a los aceptos de ética y de la ley que dictan los delitos informáticos en Colombia.

6. Bibliografía

autor, F. (s.f.).

Barboza, D. C. (02 de 06 de 2020). *Qué es un proxy y para qué sirve.* Obtenido de https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/

Brokers, S. (15 de 30 de 2018). *MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrupción.* Obtenido de https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/

Bruno, D. (26 de 03 de 2020). *Introducción al Red Team – Parte 1.* Obtenido de https://www.blackmantisecurity.com/introduccion-al-red-team-parte-1/

Calvo, J. F. (26 de 02 de 2015). *Instalación del Sistema Operativo.* Obtenido de http://www.materialestic.es/manuales/instalacion.de.Windows.7.desde.0_90calidad-150ppp.pdf

Copyright, A. (04 de 12 de 2020). *Exploits: todo lo que debe saber.* Obtenido de https://www.avast.com/es-es/c-exploits

Fernández, Y. (01 de 07 de 2020). *Xacataca basics.* Obtenido de https://www.xataka.com/basics/virtualbox-que-como-usarlo-para-crear-maquina-virtual-windows-u-otro-sistema-operativo

hat, r. (16 de 12 de 2020). *El concepto de CVE.* Obtenido de https://www.redhat.com/es/topics/security/what-is-cve

Innovación, C. (28 de 05 de 2020). *CICET - Que es el hardening de Sistemas Operativos.* Obtenido de https://www.ciset.es/publicaciones/blog/746-hardening

Luz, S. D. (21 de 01 de 2019). *Nmap: Descarga, instalación y manual de uso paso a paso.* Obtenido de https://www.redeszone.net/seguridad-informatica/nmap/

Microsoft. (11 de 12 de 2020). *Puntos de referencia del Centro de seguridad de Internet (CIS).* Obtenido de https://docs.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark

People. (09 de 06 de 2020). *Nsit SIEM en seguridad informatica.* Obtenido de https://shop.nsit.com.co/

Rizaldos, H. (22 de 10 de 2018). *Qué es Metasploit framework.* Obtenido de https://openwebinars.net/blog/que-es-metasploit/

Singh, G. D. (14 de 11 de 2019). Nombre citio web. En G. D. Singh, *Aprenda kali linux 2019* (pág. 550). Newyork: Pakt publishing. Obtenido de https://books.google.com.co/books?id=H6a-DwAAQBAJ&dq=kali+linux&hl=es&source=gbs_navlinks_s

welivesecurity. (18 de 11 de 2014). *Cómo utilizar OpenVAS para la evaluación de vulnerabilidades.* Obtenido de https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

Wikipedia la enciclopedia libre. (08 de 12 de 2020). *Wikipedia.* Obtenido de https://es.wikipedia.org/wiki/Kali_Linux