SEMINARIO DE RED TEAM & BLUE TEAM

ETAPA 5

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

INTEGRANTE

CARLOS ARTURO IBAÑEZ GUZMAN

CODIGO CURSO: 202337164_6

TUTOR:

JHON FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

16 DE OCTUBRE DEL 2020

RESUMEN

Conoceremos las estrategias de Redteam y Blueteam, aspectos a tener en cuenta en su desarrollo y los planteamientos necesarios para tener en cuenta con el fin de brindar más seguridad a una organización, adicional a una construcción del conocimiento desde el enfoque de la ciberseguridad y sus derivados.

INDICE

GLOSARIO

Blueteam: Equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva.

Escaneo: Crear una copia con el fin de exacta con el fin de ser estudiada para diversos beneficios

Firewall: Dispositivo de hardware o un software **que** nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente entre dos ordenadores

Malware: Todo tipo de amenazas informáticas o software hostil

Pilar: Soporte o base fundamental que se rige un proceso

Phishing: Estafa que tiene como objetivo obtener a través de internet datos privados de los usuarios

Redteam: Proceso de emulación de escenarios de amenazas a los que se puede enfrentar una organización, analizando la seguridad desde el punto de vista de los atacantes

S:O : Sistema operativo llámese Windows, Linux y demás

INTRODUCCIÓN

En este informe técnico se tratará sobre como desde nuestro punto de vista que podemos aportar al desarrollo de una estrategia de ataque de Redteam y desde Bluteam lograr que esta se pueda evitar.

Adicional a esto nosotros como ingenieros describiremos el Blueteam y las estrategias que manejaremos y conoceremos, un punto de vista técnico de como estos planteamientos aportan de manera proactiva a la gestión de vulnerabilidades y como proteger una organización.

Como desarrollo final construiremos un conocimiento basado en la experiencia y como desde un enfoque técnico que podemos aportar y que debemos estar atentos al momento de un ataque de ciberseguridad, sin dejar a un lado como estar siempre preparados para enfrentarlos o contrarrestarlos si colocar en riesgo una organización.

OBJETIVOS

OBJETIVO GENERAL

- Construir un informe técnico donde se presenten las estrategias RedTeam & BlueTeam planteadas en el seminario

OBJETIVOS ESPECIFICOS

- Describir de manera específica aspectos que aporten al desarrollo de estrategias de Blueteam y Readteam

- Recomendar de manera acertada el planteamiento de estrategias para endurecer la seguridad de una organización equipos de incidentes informáticos

- Argumentar y construir desde nuestro conocimiento un enfoque seguro de ciberseguridad

- Documentar y sustentar desde el desarrollo del seminario especializado un video con nuestros puntos de vistas acerca de la desarrollado en el curso

DESARROLLO DE LA ACTIVIDAD

1. INFORME TECNICO

1.1 Aspectos que aporten al desarrollo de estrategias de redteam & blueteam.

Los aspectos que más aportan al desarrollo de estrategias según lo indicado es que a modo general los ataques son cada día más comunes y que estos tienden a ser más sofisticados o con mayor riesgo de ataque, sobre todo los que son en tiempo real, en estos casos lo primero que se haría seria es siempre realizar escaneos del ataque y validar por donde se filtró la información de la organización u empresa, estrategias como los son de grupos especializados que nos eviten el envío de malware, exploits y demás ataques, adicional que en ese momento se debe proveer o generar políticas de seguridad que nos ayuden a evitar un redteam y con respecto a bluteam a bloquear todo lo concerniente al ataque , correos, logs y demás, establecer un grupo de trabajo con personas muy bien seleccionadas con el fin de garantizar una idoneidad ante el proceso, se construirá un documento legalmente constituido de un acuerdo legal con intervención de representantes legales que estudien una por una todas las cláusulas y entre todos llegar a un consenso, si existiese alguna irregularidad antes de iniciar las labores en la organización primero debe ser superada para poder avanzar, este será el primer paso legal .

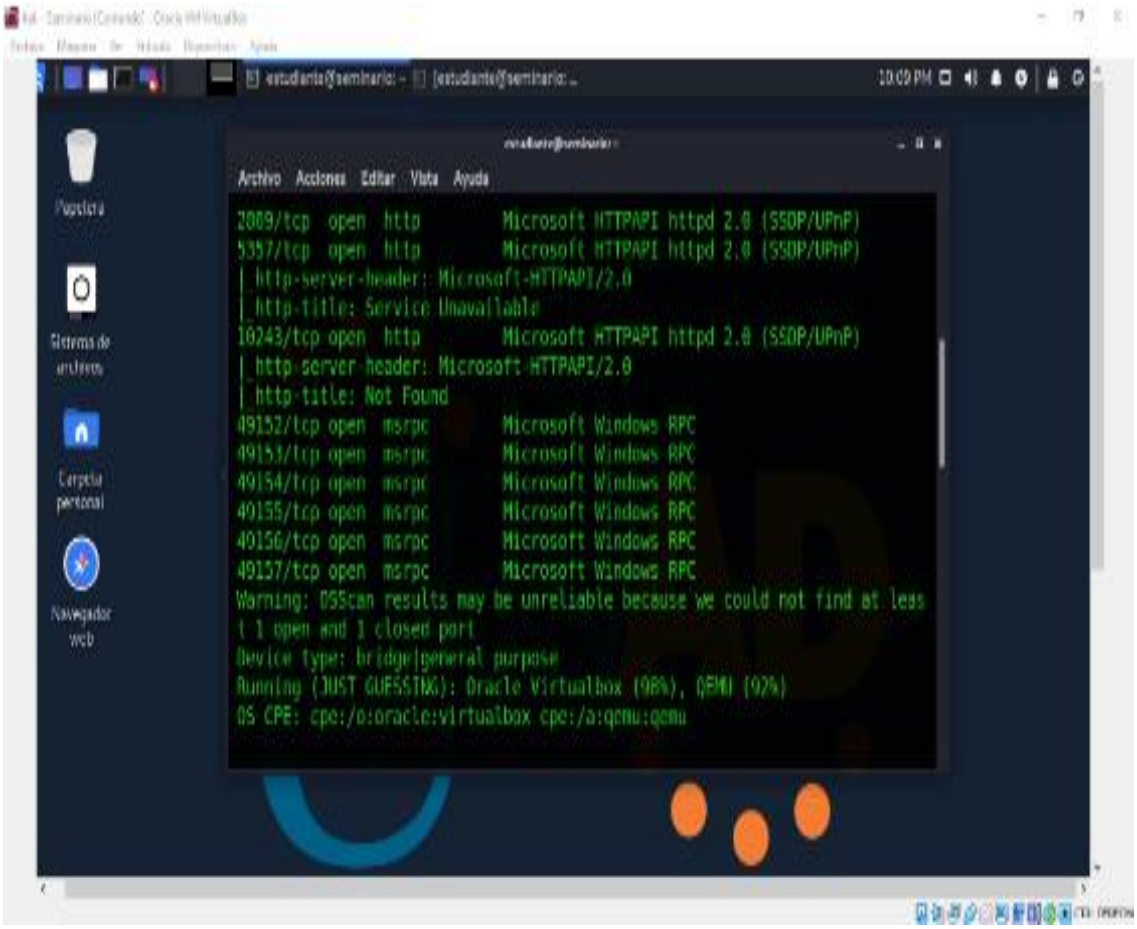
Superado este proceso comenzaría con la escogencia del personal con entrevistas, labores de conocimiento, pruebas piloto y demás antes validar quien va a trabajar con la organización, se debe tener claro el personal que trabajaría en la organización, todo debe estar regido según los estatutos de ley y los artículos 33,34,35 y 36 del capítulo 2 deberes y obligaciones de los profesionales del código de ética según la normativa COPNIA.

Apartir de tener todos estos puntos ya finalizados comenzaría el proceso de trabajo en la organización siempre respetando los valores, derechos y deberes del personal que labora y del ingeniero encargado del proyecto, esto regido bajo los artículos 35,36 ,37 ,38 y 39 del código de ética que dispone de reglamento

legales, obrar con prudencia y dignidad, mantener en reserva toda la información del cliente, ser honesto, y rendir cuentas claras y precisas todo esto según lo establecido.
(https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf, s.f.)
Un ejemplo de estos es siempre escanear o analizar un sistema operativo ya sea con Nmap u otra herramienta con el fin de validar puertos abiertos y demás

En esta imagen podemos observar como se realiza el escaneo de puertos

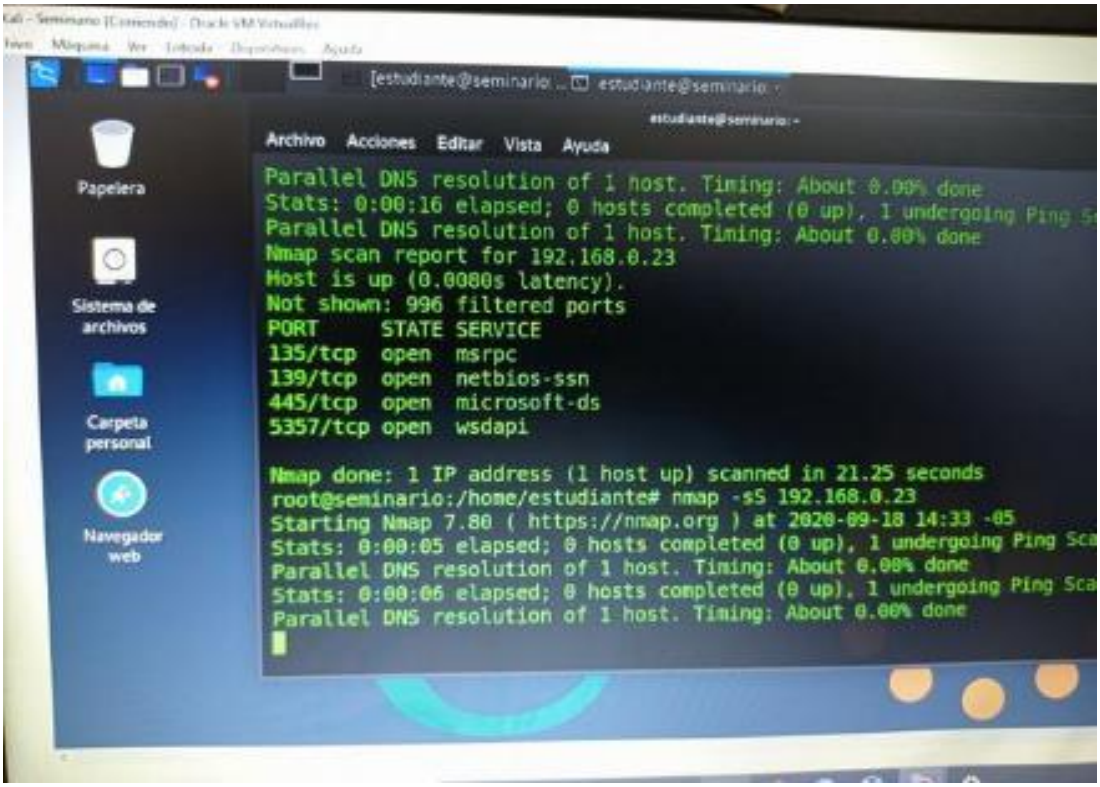
Figura 1 escaneo de puertos



Ibañez Guzman, Carlos. Escaneo de puertos, 2020

En esta figura se puede observar los puertos, el estado ,el servicio y los puertos que se encuentran abiertos y vulnerables

Figura 2 escaneo de puertos

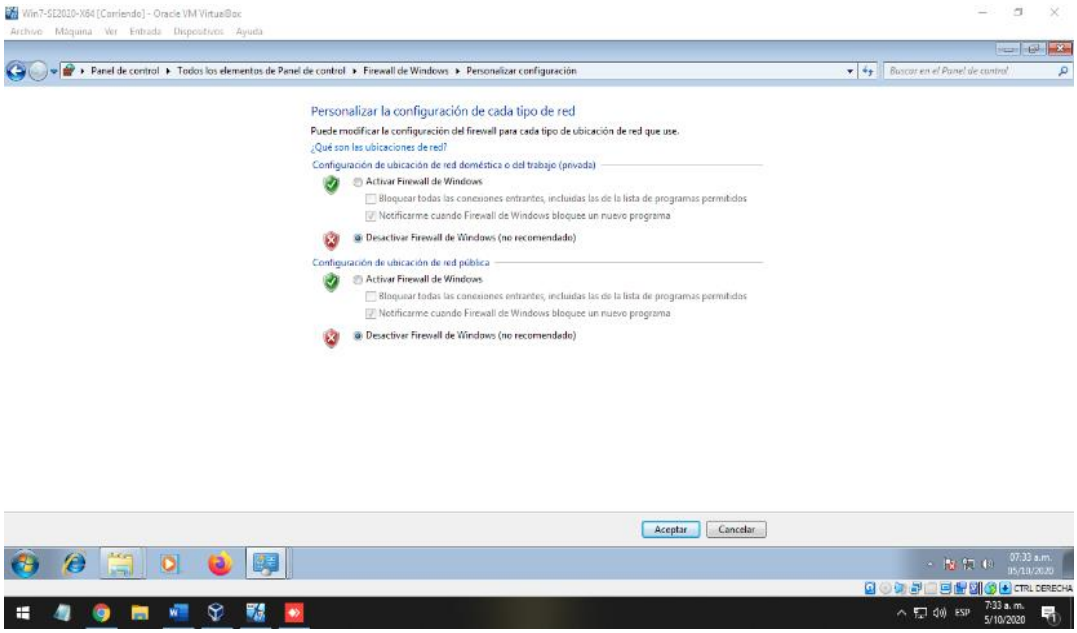


Ibañez Guzman, Carlos. Escaneo de puertos, 2020

Estrategias de seguridad muy comunes son por ejemplo el tratar de no abrir un correo atacante o desconocido y no permitir ningún flujo de información en la empresa, tener toda la gestión necesaria para bloquear todos los accesos e ingresos no autorizados al sistema, recordemos que los malware o amenazas informáticas son creados en su mayoría para hacer daño y generar desestabilización de empresa, organizaciones o gobiernos, es por tal motivo que toca estar muy vigilante de todos estos y estar atentos siempre.
Como características de contención toca mantener siempre el antivirus actualizado y el firewall

En esta imagen se puede observar como se activa el firewall en Windows para proteger nuestro sistema operativo

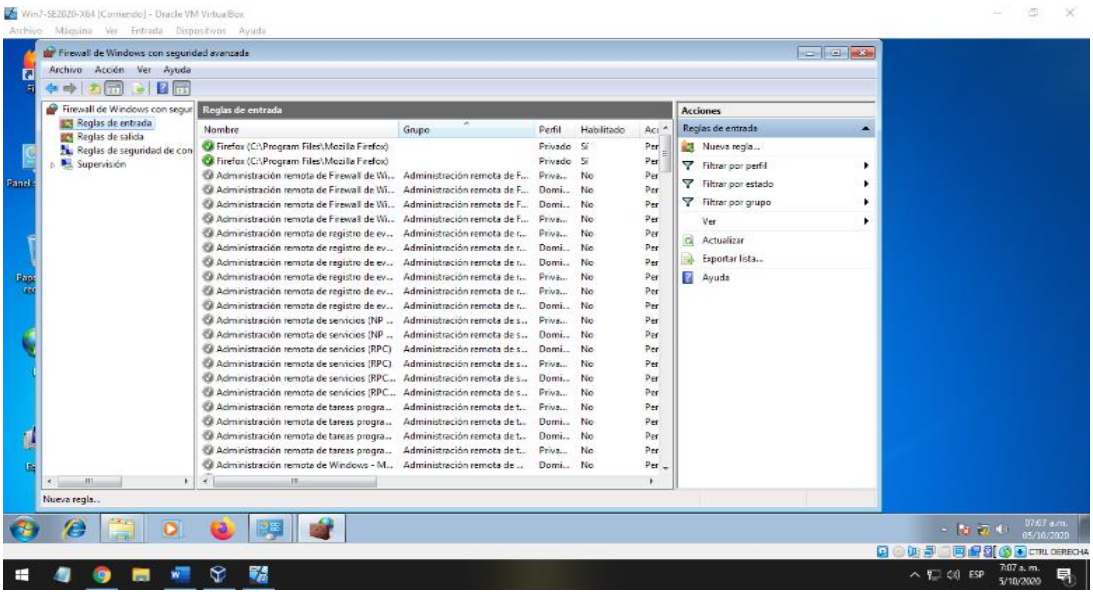
Figura 3 activación de firewall en Windows



Ibañez Guzman, Carlos. activación de firewall en Windows,2020

En esta figura se puede observar cómo habilitar los puertos y como colocarle reglas de protección especificas a cada puerto

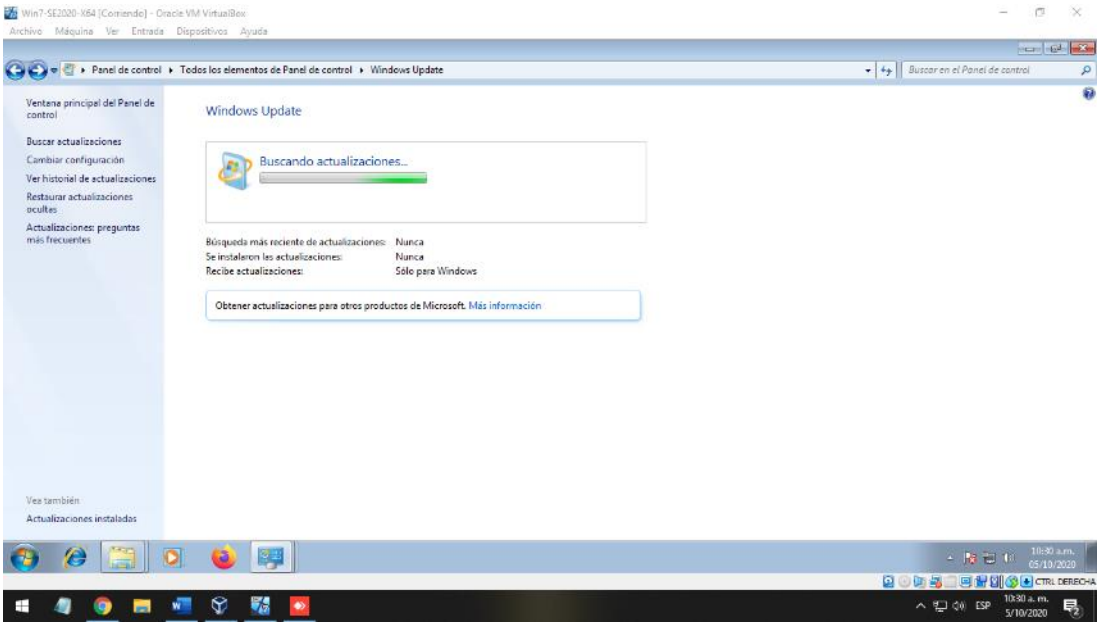
Figura 4 bloqueo de puertos en Windows



Ibañez Guzman, Carlos. bloqueo de puertos en Windows,2020

En esta figura se puede observar cómo se realiza la búsqueda automática de actualizaciones de seguridad en Windows.

Figura 5 actualización de Windows



Ibañez Guzman, Carlos. actualización de Windows,2020

con todas las reglas activas de trafico de información y bloqueo de puertos, y demás, toda estas sugerencias nos las brinda Blueteam con el fin de ayudarnos a prevenir los ataques y validar desde donde se origina, como característica adicional estar incluido siempre a modo de bluteam en un grupo de ciberseguridad con el fin de que ataques que se presenten en otros países sean de fácil detección y bloqueados de manera ágil de manera proactiva, contrarrestar un ataque significa tener conocimiento de cómo contener la afectación de todos los programas , S.O y como estos deben estar actualizados con los últimos parches , los programas que se utilizan también deben tener una actualización idónea para que ningún virus o malware pueda ingresar a la organización o la empresa.

Es de anotar que tanto bluteam como redteam y sus estructuras manejan diferentes puntos de vista y percepción, esto con el fin de complementar más y analizar de forma correcta y coherente los procesos de malware y ataques

informáticos teniendo como base principal los conceptos básicos de la seguridad informática, deben existir siempre los pilares fundamentales y no deben faltar al momento de conseguir sus objetivos.

Se debe mantener bajo protección la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado, en este punto se entra a valorar la importancia en los sistemas informáticos ya que con estas normas y políticas de seguridad casi podemos estar seguros que al a día de hoy existen nuevas formas de burlar una seguridad por lo que representan una amenaza latente a la ciberseguridad para ello siempre se están realizando nuevas normas de seguridad para proteger nuestra información.

Es necesario que la seguridad en redes sea bien utilizada para su mayor provecho y evitar el mal uso de esta.

Recordemos que la seguridad en redes tiene tres objetivos bien claros y que siempre se deben regir :

- **La integridad**

Se encarga de garantizar que los datos no hayan sido modificados desde su creación sin una autorización. Por otro lado, vela para que ningún intruso pueda capturar y modificar los datos en tránsito.

- **Confidencialidad**

Garantiza que toda la información que viaja o es transmitida en la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a ellas.

- **Disponibilidad**

Es el funcionamiento continuo de los sistemas de información.

Tener siempre presente y como recomendación en las estrategias la seguridad que siempre tenemos que velar por la protección de los datos y evitar siempre las implicaciones de operaciones indebidas que pongan en peligro el objetivo principal que es el de proporcionar una forma de almacenar y recuperar la información de manera que sea tanto practica como eficiente para la organización sí que esta se vea afectada o alterada en su transmisión.

Recordemos que el código de ética nos menciona todos los deberes que debe tener un profesional al momento de ejercer la profesión , adicional a esto está prohibido hacer parte de convenios por fuera de lo pactado , está prohibido realizar pliegos, licitaciones o concursos por fuera de la norma legal.

1.2 Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización

Las recomendaciones para el planteamiento de estrategias que nos permitirían endurecer los aspectos de seguridad siempre se deben basar en el estudio el estudio y la profundización de los ataques y amenazas más recurrentes, además de su clasificación y forma de contrarrestarlos, todos sus conceptos sobre los diferentes puntos de vista y siempre mantener un análisis de forma correcta y coherente de todos los procesos de malware y ataques informáticos teniendo como base principal los conceptos básicos de la seguridad informática.

recordemos que para esto debemos atravez de grupos especializados alrededor del mundo mantenernos actualizados con todos los malware y exploits, recordemos que los malware son creados de manera constante y toca estar atentos siempre, se debe evitar el aislamiento de datos, disminuir la inconsistencia de los datos y sobretodo garantizar la disponibilidad, integridad y confiabilidad de los datos con el fin de que el usuario tenga acceso a los datos confiables, sin ser hackeados por ciberdelincuentes, con mecanismos de defensa garantizando la transparencia de los mismos.

No solo existen dispositivos y software para garantizar la transparencia de los activos sino también culturizar a los usuarios para evitar fugas de información, recordemos que las amenazas son factores internos o externos que influyen en un sistema informático que son capaces de causar daño. Dichas amenazas pueden dar lugar a un ataque informático en los equipos, redes y comunicaciones, es por esto por lo que siempre se debe plantear una estrategia para contrarrestarlos, es de anotar que estas estrategias pueden variar dependiendo de las circunstancias y el ataque , es por esto por lo que toca siempre endurecer la seguridad de una organización y realizarle un monitoreo constante con el fin de mantenerlos siempre atento a una amenaza.

Todas las recomendaciones son bienvenidas, pero solo la organización o el personal encargado de TI de la empresa junto a su equipo de trabajo son los responsables de controlar y mantener la disponibilidad en todo momento y evitar vulnerabilidades que puedan afectar y entorpecer la productividad de una organización, entre ellas tenemos algunas de las más útiles

A continuación, se presentan una serie de recomendaciones para mitigar y reducir los ataques sufridos por la empresa:

- **Copiar los archivos frecuentemente**

Es importante crear dos copias de seguridad de los archivos, ya que una, que se puede almacenar en la nube usando herramientas como Dropbox o Google Drive; y la otra, en un dispositivo físico como un disco duro portátil, USB o PC. Se recomienda configurar en el dispositivo de backup solo permisos de lectura y escritura, sin la opción de modificarlos.

- **No abrir correos si no sabe el origen**

Es muy importante ser cuidadoso con los correos que se revisan. Los ciberdelincuentes envían todo tipo de mensajes con contenidos maliciosos, esperando que los lectores desprevenidos caigan en la trampa descargando los archivos adjuntos o solo leyendo. Active una protección antispam y nunca abra correos de remitentes desconocidos.

- **Desconfiar de todos sus contactos**

Este es quizás uno del mecanismo más utilizado para distribuir troyanos y secuestrar información. El consejo es no abrir contenidos extraños, así vengan de personas conocidas, porque podría enfrentar sobornos para recuperar los archivos.

- **Actualice su sistema operativo**

Como los ciberdelincuentes tienden a explotar vulnerabilidades en el software para cometer delitos, se recomienda hacer actualizaciones periódicas del sistema, ya que estas corrigen errores y defectos que podrían ser aprovechados

por los hackers para acceder a la información. La recomendación es activar las actualizaciones automáticas, para no olvidar hacerlas cada cierto tiempo.

- **Use un antivirus robusto**

Utilice un programa de antimalware robusto para proteger el sistema, se recomienda incluir este tipo de programas en las empresas mediante licencias multidispositivo que además de prevenir infecciones a su computadora, protegen los archivos aún si existiera una amenaza infiltrada en el sistema.

- **Actúe rápido si ve que fue atacado**

Se recomienda no apagar el equipo si el usuario descubre que está siendo víctima de un ataque informático. Cuando se apaga el equipo, se puede eliminar la evidencia digital del delito y esto es fundamental para instaurar un proceso legal. Así mismo, aconseja desconectar el equipo de cualquier red de internet para pasarle el antivirus, aunque ya hay tipos de malware que atacan sin red.

- **Detecte el nombre del malware**

Si ya fue víctima de robo de información, se recomienda reconocer cual es el nombre del malware que ha atacado el equipo, ya que si es una versión antigua puede ser relativamente fácil restaurar los archivos o es más fácil para los expertos identificar cual es la mejor forma de recuperar la información. Por ninguna razón pague un rescate, porque estaría alimentando el negocio ilegal.

Como recomendación final debemos siempre estar atentos a cualquier incertidumbre o probabilidad de que una amenaza se materialice por medio de la explotación de una vulnerabilidad existente y el control del riesgo siempre analizando su buen funcionamiento, la efectividad y el cumplimiento de las medidas de protección establecidas y así determinar y ajustar las posibles deficiencias encontradas, recordemos que hay ataques externos e internos para los cuales también debemos seguir unas reglas con el personal que labora en la organización y como contrarrestarlos, este puede ser con reglas de firewall a cada uno de los trabajadores otorgándoles ciertos accesos a unos y a otro no o con un directorio activo donde solo personal autorizado tenga ingreso a cada software de la organización, lo importante es colocarlo al servicio de la

organización y sobretodo utilizarlo y mantenerlo siempre actualizado en su proceso y desarrollo.

1.3 Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

Como conclusión y construcción del conocimiento en el desarrollo del seminario se profundizo y se entendió el proceso de ataques y amenazas más recurrentes, además de su clasificación y forma de contrarrestarlos.

Se debatieron conceptos sobre los diferentes puntos de vista de cada estudiante con respecto a las inquietudes presentadas, todo esto con el fin de complementar más y analizar de forma correcta y coherente los procesos de malware y ataques informáticos teniendo como base principal el enfoque de la seguridad informática y todo lo relacionado en ella, se comprendieron un conjunto de técnicas que se utilizaron para identificar, recuperar, reconstruir y analizar evidencias tras un incidente de seguridad, debemos tener siempre presente que la información a recuperar siempre será de gran valor para la organización y los ataques como lo son la piratería, intrusiones, hacking, spam, phishing entre otros se relacionan siempre con la ciberseguridad y con las tecnologías de la información y las comunicaciones.

En todos estos análisis realizados en los trabajos anteriores pudimos determinar cómo y qué acciones ha llevado a cabo un intruso en nuestro sistema para vulnerarlo desde el escaneo de puerto, hasta la explotación de este, siempre dando como resultado final una fuga de información y daño irreparable en la organización.

En el día a día el Internet es de vital importancia para todos, ya que muchos servicios residen y se ofrecen por este medio es por esto que siempre debe existir la forma de mitigar esos riesgos y tomar todas las consideraciones posibles, por tal motivo en las organizaciones y en nuestra sociedad el incremento del número de ataques realizados y la sofisticación de las herramientas automatizadas para realizar dichos ataques es imprescindible, cuidar la seguridad de nuestra organización se volvió una responsabilidad que si llegase a fallar puede poner el riesgo toda una organización y llegar hasta el punto de declarase en banca rota o desaparecer .

Concluiremos que existen herramientas que nos ayuda a mantenernos informado y de manera real de los malware en todo el mundo de manera gráfica como ataca, donde se originó el ataque, y demás, toca validar en todo momento que tanto somos vulnerables a una intrusión, es por eso que atravez de muchas herramientas como escáner, antivirus, antispam se podrá monitorear todos los procesos de un ataque y la incertidumbre o probabilidad de que una amenaza se materialice por medio de la explotación de una vulnerabilidad existente.

En esta construcción del conocimiento siempre debemos tener en cuenta los aspectos básicos o más puntuales para lograr protegernos de una amenaza entre las que se encuentran están:

- Verificar la fuente de la información recibida. No contestar automáticamente a ningún correo que solicite información persona, financiera o de la organización.
- Usar filtros antispam.
- Escribir la dirección en el navegador de Internet en lugar de hacer clic en el enlace proporcionado en el correo electrónico.
- Hacer un análisis de nuestro equipo y comprobar que estamos libre de phishing.

2. LINK DEL VIDEO DE SUSTENTACIÓN

https://youtu.be/nreWSC8g4YU

3. CONCLUSION

Se define un informe detallado de lo encontrado y pruebas de cómo se realiza el ataque desde su auditoria, vulnerabilidad y posterior explotación, todo esto documentado y para tener en cuenta ante un ataque similar, aprendimos sobre las cláusulas de confidencialidad, así como legislación y normativa que se le aplica a todas aquellas personas que violen las normas, pudimos analizar en un escenario los procesos ilegales que se encontraron y que no corresponden a un acuerdo legal y ético de una organización, nosotros desde nuestro punto de vista profesional debimos visualizar todas esas falencias y argumentarlas de manera idónea y eficaz.

Adicional a esto también pudimos abarcar un caso real de un ataque de ciberseguridad y como desde nuestra percepción que implicaciones se pudieron generar en esta atravez de ciertos análisis de herramientas y procedimiento, evidenciar estos fallos e identificarlos para conocer por donde se estaba filtrando la información esto con el fin de tener una base para prevenir estos ataques y entender que con solo tener un puerto abierto es suficiente para afectar un sistema.

De igual manera aprendimos de una manera proactiva podemos contener un ataque en tiempo real y como proteger una organizacional al igual que las herramientas que nos ayudaran a contener los ataques informáticos.

A modo general este trabajo nos ayudó a ampliar aún más nuestro conocimiento al respecto del bluteam y redteam y los controles, descripción y herramientas que nos ayudara a ampliar nuestro conocimiento y como explotarlo en un evento relacionado

4. RECOMENDACIONES

Como recomendación final se deben tener siempre en cuenta unos deberes y unas responsabilidades como lo es administrar y coordinar el proceso de seguridad en la organización, proponer, coordinar riesgos en la entidad u organización, se debe mantener organizado la seguridad, promover nuevos proyectos, mantener el sistema estable y alejado de vulnerabilidades internas y externas.

Se deben siempre implementar barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial, es decir todo lo concerniente a tomar las medidas necesarias para contrarrestar alteraciones de la ciberseguridad.

Debemos estar atentos a las actualizaciones de seguridad, comprobación de la integridad del Kernel de Linux (según el caso), sistema de ficheros y configuraciones, modificaciones no autorizadas de las reglas del firewall o búsqueda de software potencialmente

En cuanto a la importancia de invertir en seguridad informática recordemos que existen unos pilares fundamentales que hacen que la seguridad informática nos funcione de una manera segura y que mientras estos pilares se mantengan en la empresa no se va ver afectada y evitaremos el ataque de personas que puedan atentar contra la organización, adicional existen muchos agentes dañinos y personas que los utilizan para acceder a la información de cualquier institución de forma ilegal y así extorsionar o hacer daños que traigan consecuencias irreversibles tanto para el gobierno como de la comunidad en general; es por esto y por muchas razones más que se debe invertir en la seguridad informática y hacer de esta su mejor aliado, así se salvaguarda la información, además de su integridad de manera general.

BIBLIOGRAFIA

- https://www.linti.unlp.edu.ar/uploads/docs/adaptando_openca_para_implementar_una_pki_para_e_science.pdf

- R. Vivek, BackTrack 5 Wireless Penetration Testing Beginner's Guide. 7 ed. United Kingdom: Packt Publishing Ltd, 2011. 220 p. ISBN 978-1-849515-58-0.

- Redman, S., Idioms and Phrasal Verbs Advanced. Oxford: Oxford University Press, 2011.

- defensa contra ataques informáticos, tomado de http://www.todoecommerce.com/defensas-contra-ataques-informaticos.html

- Comfort, J., Effective Presentations, Oxford, 1995.

- Professional English in Use Engineering With Answers: Technical English for Professionals. Cambridge: Cambridge University Press, 2009. **811.111**

- Que es un antivirus, tomado de https://softwarelab.org/es/que-es-un-antivirus/

- Como funciona un cortafuegos tomado de https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

- Guías y copias de seguridad tomado de https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

- Definición de gestión de eventos en información de seguridad, tomado de https://searchdatacenter.techtarget.com/es/definicion/gestion-de-eventos-e-informacion-de-seguridad-siem

- center_for_internet_security tomado de https://en.m.wikipedia.org/wiki/center_for_internet_security

- codecademy, tomado de www.codecademy.com/es

- Ibbotson, M., Cambridge English for Engineering Student's Book with Audio CDs (2).

- Mccarthy, M. and O´Dell, F., English Vocabulary in Use, Cambridge, 2002. **811.111 MCC eng**

- Hancock, M., English Pronunciation in Use, Cambridge, 2003.