CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

NANCY VIVIANA CEBALLOS DIAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PALMIRA

2020

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

NANCY VIVIANA CEBALLOS DIAZ

Informe Final Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Director: John Freddy Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PALMIRA

2020

ÍNDICE

GLOSARIO

Seguridad Informática: Es un conjunto de herramientas que permiten proteger en gran medida los datos, redes y comunicaciones, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad: "Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados"[1]

Integridad: "Propiedad de salvaguardar la exactitud y estado completo de los activos".[2]

Disponibilidad: "Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada"[3].

Sistema Operativo: "El sistema operativo es el software que coordina y dirige todos los servicios y aplicaciones que utiliza el usuario en una computadora, por eso es el más importante y fundamental. Se trata de programas que permiten y regulan los aspectos más básicos del sistema. Los sistemas operativos más utilizados son Windows, Linux, OS/2 y DOS"[4]

---

[1]NORMA TÉCNICA NTC-ISO/IECCOLOMBIANA (2006), Recuperado de : http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[2] NORMA TÉCNICA NTC-ISO/IECCOLOMBIANA Pág. 2 (2006), Recuperado de : http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[3] NORMA TÉCNICA NTC-ISO/IECCOLOMBIANA Pág. 3 , (2006), Recuperado de : http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[4] Concepto. De (2020) Que es un sistema operativo, recuperado de: https://concepto.de/sistema-operativo/

Pentesting: “El Pentesting es una abreviatura formada por dos palabras *“penetration”* y “testing” y es una práctica/técnica que consiste en atacar diferentes entornos o sistemas con la finalidad de encontrar y prevenir posibles fallos en el mismo”[5]

Protocolo SMB: “SMB es un servicio que está disponible universalmente para los sistemas Windows y las versiones heredadas de los protocolos SMB podrían permitir a un atacante remoto obtener información confidencial de los sistemas afectados”[6]

Metasploit: “Es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos”[7]

Nmap: “Nmap es muy reconocida en el mundo de seguridad informática por su funcionalidad de escaneo de redes, puertos y servicios. No obstante, la herramienta ha ido mejorando con el correr de los años, ofreciendo cada vez más posibilidades que resultan muy interesantes. Actualmente incorpora el uso de scripts para comprobar algunas de las vulnerabilidades más conocidas”[8]

Hardening: Hardening es un proceso que tiene como objetivo reducción de posibles vulnerabilidades en sistemas que ya vienen configurados, “es el término que se le da al proceso de reducción de vulnerabilidades en el sistema. Esto se consigue, estableciendo unas medidas de seguridad con el objetivo de estar preparados ante un ataque informático” (CISET, 2020)

Firewall: El firewall es un dispositivo que apoya el bloqueo de conexiones entrantes y salientes de una red, esto con el fin de limitar accesos no deseados que puedan

---

[5] Ciberseguridad (2020) Que es el pentesting. Recuperado de: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

[6] Segu-Info .(2017) Microsoft lanzará parche para vulnerabilidad 0-Day en SMB en febrero. https://blog.segu-info.com.ar/2017/02/microsoft-lanzara-parche-para-una.html

[7] Hardening (2020). Que es el hardening de sistemas Operativos. Recuperado de: https://www.ciset.es/publicaciones/blog/746-hardening

[8] Welivesecurity (2015). Auditando con Nmap y sus scripts para escanear vulnerabilidades. Recuperado de: https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-e
scanear-vulnerabilidades/

vulnerar los equipos de la red. “Existen firewall de red o de host, los de red son implementados para proteger los equipos y sistemas de información de una red y los de host protegen a los equipos de cómputo o servidores directamente desde su núcleo de conexiones”[9]

Antivirus: Son programas que acceden a tus sistemas con el objetivo de modificar el funcionamiento de tu computadora, por lo general atacan los archivos o datos almacenados con el fin de modificarlos o causar perjuicios. “Entre los principales daños que pueden causar estos programas están: la pérdida de rendimiento del microprocesador, borrado de archivos, alteración de datos, información confidencial expuestas a personas no autorizadas y la desinstalación del sistema operativo”[10]

[9] Cisco. (SF) ¿Qué es un firewall? https://www.cisco.com/c/es_es/products/security/firewalls/what-is-a-firewall.html

[10] Tecnología Informática. (2020). ¿Qué es un Antivirus? ¿Como funciona? Recuperado de : https://www.tecnologia-informatica.com/que-es-un-antivirus-como-funciona/

RESUMEN

Los sistemas informáticos deben de contar con diversos mecanismos que protejan en gran medida la información, y aunque según los estudios realizados desde los diferentes entes especialistas en seguridad informática, no hay estrategias que garanticen el 100% de protección, esto ocurre por el mismo entorno digital, los riesgos persisten, crecen y ocasionan afectación si no existen parámetros que minimicen estos riesgos.

La importancia más relevante se da, desde el momento en el que se seleccionan los sistemas operativos, pues se debe priorizar, que tipo de características serán implementadas, las cuales por ninguna razón deben de ser parametrizadas de manera automática, ya que de esto dependerá la seguridad con la cuenten los sistemas operativos.

En el presente trabajo se da a conocer los diferentes procesos ejecutados para el caso de seguridad en la organización **"The WhiteHose Security**" donde se identifican fallas de seguridad en los sistemas de información y se implementan estrategias para subsanar de manera eficiente las vulnerabilidades identificadas.

Como primera medida se identifican aspectos legales, la manera en cómo se pueden implementar mecanismos de seguridad que lleven a garantizar la confidencialidad, integridad y disponibilidad de la información, se ilustrarán los mecanismos generados a partir de pruebas ejecutas utilizando mecanismos de pentesting, contención de ataques a través de algunas estrategias hardening.

La seguridad en los sistemas operativos es analizada, identificando vulnerabilidades, partiendo de ello se realiza el estudio pertinente para ejecutar un proceso de contención de ataque informático con el fin de ejecutar pruebas que permiten identificar los fallos de seguridad y posteriormente ser solucionados.

El proceso se realizó a través de un banco de trabajo, con una máquina con Sistema Operativo Kali Linux y la ejecución de pruebas en dos máquinas con sistema operativo Windows7x64 y otra Maquina con Windows7x86, Al finalizar esta implementación en los equipos, se debe poder evidenciar una reducción considerable de vulnerabilidades al realizar el aseguramiento de los sistemas operativos de la organización.

INTRODUCCIÓN

El presente documento tiene como propósito dar a conocer el proceso realizado durante fases de análisis en los sistemas de información de la compañía “The WhiteHose Security” donde se evidencian aspectos legales durante el proceso ejecutado, teniendo en cuenta la legislación relacionada con delitos informáticos.

La implementación de estrategias se realiza a los sistemas operativos Windows en dos máquinas identificadas como sospechas de la fuga de información, el propósito del equipo Blue team- Red team es identificar vulnerabilidades en dichos sistemas e implementar medidas que permitan reducirlas. Se logra evidenciar que los mecanismos de seguridad actuales tienes fallos y no son eficientes. Esto pone en riesgo la información de la compañía.

El proceso de análisis de vulnerabilidades se realizó siguiendo la estructura de un pentesting y con los resultados obtenidos se inicia el proceso de análisis para la identificación de estrategias que permitan medir la reducción de vulnerabilidades, enfocado, en brindar seguridad a los sistemas operativos lo cual permita minimizar los riesgos evidenciados.

Con la implementación de herramientas de contención y detección de ataques informáticos se garantiza alertas de seguridad que permitirán reaccionar ante accesos no autorizados a los sistemas, así mismo se reduce significativamente los riesgos, impidiendo que las amenazas se materialicen y pongan en peligro la información de la organización.

OBJETIVOS

4.1. Objetivo general

Identificar y minimizar las vulnerabilidades en los sistemas de información de la organización The WhiteHose Security

4.2. Objetivos específicos

- Indicar aspectos legales que comprometen la seguridad de la información en la organización.

- Identificar las vulnerabilidades que ponen en riesgo la seguridad de la información en la organización.

- Implementar estrategias para minimizar los riesgos en la seguridad de la información en la organización.

- Proponer recomendaciones para la seguridad de la información en la organización.

INFORME

Actualmente las organizaciones buscan prevenir acciones que afecten la disponibilidad de la información y protegerse en las diferentes instancias con el fin de dar valor a su servicio, garantizando confidencialidad e integridad en sus sistemas de información, pues es de suma importancia fortalecer protocolos de seguridad que evidencien una visión más precisa ante las amenazas permanentes que hay en el día a día sobre los sistemas de información.

Teniendo en cuenta los requerimientos de la organización "***The WhiteHose Security***" de mejorar los niveles de seguridad, ya que se detectaron fallos en los sistemas informáticos, donde se estaba generando una fuga de información lo cual afectaba de manera directa la confidencialidad en la compañía, se procede a ilustrar las fases realizadas durante el estudio para dar solución a dichos fallos de seguridad.

4.3. Análisis aspectos legales:

Teniendo en cuenta los artículos que componen la ley 1273, donde se evidencia que en Colombia se plantean procedimientos con el fin de combatir y minimizar los delitos informáticos, es importante que en las organizaciones los procesos rijan sobre las diferentes leyes que permitan implementar estrategias que garanticen protección en los sistemas de información.

Cada vez es más necesario tomar medidas con las cuales se logre un mayor control ante los casos de ciberdelincuencia ya que las personas que realizan actos perjudiciales logran identificar las debilidades en los sistemas de información, lo cual, les facilita ejecutar acciones ilícitas como ataques informáticos.

La ley 1273 de 2009 que adiciona al Código Penal colombiano el Título denominado "*De la Protección de la información y de los datos, que se divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones*"[11]

[11] Mintic. (2009). *LEY No. 1273* (p. 4) recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

“Artículo 269A: 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 1000 salarios mínimos legales mensuales vigentes” [12]

Teniendo en cuenta la ley 1273 Artículo 269A se logra identificar que en la situación actual de la compañía, se estaba generando el acceso abusivo a los sistemas de información, lo cual sostuvo en riesgo la disponibilidad de los servicios de la organización, ante dicha situación se procede a iniciar determinadas actividades que logran mediar este escenario donde se garantiza que los aspectos legales quedan en regla, es decir “ Se logra minimizar significativamente el acceso abusivo a los sistemas de información de personas no autorizadas”

4.4. Análisis de vulnerabilidades:

En este proceso se llevó a cabo la implementación de etapas de un pentesting, lo cual permitió identificar de manera precisa las vulnerabilidades en los sistemas de información de la compañía, el proceso de este análisis se realiza a través de un banco de trabajo donde se ejecutaron las pruebas en un sistema operativo Kali Linux a dos máquinas con sistema operativo Windows, donde se identifican de la siguiente manera:

- Maquina1 con sistema Operativo Windows 7 de 64 Bits (IP 172.16.2.4)
- Maquina2 con sistema Operativo Windows 7 de 32 Bits (IP 172.16.2.6)

Estas máquinas fueron identificadas como sospechosas de la fuga de información, la compañía como punto partida para el análisis precisa la siguiente información:

- Los sistemas operativos son obsoletos
- Los dos equipos indicados cuentan con un SMBv1 Activo para compartir impresoras y archivos en red
- Los sistemas operativos no se encuentran actualizados
- Identificación de fugas de información

[12] Mintic. (2009). LEY No. 1273 (p. 4) recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

ETAPAS PENTESTING

A continuación, se ilustran las etapas ejecutas con los resultados obtenidos

4.4.1. Reconocimiento

- Análisis de aspectos legales
- Recolección de Información relevante
- Identificación de IP de las maquinas sospechosas
- Análisis de la información suministrada por la compañía y verificación de posibles riesgos acorde a las características de los sistemas operativos de la compañía.

4.4.2. Escaneo

- Herramienta Usada NMAP
- Identificación de Puertos Cerrados en la Maquina2 Windows7x86 y Maquina1 Windows7x64
- Identificación de Puertos Abiertos Maquina1 Windows7x64 y Maquina2 Windows7x86

4.4.3. Identificación y Análisis de vulnerabilidades

- Herramienta Usada NMAP
- Comando ejecutado: Nmap 172.16.2.4 –script vuln
- Vulnerabilidad en el protocolo de seguridad SMBv1
- Vulnerabilidad identificada MS17-010
- Análisis de vulnerabilidad identificada

4.4.4. Plan de explotación

- Herramienta Usada Metasploit
- Ejecución de test de penetración y acceso a las máquinas Windows
- Control de la Maquina1 con Windows7x64 con el meterpreter activo se obtiene toda la información de la maquina y finalmente se determina que se encuentra totalmente comprometida
- Para la Máquina2 con Windows7x86 se ejecuta el mismo proceso, pero no es posible comprometerla en un 100%

4.4.5. Resultados

- Detección de vulnerabilidades en los sistemas operativos
- Ejecución de herramientas las cuales permitieron detectar los fallos de seguridad en los sistemas operativos.
- Control de la Maquina con sistema Operativo Windows7x64 Profesional
- No se logra el control total de la maquina2 con Sistema Operativo Windows7x86
- Identificación del archivo .exe por donde se estaba generando la fuga de información

Como se puede evidenciar, la ejecución de pentesting a través de las herramientas "**Nmap" y "Metasploit"** permitieron identificar la vulnerabilidad a la cual se encontraba expuesto el sistema informático y los sistemas operativos de la organización. El proceso inicia, con la recolección de información de manera detallada, como son las funciones organizacionales, identificación de datos internos, verificación de la versión de sistemas operativos, que servicios se encontraban operativos, falencias identificadas, tipo de usuarios.

Después de ejecutar la etapa de recolección de información, la cual es una actividad de gran relevancia ya que es el punto clave para tener éxito en las siguientes etapas, se procede a consultar de manera precisa cuales herramientas serán de ayuda para ejecutar el proceso de identificación de vulnerabilidades, como se ha indicado se hace uso de las siguientes herramientas

NMAP "*Una de las características más conocidas de Nmap es la detección remota del sistema operativo, analizando la huella de la pila TCP/IP. Se envían paquetes TCP y UDP al host remoto y se examinan los bits en las respuestas. Reconocer el sistema operativo de host remoto permite orientar la parametrización de las herramientas de análisis de vulnerabilidades*" [13]

Para este proceso se identifican las IP de las máquinas Windows las cuales permitieron ejecutar de manera precisa las pruebas de pentesting, se hace un chequeo a las características del sistema en las máquinas, memoria instalada, nombre, red a la pertenece, procesador, dominio, licencias y demás información precisa que permitió identificar el estado de las maquinas a las cuales se les realizó el proceso con el fin de obtener resultados esperados.

Al iniciar las etapas de pentesting haciendo uso de la herramienta NMAP, se evidencia durante el proceso que en la Máquina con Sistema Operativo Windows7x86 con ip 172.16.2.6 se lograron ver puertos abiertos, el puerto 80/tcp, puerto 135/tcp, puerto 139/tcp, puerto 445/tcp, puerto 554/tcp, puerto 2869/tcp, puerto 5357/tcp, puerto 49152/tcp.

[13] Alcaldía de Bogotá, (2018) Guardianes de la información, Penetration testing, Fase Escaneo de puertos, servicios, OS, recuperado de: https://tic.bogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

De igual manera para la Máquina con sistema Operativo Windows7x64 con ip 172.16.2.4 se identificaron puertos abiertos, el puerto 135/tcp, puerto 139/tcp, puerto 445/tcp, puerto 554/tcp, puerto 2869/tcp, puerto 5357/tcp, puerto 49152/tcp.

Después de identificar los puertos que se encontraban abiertos, se realizó el escaneo de vulnerabilidades y como resultado se evidencia que las máquinas con sistema Operativo Windows7 son vulnerables al protocolo SMBv1 lo cual afectaba la seguridad en los sistemas de información de la organización, se procede a identificar cuáles son los riesgos que puede ocasionar el tipo de vulnerabilidad hallada, como se puede remediar y la implementación de mecanismos que permiten subsanar el fallo de seguridad identificado.

Es importante precisar que este protocolo es "*la primera versión de los protocolos SMB que sirve para intercambiar archivos entre un servidor y un cliente, así también con dispositivos como impresoras, la versión SMBv1 se ejecuta en el puerto 445*"[14] sin embargo, este protocolo fue creado en tiempos en donde las amenazas y las vulnerabilidades no se presentaban tan frecuentemente, sin embargo, es relevante tener presente que en la actualidad los protocolos deben de brindar mayor seguridad a los sistemas operativos por lo cual hasta que no se realice el cambio a protocolos con versiones actualizadas el problema de seguridad puede ser persistente.

Después de indagar la vulnerabilidad SMBv1, se inició el proceso de pruebas con la herramienta ***Metasploit*** la cual se puede comprender como "Un conjunto de herramientas utilizadas para probar vulnerabilidades de sistemas informáticos" [15] esta herramienta facilita la ejecución de pruebas pues es muy sencilla y fácil de manejar.

Con las pruebas ejecutadas a través de la herramienta Metasploit se logra comprometer en su totalidad a la máquina Windows7 Profesional de 64 bit, de esta manera se cumplió con el objetivo de identificar el archivo.exe por el cual se estaba realizando la fuga de información de organización.

[14] Nerion, (SF) Conoce todo sobre el protocolo SMB, Recuperado de: https://www.nerion.es/blog/protocolo-smb1/

[15]Alcaldía de Bogotá, (2018) Guardianes de la información, Penetration testing, recuperado de: https://tic.bogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

La siguiente imagen confirma el proceso ejecutado:

Figura. 3. Archivo.exe identificado

Fuente – Unidad II etapa 3 Etapa de Documentación y resultado final

De esta manera se concluye que las pruebas pentesting realizadas fueron exitosas, ya que se logra identificar las vulnerabilidades en los sistemas de información y el fallo se seguridad que atenta contra la confidencialidad, integridad y disponibilidad de la organización.

SOLUCIÓN A FALLOS DE SEGURIDAD

Se identificaron vulnerabilidades críticas a las cuales se les realizó el tratamiento necesario, con el fin de evitar que se sigan presentando accesos no autorizados a los sistemas y fugas de información, a continuación, se describen las fallas identificadas:

- Fallos a nivel de sistema operativo
- Actualizaciones de seguridad de Windows Update no instaladas
- Vulnerabilidades en la red (Puertos Abiertos)
- Vulnerabilidad para el protocolo SMBv1
- No se cuenta con Antivirus

A partir de las vulnerabilidades identificadas se hizo necesario implementar medidas que garanticen la protección de datos, a través de herramientas que permitan minimizar futuros ataques informáticos, se implementaron estrategias hardening las cuales permitieron llevar a cabo con éxito el proceso de reducción de vulnerabilidades identificadas.

4.5. Actualizaciones del Sistema Operativo

Como primera medida se procede a chequear actualizaciones, pues una de las acciones fundamentales en los sistemas operativos es ejecutarlas con el objetivo de minimizar riesgos, el proceso de actualización debió realizarse de manera individual ya que por ser un sistema Operativo Obsoleto se presentaron dificultades en el momento de ejecutarlas de manera automática.

Se realizó la actualización requerida a través de la "herramienta WHDownloader"[16] como se evidencia en la imagen a continuación:

Figura 4. Instalación de actualización sistema operativo

Fuente Momento de la evaluación: Intermedio – etapa 4 -Actualizaciones del Sistema Operativo Maquina Windows7 x 64

Los sistemas Operativos quedan debidamente actualización brindando mayor seguridad en los procesos.

4.6. Activación Firewall

Se realizó chequeo sobre el Firewall el cual se encontraba desactivado, se realiza la activación del servicio para brindar mayor seguridad al sistema teniendo en cuenta que al estar desactivado la maquina es vulnerable a diversas amenazas, a continuación, se podrá evidenciar la actividad realizada:

[16] Tecno programas. (2015). WHDownloader, Recuperado de: https://tecnoprogramas.com/whdownldr-descarga-actualizaciones-windows-y-office/

Figura 5. Firewall activo

Fuente Momento de la evaluación: Intermedio – etapa 4 -Activación Firewall Maquina Windows7 x 64

Posteriormente para mayor seguridad se procede a cerrar en el firewall los puertos del SMB, se identifican y se activa la opción de Bloqueo de conexión, este procedimiento se realiza tiendo en cuenta que la protocolo SMBv1 es inseguro por tanto hasta no pasar a la V2 y/o V3 no brindara seguridad a los sistemas.

4.7. Instalación antivirus

Se evidenció que la máquina (Windows7x64) afectada no tenía Antivirus instalado, se procede a identificar un buen End Point que brinde seguridad al sistema y contenga diversas herramientas en su beneficio, para ello se descarga e instala el antivirus Kaspersky.

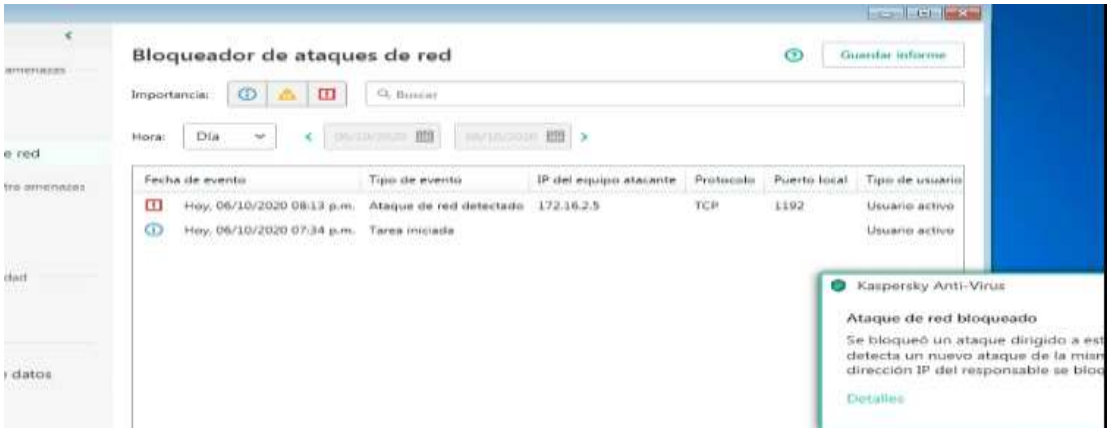
Figura 6. Antivirus instalado

Fuente Momento de la evaluación: Intermedio – etapa 4 -Instalación Antivirus en la Máquina Windows7 x 64

Con la instalación del End Point se realiza un escaneo de fondo con el objetivo de identificar amenazas en los sistemas, de igual manera se hace uso de las herramientas para brindar seguridad a los sistemas informáticos activando el servicio de bloqueador de ataques de red.

Como se puede ilustrar esta herramienta permito capturar un ataque en tiempo real, identificando la IP de la máquina que está intentando acceder de manera intrusiva al equipo, realiza el proceso para bloquear todo el tráfico de red y procede a bloquear la ip que está ocasionando la intrusión.

Figura 7. Ataque de red bloqueado



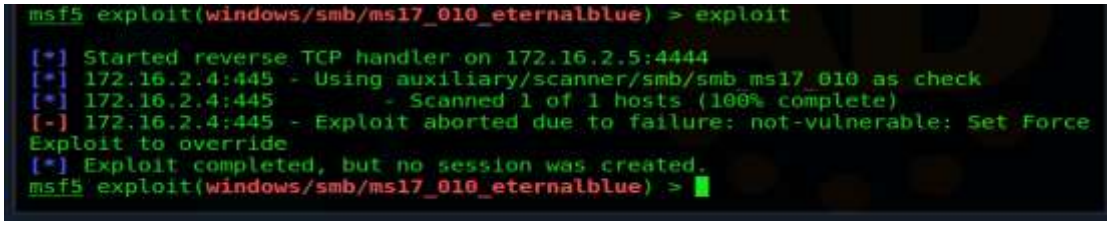
Fuente Momento de la evaluación: Intermedio – etapa 4 - *Alertas de detección Kaspersky en* Máquina Windows7 x 64

4.8. Resultados

Para garantizar que la implementación de estrategias Hardening cumplieron con el objetivo final, minimizar riesgos en los sistemas operativos, se realizan pruebas en aras de acceder nuevamente de manera intrusiva a la maquina1 Windows7x64 Profesional, haciendo uso de las herramientas que se indicaron para la identificación de vulnerabilidad y escaneo, “**Nmap” y “Metasploit”.**

El resultado final nos indica que no es posible acceder a las maquinas, pues sus puertos ya se encuentran cerrados y no se visualiza la vulnerabilidad identificada inicialmente, como se ilustra a continuación no es posible acceder a las maquinas después de realizar el escaneo y el intento de acceso intrusivo:

Figura 8. Prueba final_ No hay vulnerabilidad



Fuente Momento de la evaluación: Intermedio – etapa 4- Resultados Metasploit *en* Máquina Windows7 x 64

Después de las estrategias implementadas, el resultado final nos indica que la vulnerabilidad ha sido Remediada de manera satisfactoria.

RECOMENDACIONES

A continuación, se listan las recomendaciones que se consideran pertinentes que sean estudiadas e implementadas con el objetivo de minimizar los riesgos a los que se encuentran expuestos los sistemas de información de la organización:

- Se sugiere realizar cambio de sistema Operativo, ya que la versión de Windows7 con el que cuenta la organización es obsoleto y esto genera más riesgos teniendo en cuenta que los servicios de actualizaciones que brinda Microsoft para esta versión ya están fuera de servicio y el proceso se hace más dispendioso.

- Los sistemas operativos deben de ser Licenciados para garantizar seguridad en los mismos, actualizaciones permanentes y soporte técnico, es de suma importancia frecuentemente chequear las actualizaciones, con sus parches de seguridad y permanecer al día con este tipo de actividades.

- Los sistemas de Antivirus conocidos en la actualidad como End Point deben de contar con licencia y herramientas que permitan ejecutar de manera eficaz contención y detección de ataques informáticos.

- Las APP instaladas en las máquinas de igual manera deben de contar con licencias, ya que esto garantiza que su funcionamiento sea eficaz y que no se presenten problemas de seguridad en las máquinas.

- El firewall debe permanecer Activo, esto brinda mayor seguridad a los sistemas de información.

- Automatizar medidas de seguridad y restricción de privilegios en los equipos de cómputo asignados al personal.

CONCLUSIONES

Durante el desarrollo de las etapas de análisis, teniendo en cuenta los fallos de seguridad en la compañía, se logra establecer el impacto que puede ocasionar el no realizar una gestión adecuada de vulnerabilidades, las amenazas pueden materializarse ocasionando perdida de información, lo que conlleva a la afectación del servicio en la organización.

Se logra evidenciar que las vulnerabilidades son asociadas a las actualizaciones de los sistemas, donde es de gran importancia ejecutarlas, tanto para sistemas operativos, aplicaciones y contar con un soporte en la infraestructura tecnológica que brinde mecanismos de protección, contención y detección.

Algunas de las vulnerabilidades identificadas como críticas fueron mitigadas en gran medida implementando herramientas de actualización y aseguramiento de sistemas operativos, con la instalación de Anti-Virus, se logra garantizar un plan detección que permitirá ejecutar medidas para la protección de los sistemas informáticos.

El presente Informe puede encontrarse a través del siguiente enlace:

https://youtu.be/7i19AT2jw3M

REFERENCIAS BIBLIOGRAFICAS

Mintic. (2009). *LEY No. 1273* (p. 4). Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

NORMA TÉCNICA NTC-ISO/IECCOLOMBIANA (2006), Recuperado de : http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

NORMA TÉCNICA NTC-ISO/IECCOLOMBIANA Pág. 2 (2006), Recuperado de : http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

NORMA TÉCNICA NTC-ISO/IECCOLOMBIANA Pág. 3 , (2006), Recuperado de : http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

Concepto. De (2020) Que es un sistema operativo, recuperado de: https://concepto.de/sistema-operativo/

Ciberseguridad (2020) Que es el pentesting. Recuperado de: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

Segu-Info .(2017) Microsoft lanzará parche para vulnerabilidad 0-Day en SMB en febrero. https://blog.segu-info.com.ar/2017/02/microsoft-lanzara-parche-para-una.html

Hardening (2020). Que es el hardening de sistemas Operativos. Recuperado de: https://www.ciset.es/publicaciones/blog/746-hardening

Welivesecurity (2015). Auditando con Nmap y sus scripts para escanear vulnerabilidades. Recuperado de: https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

Cisco. (SF) ¿Qué es un firewall? https://www.cisco.com/c/es_es/products/security/firewalls/what-is-a-firewall.html

Tecnología Informática. (2020). ¿Qué es un Antivirus? ¿Como funciona? Recuperado de : https://www.tecnologia-informatica.com/que-es-un-antivirus-como-funciona/

Mintic. (2009). *LEY No. 1273* (p. 4) recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Alcaldía de Bogotá, (2018) Guardianes de la información, Penetration testing, Fase Escaneo de puertos, servicios, OS, recuperado de: https://tic.bogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

Nerion, (SF) Conoce todo sobre el protocolo SMB, Recuperado de: https://www.nerion.es/blog/protocolo-smb1/

Nessus, (2015), Análisis de vulnerabilidades, recuperado de: http://www.cursodehackers.com/nessus.html

Tecno programas. (2015). WHDownloader, Recuperado de: https://tecnoprogramas.com/whdownldr-descarga-actualizaciones-windows-y-office/

INCIBE (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditandoseguridad-tus-sistemas

Microsoft (2020) Detección y habilitación de SMBV1, SMBV2 y SMBV3 En Windows. https://docs.microsoft.com/es-es/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

IWEB. (2018) Proteger los servicios Windows SMB y NetBios/NetBT. https://kb.iweb.com/hc/es/articles/115000274491-Proteger-los-servicios-Windows-SMB-y-NetBios-NetBT

Microsoft. (2017) Security Bulletin MS17-010 – Critical. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN