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

NOFAL JAVIER ALVIRA MANIOS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
PITALITO
2021

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

NOFAL JAVIER ALVIRA MANIOS

TUTOR:
JOHN FREDDY QUINTERO

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
PITALITO
2021

RESUMEN

Con el desarrollo del seminario especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, se ha planteado una problemática en la empresa WhiteHouse Security, en el cual se plantearon unos requerimientos para la selección de personal, en el que el candidato debe poner a prueba sus conocimientos en Ciber Seguridad, los cuales son puestos en prueba durante el desarrollo de 4 etapas así:

Etapa 1 - Conceptos equipos de Seguridad

Etapa 2 - Actuación ética y legal.

Etapa 3 - Ejecución pruebas de intrusión.

Etapa 4 - Contención de ataques informáticos.

Para el desarrollo de estas etapas el candidato debe establecer un banco de trabajo, haciendo uso de software Libre, atendiendo el marco de los criterios éticos y legales, que caracterizan la labor de un equipo Blue Team, Red Team, para dar solución a los requerimientos de la empresa WhiteHouse Security.

El candidato presenta un informe final donde se especifica las acciones realizadas.

TABLA DE CONTENIDO

TABLA DE FIGURAS

GLOSARIO

Arp. Protocolo de resolución de direcciones a nivel de capa de red responsable de encontrar la dirección MAC que corresponde a una dirección IP.

Atacante. Persona con conocimientos informáticos que está acechando un sistema.

Ataque. Es un proceso dirigido por un atacante a través de un programa intenta ingresar a un sistema.

Auditoría. proceso de verificación y/o validación del cumplimiento de una actividad según lo planeado y las directrices estipuladas.

Autenticación. Es el proceso de establecimiento y verificación de la identidad para realizar una petición.

Backtrack. Distribución de Linux para realizar un ethical hacking, contiene varias herramientas de hacking.

Contraseña. Es una clave para la autenticación que tiene información secreta para el acceso.

Criptografía. Proceso de transformar un test plano a un texto descifrado.

Denegación de Servicio. Es interrumpir el funcionamiento correcto de un servicio.

Firewall. Es un cortafuegos/ software para controlar las comunicaciones denegando o permitiendo.

FTP. (File Transfer Protocol) Protocolo de transferencia de archivos.

Hacker. Individuo con conocimientos informáticos, pero no tiene intenciones maliciosos y es apasionado a la seguridad informática

HTTP. (HiperText transfer protocol) protocolo perteneciente a la capa de aplicación usadapar a las transacciones world wide web.

HTTPS. (HiperText transfer protocol Secure) es un protocolo basado en http, asegurando la transferencia de los datos.

IDS. Sistema de detección de intrusos que detecta accesos no autorizados a una red o computador.

Ingeniería Social. Técnica que se aprovecha la ingenuidad de las personas con el objetivode obtener información.

Intrusión: En nuestro escenario es el control de un sistema para la obtención de un objetivo, este no suele ser el caso de los DoS o DDoS.

IPS. Sistema de prevención de intrusos que previene accesos no autorizados. IPSEC. Protocolo Seguro sobre el protocolo IP.

Nessus. Herramienta para el análisis de vulnerabilidades.

Netbios. Protocolo que permite el establecimiento y mantenimiento de sesiones de comunicaciones entre computadores.

Nmap. Herramienta para el escaneo de puertos.

Pentesting: o test de penetración es una prueba simulando un ataque real, pero este tiene que estar controlado y con permiso de la "víctima".

Ping. Comando que prueba el estado de conexión con un equipo.

Protocolo. Conjunto de reglas que establecen la comunicación entre dos computadoras.

TCP. Protocolo de control de transmisión orientado a la conexión, ofreciendo mecanismos de seguridad en el proceso de comunicación.

TCP/IP. Modelo de descripción de protocolos de red Telnet. Protocolo que permite la conexión desde un terminal remoto.

Test de Penetración. Es un conjunto de metodologías y técnicas que permitan analizar debilidades de los sistemas informáticos.

Vulnerabilidad. Es una debilidad presente en cualquier sistema pudiendo ser explotada.

Xploit. Es un mecanismo que consiste en que la víctima recibe una postal falsa en su correo electrónico que contiene el link de una web falsa.

INTRODUCCIÓN

Con el desarrollo de este proyecto se pretende identificar lo más notable en el desarrollo de las etapas propuestas para ser realizadas en el seminario Equipos Estratégicos en Ciberseguridad Red Team & Blue Team, presentando los análisis correspondientes procesos y resultados obtenidos durante el proceso.

Se busca adquirir destreza para estar preparados para atender eventos de intrusión en tiempo real, lo que permite generar habilidades tanto en seguridad informática como en ciberseguridad, para poder dar una respuesta oportuna en el tiempo indicado.

El Seminario genera pautas que facilita el conocimiento, análisis e implementación de estrategias que permiten generar pruebas pentesting, contención de vulnerabilidades que pueden llegar a afectar la seguridad de la información de cualquier entidad.

Se ha generado un documento donde se encuentran las acciones que se pueden generar para la contención de posibles ataques informáticos y que pueden ser analizados por el equipo Red Team & Blue Team.

1. OBJETIVOS

1.1.1. OBJETIVOS GENERALES

Generar un Informe Técnico, detallado de las acciones realizadas en el banco de trabajo, donde se atendieron los requerimientos de la empresa WhiteHouse Security.

1.1.2. OBJETIVOS ESPECIFICOS

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.
- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

2. DESARROLLO DEL INFORME TÉCNICO

2.1. CONCEPTOS EQUIPOS DE SEGURIDAD

2.1.1. Análisis de la legislación relacionada con delitos informáticos.

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación "leyes, decretos" existen actualmente y las características principales de cada ley.

Desde la creación de la internet en 1980 el ministerio de defensa de los Estados Unidos ArpaNet (Advanced Research Projects Agency Network), pudo evidenciar unos eventos anormales en la transmisión de datos y algunos programas que sufrían un tipo de variación, fue aquí donde se generó el antivirus para contrarrestar estos eventos durante el 2008.

Con el paso del tiempo y los constantes ataques cometidos por los delincuentes cibernéticos que viajan por el mundo virtual, como la piratería informática fraude financiero, pornografía infantil, el acceso sin autorización a sistemas de información, sabotaje informático entre otros, por tal motivo varios países incluyeron dentro de su sistema judicial este delito que permite procesarlos y castigarlos; en el 2009 nuestro país Colombia se unió a este grupo de países.

En la Constitución política de Colombia del 1991 en su artículo 15 no se encontraban estipulados como tal los delitos informáticos, nos habla de los derechos de autor y protección de datos.

> "*Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*
>
> *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.*
>
> *La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.*
>
> *Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley* "

Con la promulgación de la Ley 565 de 2000; con la cual es aprobado el "Tratado de la OMPI - Organización Mundial de la Propiedad Intelectual- que trata sobre los Derechos de Autor (WCT)" que fue adoptado en Ginebra, el 20 de diciembre 1996, esta Ley es declarada EXEQUIBLE en la Corte Constitucional por el Magistrado Ponente Doctor Vladimiro Naranjo Mesa mediante la Sentencia C1183-00 de 13 de septiembre de 2000.

Con la Ley 1273 del 5 de enero de 2009 que modificó el código penal por la cual se crea un bien jurídico 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"

Con esta ley se disponen el título VII BIS con el capítulo I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos con ocho artículos que protegen los datos e información de los colombianos permitiendo interponer sanciones y penalizar a quienes incurran en este tipo de delitos, de la misma maneta el capítulo II De los atentados

informáticos y otras infracciones compuesto por artículos tratantes del hurto de información y/o transferencia de activos también sancionables y penalizados.

Capítulo 1

Artículo 269A: acceso abusivo a un sistema informático
Artículo 269B: obstaculización ilegítima de sistema informático o red de telecomunicación.
Artículo 269C: interceptación de datos informáticos.
Artículo 269D: daño informático
Artículo 269E: uso de software malicioso
Artículo 269F: violación de datos personales
Artículo 269G: suplantación de sitios web para capturar datos personales
Artículo 269H: Circunstancias de agravación punitiva

Capítulo 2
Artículo 269I: hurto por medios informáticos y semejantes
Artículo 269J: Transferencia no consentida de activos

Mediante decreto 1078 de 2015 el estado colombiano implementa de manera obligatoria para todas sus Entidades Estatales en la implementación de un Modelo de Seguridad y privacidad de tecnología de la Información del Ministerio de las TIC.

La ley 1915 de 2018 julio 12, "*por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones de materia de derecho (SIC) de autor y de derechos conexos*" en su artículo 12 del Código Civil, que nos habla sobre que quien incurra de alteraciones, daños, fabrique entre otras faltas haciendo uso de medios tecnológicos a los derechos de autor incurrirá en una responsabilidad civil.

2.1.2. Análisis sobre el ejercicio de pentesting.

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Las pruebas de penetración o pentesting son un tipo de pruebas encaminadas en realizar un análisis de los mecanismos de seguridad establecidos en determinada entidad, en busca de posibles fallas o vulnerabilidades para ser solucionadas y evitar posibles ataques por agentes externos y evitar fugas de información.

Para poder llevar a cabo estas pruebas que se realizaran en distintos ámbitos y entornos, debemos tener en cuenta una serie de fases del análisis

2.1.2.1. Fase de reconocimiento:

En esta fase nos corresponde como su nombre lo indica el reconocimiento, se realiza la recopilación de toda la información que más podamos investigar con los clientes del sistema que vamos a analizar, de esto depende el éxito de la auditoria que vamos a realizar; de la colaboración por parte de los empleados y administrativos.

La herramienta que se utiliza para esta fase es la ingeniería social.

2.1.2.2. Fase de recolección de información:

para esta fase nos dedicamos a realizar la recolección de información que más podamos, como tener información del host que están en el sistema, direcciones IP, puertos disponibles, correos electrónicos, sistemas operativos, sistemas que utilizan, redes sociales entre otros.

Para el desarrollo de esta fase podemos hacer uso de una de las herramientas que esta diseñaba bajo código abierto, que es utilizada para la auditoria de seguridad y análisis de redes, estamos hablando de Nmap (Network Mapper)

FOCA es una herramienta utilizada para el análisis de metadatos

2.1.2.3. Fase de Análisis de vulnerabilidades:

Ya con la información recolectada anteriormente debemos iniciar el proceso de escaneo de las posibles vulnerabilidades que se encuentren, con la finalidad de definir los vectores para aprovechar o identificar esas fallas que puedan existir en la red, equipos de cómputo, correo electrónico entre otros.

En esta fase también podemos aplicar la ingeniería social.

Dentro de las herramientas que podemos utilizar encontramos Nessus

2.1.2.4. Fase de Explotación:

Una vez se tiene el análisis de las vulnerabilidades que nos ayuda a ver de que forma o manera vamos a realizar el ataque al sistema que van a ser objeto del análisis de penetración, porque puertos vamos a ingresar o por cual vulnerabilidad activa vamos a explotar, se inicia con los exploits contra todas las vulnerabilidades encontradas en las fases anteriores, teniendo en cuenta que no todos los exploits nos dan acceso total al sistema

Una de las herramientas que se utiliza es Metasploit, esta herramienta ayuda además de verificar vulnerabilidades, administrar evaluaciones de seguridad y mejorar la conciencia de seguridad.

2.1.2.5. Fase de Post-Explotación:

En esta fase se trata de conseguir el nivel máximo de privilegios, acceso sistema, datos y servicios que tengamos al alcance; como para esta fase ya tenemos el control del host.

Así mismo en esta fase debemos determinar el valor del Host a auditar y por supuesto mantener el control de ella, como podemos determinar el valor de esta máquina, depende del valor de los datos que se encuentran almacenados en ella y lo útiles que son.

podemos realizar saltos entre ellos siempre y cuando pertenezcan a la misma red.

Para el análisis de datos en esta fase y poder dar un valor al sistema nos podemos apoyar en la herramienta Wireskark

2.1.2.6. Fase de Informe:

Por último, se debe generar un informe con el resultado obtenido durante las pruebas o ataques realizados al sistema, donde se informe de una manera clara los tipos de riesgos encontrados.

De la misma manera se debe incluir en el informe las técnicas utilizadas, vulnerabilidades descubiertas y las herramientas utilizadas.

2.1.3. Explicación de las herramientas y servicios utilizados en ciberseguridad.

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

2.1.3.1. Metasploit:

Es una herramienta o conjunto de herramientas que permite analizar las vulnerabilidades de sistemas informáticos mediante una serie de Exploits, nos permite entrar a sistemas remotos, es una herramienta que puede ser utilizada para actividades Licitas como Ilícitas.

Existen dos versiones Metasploit Express y Metasploit Pro, en estas dos encontramos diferencias la Express no cuenta con todos los exploit actualizados, cosa que no pasa con la versión Pro que mantiene todos los exploit actualizados, todos los códigos que permiten atacar las vulnerabilidades.

2.1.3.2. Nmap:

Es una herramienta gratiuta de código abierto que permite realizar auditorias de seguridad, descubir redes y host, escanea puertos a través de segmentos TCP, datagramas UDP o paquetes ICMP.

Esta herramienta detecta host en redes locales como internet, de esta manera sabemos que dispositivos activos se encuentran conectados a la red Local.,

2.1.3.3. OpenVas.

El Open Vulnerability Assessment Scanner, es un scaner para evaluar vulnerabilidades (VT) contra los sistemas destino, esta herramienta realiza la detección de problemas de diferentes categorías, como lo son de bajo riesgo hasta de un riesgo grave para los dispositivos que se encuentren en la red, este cuenta con una interfaz que lo hace mas sencilla para el usuario..

Servicios en línea:

2.1.3.4. ExploitDB

La base de datos de Exploit es un repositorio de exploits públicos y pruebas de conceptos, software vulnerable, que fue desarrollado para realizar penetraciones e investigación de vulnerabilidades

2.1.3.5. CVE

Los puntos vulnerables y las exposiciones comunes (CVE) son una lista de fallas en la seguridad informática que se encuentran disponibles al público; estas permiten que los especialistas en Tecnología de la Información coordinen las iniciativas para priorizar y solucionar vulnerabilidades con la finalidad de mejorar la seguridad de la información de los sistemas.

2.1.4. BANCO DE TRABAJO

Teniendo en cuenta el requerimiento de la empresa se debe realizar la instalación de un banco de trabajo, como requisito para el personal postulado a hacer parte de la organización el cual deberá utilizar en una serie de escenarios y problemas complejos al interior de The WhiteHouse Security, para poder conocer el conocimiento en ciberseguridad de los aspirantes.

Paso A: Se da inicio con la descarga de la herramienta virtualizadora "VirtualBox" en su última versión.
Desde la página web se realiza la descarga del VirtualBox-6.1.26-145957 https://download.virtualbox.org/virtualbox/6.1.26/VirtualBox-6.1.26-145957-Win.exe

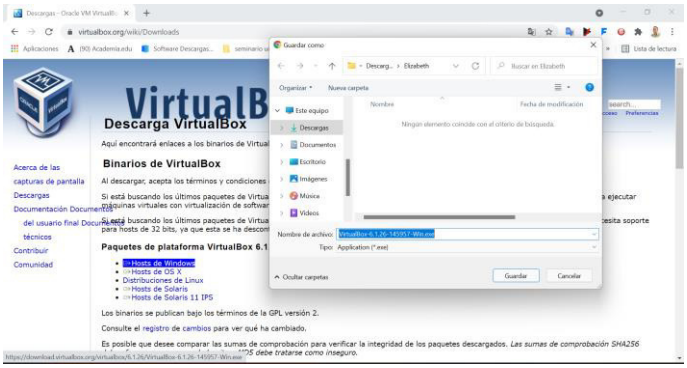

Figura: 1 Descarga VirtualBox
Fuente: Autor

Para el desarrollo del montaje del banco de trabajo se da inicio con la instalación del VitualBox en su versión 6.1.26-145957 para Windows

Figura: 2 Instalación VirtualBox -
Fuente: Autor

Se da inicio con la instalación por defecto de la herramienta, sin realizar ninguna modificación durante el proceso.

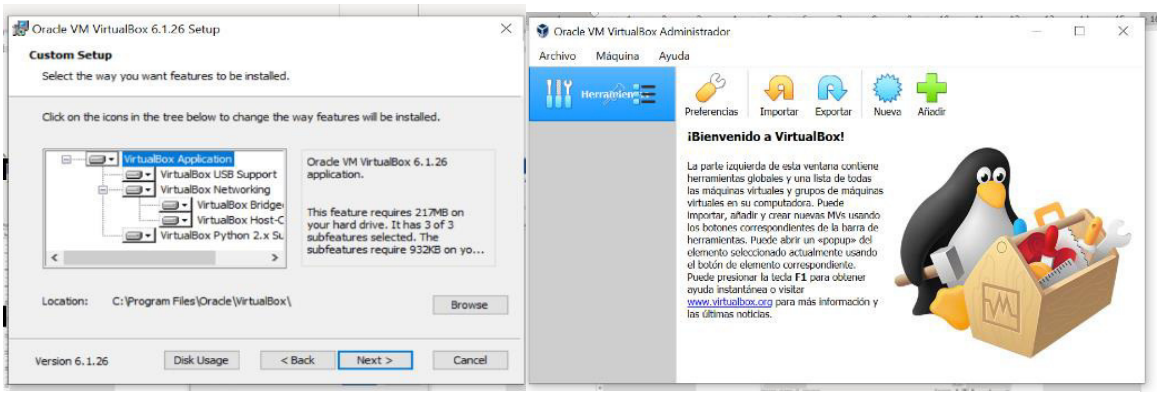

Figura: 3 Instalación VirtualBox
Fuente: Autor

Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

Una vez instalada la herramienta VirtualBox se procede a realizar el montaje de la maquina virtual de Kali - Seminario-003.

Le damos doble clik sobre la OVA Kali para realizar el montaje correspondiente realizando la importación de la máquina virtual.

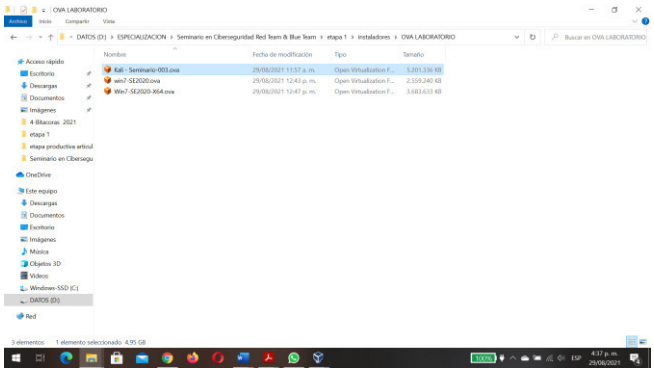

Figura: 4 Images de Máquinas Virtuales
Fuente: Autor

Se da inicio con la importación de la máquina las tres máquinas virtuales siguiente el mismo proceso con todas.

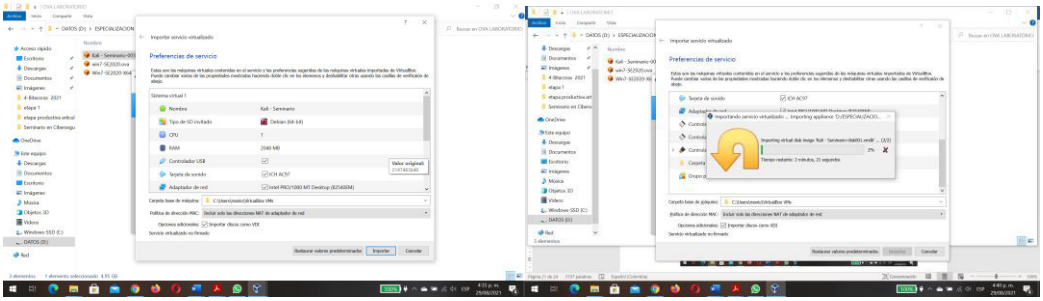

Figura: 5 Importación Máquinas Virtuales
Fuente: Autor

En las siguientes imágenes podemos ver que fue instalada la maquina virtual de Kali Linux y se utiliza las credenciales de acceso por defecto USUARIO: kali y contraseña: kali

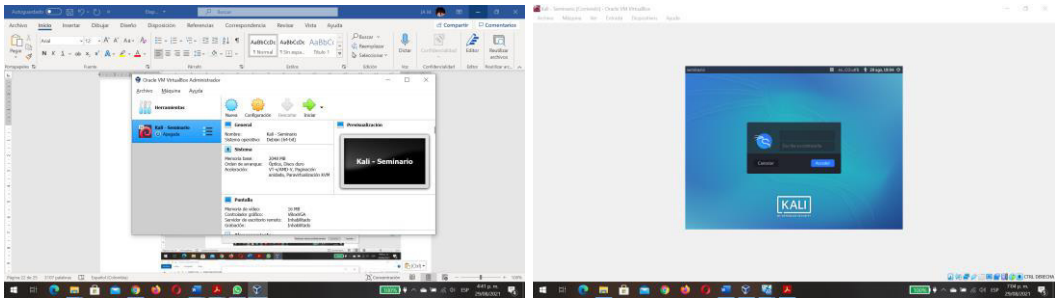

Figura: 6 Máquina Virtual Kali Linux
Fuente: Autor

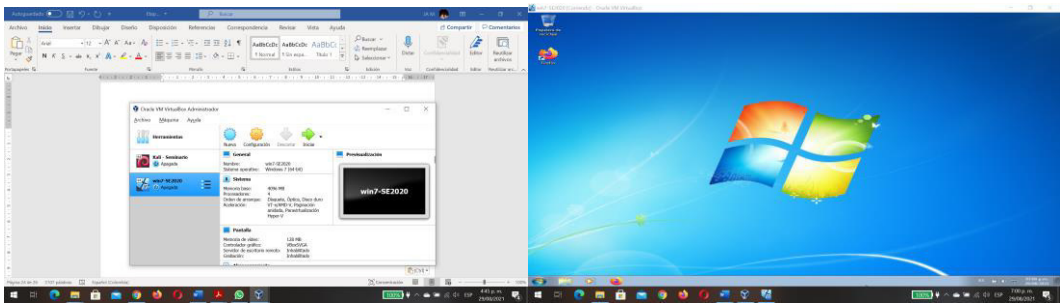

Figura: 7 Máquina Virtual W7 32 bits
Fuente: Autor

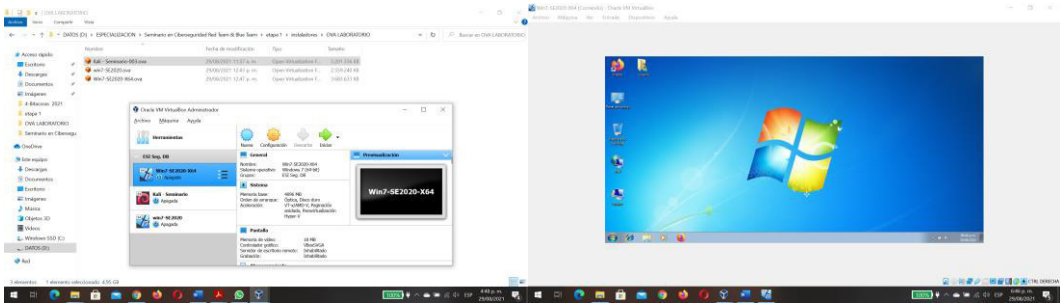

Figura: 8 Máquina Virtual W7 64 bits
Fuente: Autor

Paso C: Se realiza la validación que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux.

Una vez instaladas las máquinas virtuales se procedes a realizar un ping entre ellas para confirmar que existe comunicación.

Las direcciones ip asignadas son las siguientes

Windows 7 de 32 bits	192.168.100.27
Windows 7 de 64 bits	192.168.100.29
Kali Linux	192.168.100.27

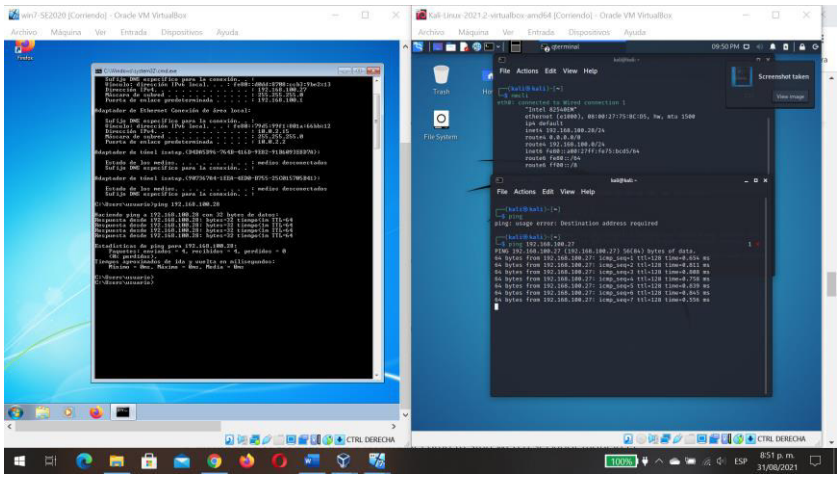

Figura: 9 Ping W7 x64 y Kali Linux
Fuente: Autor

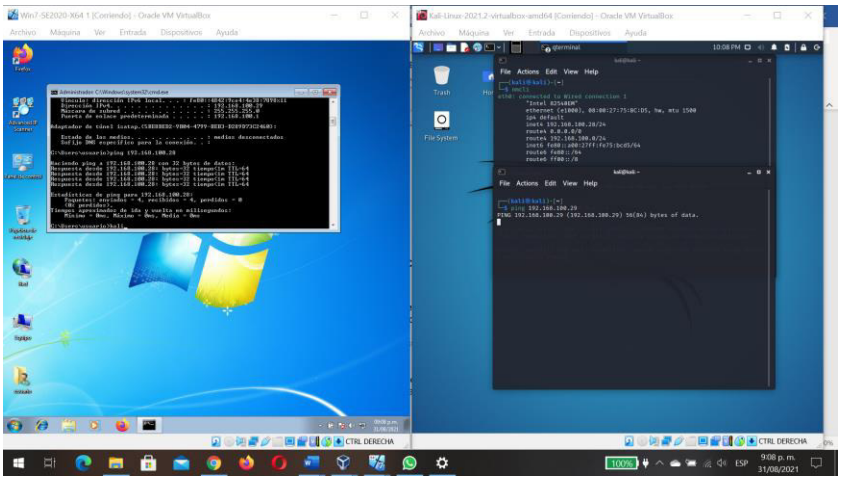

Figura: 10 ping w7 X32 y Kali Linux
Fuente: Autor

Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Se realiza la verificación de las características técnicas del Hardware de las maquinas virtuales de Windows 7 32 bits, Windows 7 64 bits y Kali Linux.

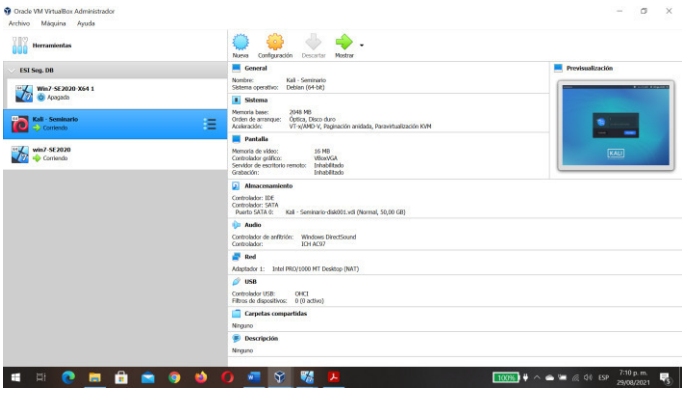

Figura: 11 Características Máquina Kali Linux
Fuente: Autor

Estas son las características en cuanto Hardware
SO Kali Linux 64 Bits
Disco Duro de 50 GB
Ram de 2048 Mb
1 procesador
1 tarjeta de Red

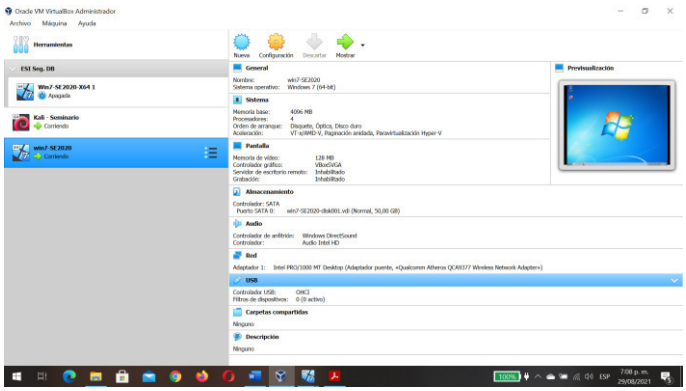

Figura: 12 Características Máquina Virtual W7 x32
Fuente: Autor

Aquí podemos evidenciar las características técnicas del Hardware de la maquina

SO Windows 7 de 32 Bits
Disco Duro de 50 GB
Ram de 4096 Mb
4 procesadores
1 tarjeta de Red

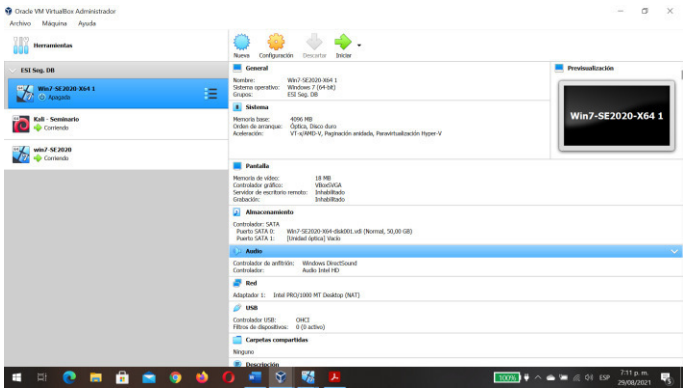

Figura: 13 Características Máquina Virtual W7 x64
Fuente: Autor

Aquí podemos evidenciar las características técnicas del Hardware de la maquina

SO Windows 7 de 64 Bits
Disco Duro de 50 GB
Ram de 4096 Mb
4 procesadores
1 tarjeta de Red

2.2. ACTUACIÓN ÉTICA Y LEGAL

2.2.1. Reconocer aspectos éticos y legales

Teniendo en cuenta que como profesionales primero que todo realizamos el juramento hipocrático en el momento de nuestra graduación debemos cumplirlo.

Como seres humanos debemos tener en cuenta los principios morales y éticos con los cuales fuimos criados para enfrentarnos ante la sociedad.

Dentro del presente acuerdo realizan una serie de exigencias con las que no estoy de acuerdo independiente mente el objeto contractual que tenga la empresa, no debe estipular en los contratos que si se encuentran temas ilegales pasemos por encima de ellos y nos hagamos los de la vista gorda.

Desde mi punto de vista no es una empresa confiable con la que quisiera laborar, puesto que tengo que hacerme cargo la responsabilidad del este tipo de información si algún ente del estado lo encuentra, y peor aún no se tiene ningún respaldo por parte de la empresa.

Fragmentos con los que no estoy de acuerdo:
Anexo 3 – Acuerdo

Primera. Objeto:
"la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados."

Segunda. Definición de información confidencial:

"datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"

Cuarta. Obligaciones de la parte receptora: en sus ítems

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

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

6. Mantener la información confidencial en reserva hasta tanto adquiera el carácter de pública.

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

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

9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security."

Octava. Solución de controversias:

"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."

2.2.2. Artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

Los siguientes artículos son los que considero son vulnerados, según las cláusulas citadas en el en el ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y WHITEHOUSE SECURITY.

Teniendo en cuenta que se puede encontrar información que ha sido producto de la actividad comercial a la que esta dedicada la empresa y que pese a que uno se percate que la información entregada y que la actividad que se puede realizar es ilegal en las cláusulas la empresa WHITEHOUSE SECURITY lo están limitando a realizar un trabajo con ética profesional, y como es bien sabido el desconocimiento de la ley no lo exime del cumplimiento de esta.

La vulneración se está llevando a cabo por parte de la empresa, pues como lo dicen en las clausulas el que firme el contrato no puede realizar las denuncias correspondientes de la información encontrada dentro de procesos ilegales realizados por la empresa, con el simple echo de tener conocimiento de esta información y no realizar las denuncias correspondientes ya lo hace cómplice de este tipo de ilícito.

Artículo 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 incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

2.2.3. Como experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio, Teniendo en cuenta el COPNIA en su código de ética para ingenieros.

Teniendo en cuenta algunos aparte de las cláusulas del contrato, pese a la asignación salarial que es muy buena, creo que prima mi buen nombre, mi reputación, mi carrera, mi familia y no va a existir ningún dinero que haga que uno viva tranquilo, con la conciencia tranquila; por eso NO firmaría el contrato ni haría la prueba la prueba de admisión.

Por eso cuando nos graduamos realizamos un juramento en el cual nos comprometemos a realizar las cosas de la mejor manera y debemos actuar con ética profesional en todos los trabajos que realizamos; así mismo sabemos que a los ingenieros estamos regulados por una normatividad legal que está dispuesta en COPNIA, que tiene un código de ética para ingenieros, estamos regidos por estas normas imperativas o de obligatorio cumplimiento que sirven de parámetro para analizar si la conducta profesional es ética o no, como profesionales tenemos que cumplir con unos deberes y obligaciones que están reglados en el capitulo II del Código de Ética de COPNIA.

Con esta normatividad estamos expuestos a la imposición de un tipo de sanciones de la siguiente manera, Amonestaciones escritas, Suspensión de la matricula profesional y hasta la cancelación de la matricula profesional, dependiendo el tipo de falta cometida, lo que nos impediría realizar cierto tipo de trabajos, o contratar con el estado.

2.2.4. Punto de vista teniendo en cuenta las implicaciones legales y éticas caso "OPERACIÓN ANDROMEDA BUGGLY" en la ciudad de Bogotá.

La "operación Andrómeda" fue un caso altamente mediático, muchas versiones se divulgaron sobre el particular, sin embargo, la realidad fáctica y jurídica del mismo no ha sido plenamente divulgado, muestra de ello es que al consultar la página de la Corte Suprema de Justicia y su sala penal, poca información se encuentra y todo se resume en la aceptación de cargos efectuada por el denominado hacker Andrés Sepúlveda por los delitos de violación ilícita de comunicaciones, uso de software malicioso, espionaje, concierto para delinquir agravado y usurpación de función pública, ya que el juez 16 de conocimiento decretó reserva en el proceso, en razón a que los dos acusados Carlos Alberto Betancur Sánchez y Luis Humberto Moreno Montes, recluidos en el Centro de Gestión Militar de Telecomunicaciones, y Wilson Leonardo Wilches oficial de la Dirección Nacional de Inteligencia, eran agentes de inteligencia, y la información allí divulgada ponía en riesgo la seguridad nacional, de ahí que la información filtrada a los medios de comunicación es limitada.

Sin embargo, y pese a la limita información existente, se puede inferir que las implicaciones legales son muchas; la Constitución Política de Colombia, a través del art. 209 permite la descentralización de la función administrativa, elemento que ha permitido que civiles puedan ejercer funciones públicas, teniendo que salvaguardar y respetar los principios constitucionales y la seguridad estatal, bajo el principio de la buena fe, principio ético atacado directamente a través de dichas salas de interceptación que muestran como los civiles estamos vulnerables ante las interceptaciones legales, hecho que a la postre debilita la institucionalidad, como diría Robert I. Rotberg, refiriéndose a los estados fallidos, los comportamientos anómicos se convierten en norma y "los gobiernos pierden credibilidad y la permanencia de la naturaleza del propio Estado-nación se vuelve dudosa e ilegítima en los corazones y en las mentes de los ciudadanos".

En el caso que nos ocupa, y a consideración del suscrito, considero que en materia penal se registró una violación a la protección de la información y de datos, específicamente la contenida en los artículos 269 A, 269 C, 269 E, 269 G, de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos de los sistemas informáticos, contenidos en la Ley 599 de 2000 (Código penal Colombiano) en circunstancias de agravación punitiva de que trata el art. 269H, numerales 2, 4, 6 y 8. Además de una clara violación de los preceptos y principios constitucionales, ya que no solo fueron particulares administrando información publica los que estuvieron inmersos en dichos hechos, si no también militares que violaron su juramento de proteger la Nación, demostrando una grave falla en la inteligencia militar.

En cuanto a implicaciones éticas, todos los Colombianos debemos regirnos por los principios soberanos contenidos en la Constitución Política, norma de normas, y con éste caso se mostró que para algunas personas los valores éticos poco importan a la hora de obtener unos ingresos económicos significativos, llegando a un punto de no diferenciar entre lo bueno y lo malo, de lo moral y derecho, desconociendo los principios fundamentales de legalidad y el mensaje dogmático de la misma, atentando contra la libertad y la paz, dentro de un marco jurídico.

Creería que la que una de las grandes fallas que tuvieron, fue la venta de información, falla que permitió que fueran denunciados.

2.3. EJECUCIÓN PRUEBAS DE INTRUSIÓN

2.3.1. Respuestas interrogantes

Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

Para la verificación de los equipos activos conectados a la red y poder identificar la máquina de Windowa 7 se utilizó la herramienta NMAP

Con el comando nmap -sn dirección ip, con el modificador -sn se configuró a nmap para que no escaneara los puertos.

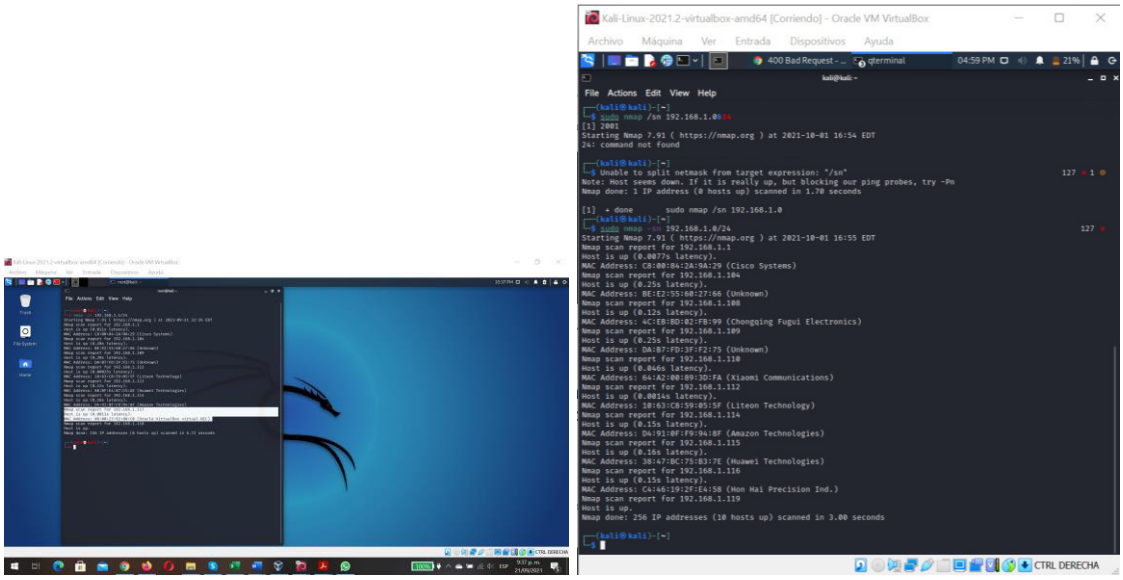

Figura: 14 Verificación Equipo en Red
Fuente: Autor

Con el comando nmap dirección ip se realizó el escaneo de los equipos activos en la red con la lectura del estado de los puertos

PORT	STATE	SERVICE
80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
554/tcp	open	rtsp
2869/tcp	open	icslap
5357/tcp	open	wsdapi
10243/tcp	open	unknown
49152/tcp	open	unknown
49153/tcp	open	unknown
49154/tcp	open	unknown
49155/tcp	open	unknown
49157/tcp	open	unknown

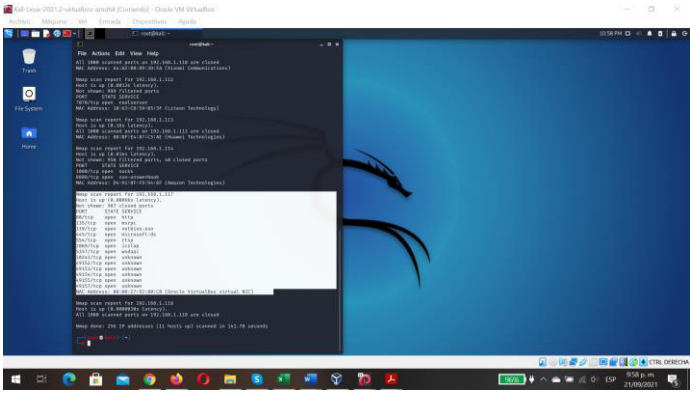

Figura: 15 Escaneo de Puestos
Fuente: Autor

Con el comando nmap -A -T4 dirección ip objetivo se realizó un escaneo para identificar el sistema operativo, el estado de los puertos con las aplicaciones que están haciendo uso de ellas.

```
┌──(root💀kali)-[~]
└─# nmap -A -T4 192.168.1.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-21 23:15 EDT
Nmap scan report for 192.168.1.117
Host is up (0.00080s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3m
|_http-server-header: HFS 2.3m
|_http-title: HFS /
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup:
WORKGROUP)
```

```
554/tcp   open  rtsp?
2869/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49157/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: PC202006, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:92:80:c0
(Oracle VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: PC202006
|   NetBIOS computer name: PC202006\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-09-21T22:17:16-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-09-22T03:17:16
|_  start_date: 2021-09-22T01:28:25

TRACEROUTE
HOP RTT     ADDRESS
1   0.80 ms 192.168.1.117

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 187.13 seconds
```

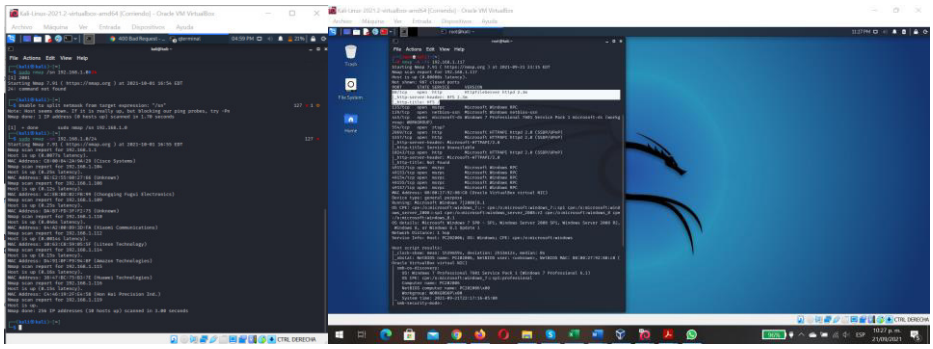

Figura: 16 Escaneo SO y Puertos
Fuente: Autor

2.3.2. Instalación de Nessus

Una vez descargo se procede a realizar la instalación de la herramienta Nessus, subir el servicio y verificación del estado del servicio, con los siguientes comandos

Instalación: *dpkg -i Nessus-8.15.2-debian6_amd64.deb*

subir el servicio: *Sudo systemctl enable nessusd*
Sudo systemctl start nessusd

verificación del estado del servicio: *Systemctl status nessusd.service*

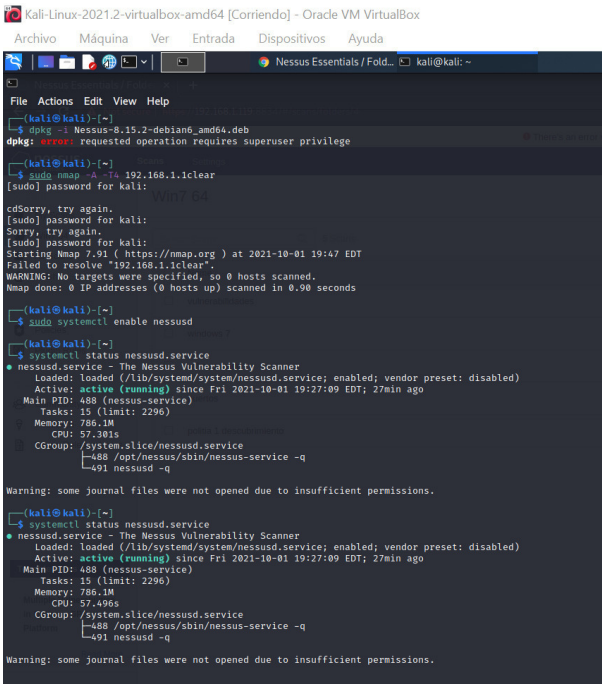

Figura: 17 Verificación Estado Servicio Nessus
Fuente: Autor

2.3.3. Escaneo de puertos con Nessus

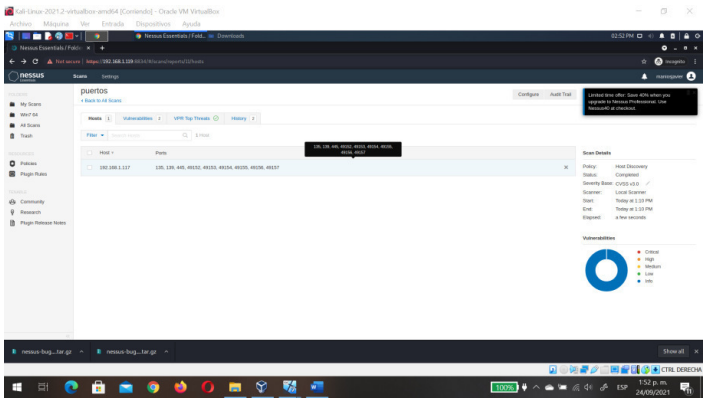

Figura: 18 Escaneo Puertos con Nessus
Fuente: Autor

2.3.4. Identificación de fallos de seguridad específico el cual ataca a la máquina windows 7 X64.

"*La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64*"

Con la información que reposa en éste párrafo es claro que nos están dando la información que es un equipo con W7 y nos están suministrando el nombre y versión de la aplicación que está facilitando la fuga, o la puerta de entrada al pc.

Fuera de esto "*asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter*"

2.3.5. Herramientas utilizadas para poder identificar los fallos de seguridad de la “máquina Windows 7”. ¿Qué puerto abre la aplicación específica en el anexo?

Para identificar los fallos de la máquina Windows utilice la herramienta Nessus

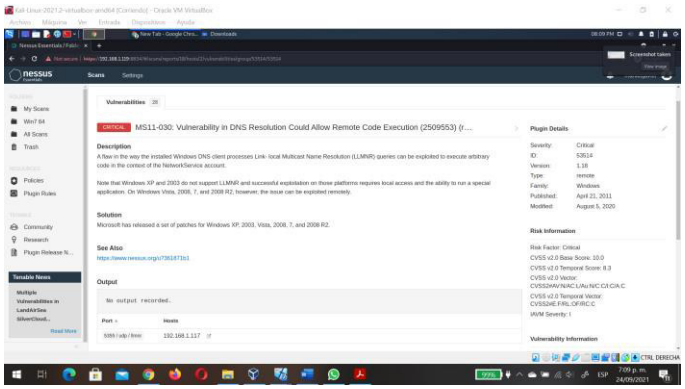

Figura: 19 Identificando Fallas W7 con Nessus
Fuente: Autor

Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.

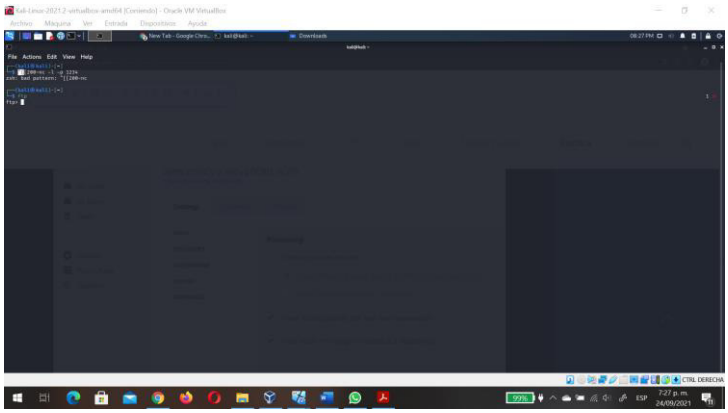

Figura: 20 Iniciando la Explotación de Vulnerabilidades
Fuente: Autor

Pasos ejecutados para explotar la vulnerabilidad en la máquina Windows 7.

Para explotar la vulnerabilidad se hace uso de la herramienta Metasploit Framework Armitage 08.13.15

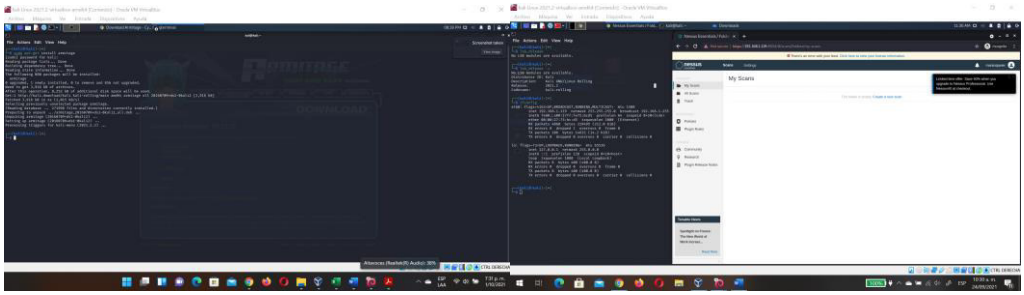

Figura: 21 Instalando Herramienta Metasploit
Fuente: Autor

Se realiza la configuración de las políticas para el escaneo general de los puertos

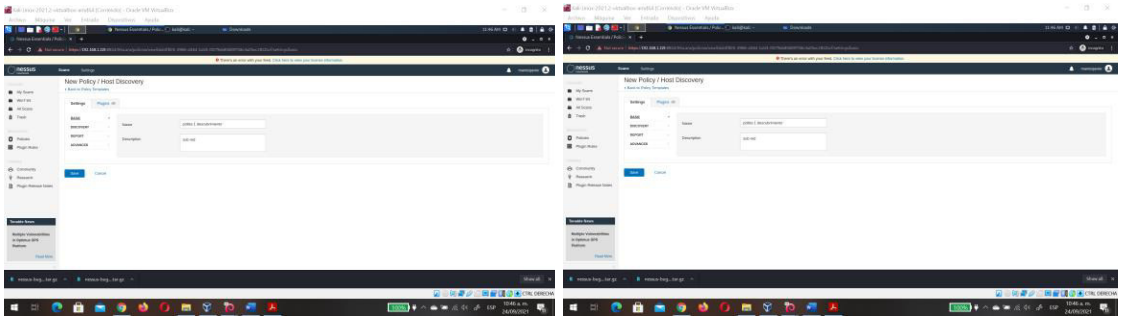

Figura: 22 Configuración Nessus para Escanear Puertos
Fuente: Autor

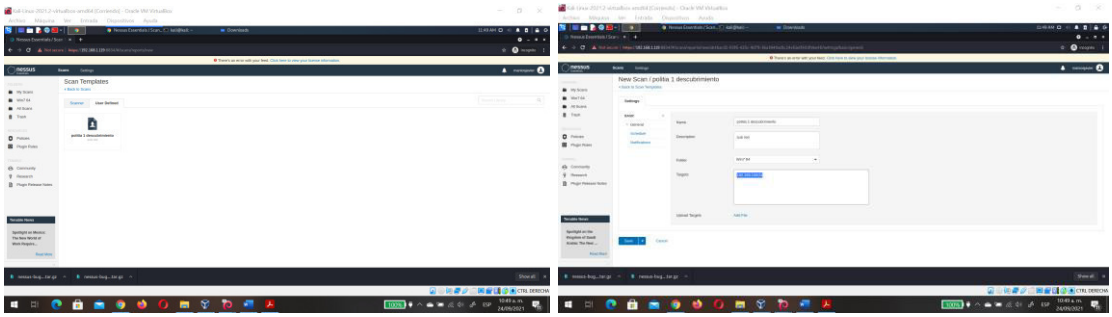

Figura: 23 Especificación de Targets y Rango de Red
Fuente: Autor

Se especifica en los targets el rango de red completo, en notificaciones especifico mi correo electrónico para que me lleguen el resultado

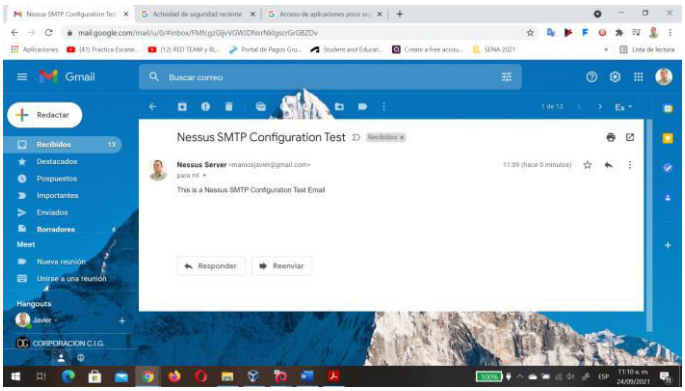

Figura: 24 Configuración Correo para reporte
Fuente: Autor

Se realiza el escaneo de los puertos

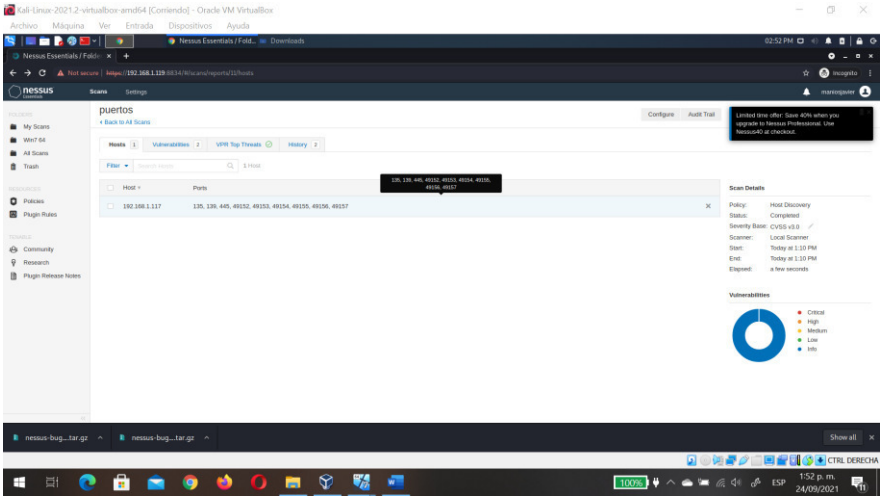

Figura: 25 Escaneo de Puertos con Nessus
Fuente: Autor

Escaneo de vulnerabilidades

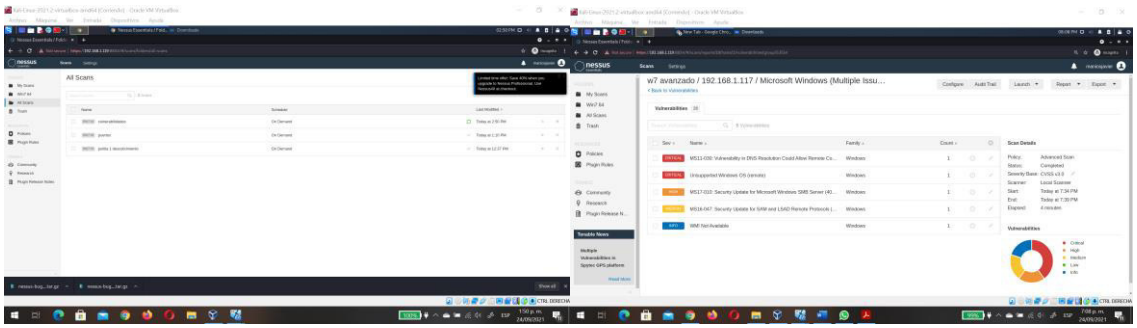

Figura: 26 Escaneo Vulnerabilidades con Nessus
Fuente: Autor

2.4. Contención de ataques informáticos

2.4.1. Análisis con acciones necesarias para contener un ataque en tiempo real.

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Como primer punto se realizaría una validación con el quipo de Red Team de la empresa sobre las anomalías que han observado y probablemente se están presentando en el sistema y teniendo en cuenta la información obtenida del equipo Read Team, realizaría el análisis al equipo que presente las vulnerabilidades.

Dentro de las vulnerabilidades más visibles podemos evidenciar que el equipo no cuenta con un sistema de antivirus, el firewall esta desactivado y teniendo en cuenta que el soporte de Windows 7 ha finalizado el 14 de enero de 2020, al dejar de recibir actualizaciones de software y seguridad continuas, estarás más expuesto a riegos de virus y malware. [1]

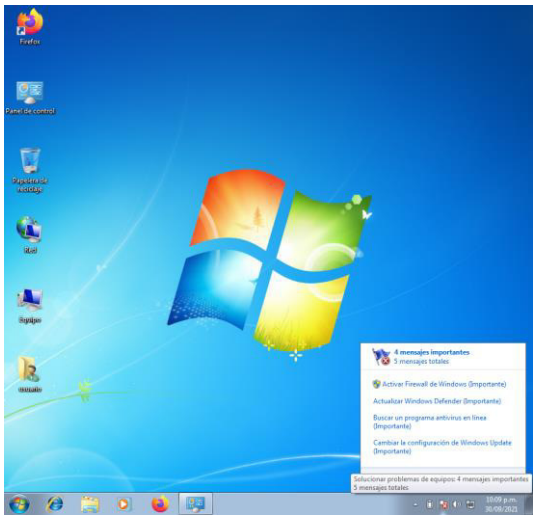

Figura: 27 vulnerabilidades w7 64
Fuente: Autor

Con la finalidad de interrumpir el ataque que se encuentra en progreso, se suspender la conexión de la red de datos con la red del ISP, para bloquear cualquier acción que se esté llevando, y se da inicio al análisis del equipo para verificar que se puede estar ejecutando.

[1] https://www.microsoft.com/es-co/windows/windows-7-end-of-life-support-information

2.4.2. Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

Teniendo en cuenta el ataque ejecutado las medidas de endurecimiento informático que propondría para garantizar la seguridad y buena defensa sería lo siguiente.

Realizar el cambio de las claves que hayan generado por defecto.
Realizar la desinstalación del software que no sea requiera.
Si existen varios usuarios, dejar solo los usuarios que sean necesarios.
Deshabilitar los servicios que no se están utilizando.
Verificar los puestos que estén en uso y cerrar los que están sin uso.
Recomendar la realización de backup de respaldo de toda la información.
Realizar la instalación del firewall.
Generar la actualización de los sistemas operativos en cuanto a parches de seguridad.

En cuanto a usuarios se recomienda:
Que no se abran archivos que no sean conocidos.
No abrir correos con archivos adjuntos o link de remitentes desconocidos.
Estar cambiado constantemente las credenciales de acceso.

2.4.3. Análisis sobre las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos

¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

En equipo Blueteam está dedicado a realizar todo lo correspondiente a análisis de comportamientos del sistema, aplicaciones y personas, realiza la evaluación de riesgos, análisis forense, es el encargado de proponer soluciones y establecer las respectivas medidas para la detección de futuras eventualidades y además, propone las respectivas mejoras de Ciberseguridad para la Empresa; así mismo realiza el rastreo de los posibles ataques de Ciberseguridad.

En cuando al Equipo de Respuesta a Incidentes Informáticos está dedicado realizar la identificación de las causas y consecuencias de los incidentes, realiza análisis y responde a los incidentes, es el encargado de actuar en el momento que se presentan los hechos sospechosos, realiza la hardenización, y están dedicados

a dar una respuesta rápida y efectiva a incidentes para garantizar la operabilidad total de la empresa.

2.4.4. Análisis sobre la pertinencia de trabajar con CIS "Center For Internet Security" como propuesta de aseguramiento por parte de un equipo de Blue Team.

¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

Teniendo en cuenta que el CIS es utilizado son un conjunto de medidas de ciberdefensa recomendadas diseñadas para proteger su organización contra piratas informáticos y ciberdelincuentes[2], yo utilizaría el CIS en general contra la prevención de amenazas, y a su vez se realizaría para protección de datos, gestión de respuestas a los incidentes que se presenten y a realizar las respectivas pruebas de penetración, que serían una herramienta primordial para dar un valor agregado a la empresa.

2.4.5. Análisis sobre las funciones y características principales de un SIEM.

Explique y redacte las funciones y características principales de lo que es un SIEM.

SIEM Security Information and Event Management es una herramienta que nos facilita la detección, responder y neutralizar las amenazas informáticas rápidamente.

Dentro de las principales características de las que se dispone en un buen sistema SIEM es aplicado a la seguridad y respuesta rápida, teniendo en cuenta que el SIEM está elaborado para fortalecer e incrementar el nivel de seguridad de la empresa y dentro de esas características tenemos.

- Funciona con agregación de datos de fuentes diferentes: sistemas de seguridad como IDS o IPS, de routers y de sistemas.
- Presenta reglas internas de correlación, para poder inferir actividad maliciosa.
- Es capaz de generar alertas propias cuando hay indicios de posibles ciberataques o amenazas.
- Permite la visualización de los datos en cuadros de mando para obtener métricas y poder tomar las decisiones estratégicas necesarias en materia de seguridad informática.

[2] https://www.rsisecurity.com/center-for-internet-security/

- Un Sistema SIEM almacena información durante largos períodos de tiempo. Esto permite poder visualizar todo el proceso de una intrusión: el antes, el durante y el después

2.4.6. Informe de elección de 3 herramientas que permitan contener ataques informáticos.

Defina por lo menos 3 herramientas de contención de ataques informáticos "hardware o software", recuerde que las herramientas de contención son diferentes a las herramientas de detección.

2.4.6.1. Servidor Proxy

Un servidor proxy es un programa que actúa como intermediario entre las conexiones del navegador e Internet, filtrando todos los paquetes entre ambos, es una de las herramientas utilizadas en seguridad informática por ser utilizada para bloquear sitios web que sean catalogados como sospechosos o peligrosos; este servidor es utilizado para limitar el acceso a la red externa.

2.4.6.2. Escáner de vulnerabilidades

Es una herramienta de seguridad informática que se encarga de detectar, analizar y gestionar los puntos débiles del sistema.

2.4.6.3. Firewall Perimetral de Red

Es una herramienta de ciberseguridad que es el encargado de escanear los paquetes de red, que según la parametrización definida por el administrador permitiéndoles o bloqueándoles el paso.

Si bien es cierto que su estructura es básica si se compara a la sofisticación de las amenazas, se pueden encontrar firewalls modernos que pueden clasificar los archivos utilizando varios parámetros. Así, se puede inspeccionar con eficiencia el tráfico web, identificar a usuarios, bloquear el acceso que no está autorizado, entre otras acciones.

3. CONCLUSIONES

Aunque existe una normatividad en Colombia que regula los delitos informáticos, se hace necesario que exista en el estado una dependencia dedicada a realizar un seguimiento arduo en las redes.

Con el pasar del tiempo se deben ir generando he implementado mas medidas de seguridad y contención de ataques en las empresas, porque los ciberdelincuentes se están actualizando constantemente.

El seminario de Equipos Estratégicos en Ciberseguridad Red Team & Blue Team juega un papel muy importante en cuanto a la ampliación de conocimiento frente a la seguridad informática.

4. RECOMENDACIONES

Toda empresa del país debería tener dentro de su equipo de trabajo, al personal de experto en Red Team & Blue Team, teniendo en cuenta que contamos con acceso a internet y esto nos hace vulnerables.

El personal encargado de la parte tecnológica de las empresas, capacitarse sobre como reaccionar frente a un posible ataque informático, mientras es contactado personal idóneo en el área.

Las empresas deberían capacitar a su personal frente a las medidas de seguridad sobre la manera correcta del manejo de la información de la empresa y la importancia de utilizar credenciales seguras y su responsabilidad.

Se debe realizar a diario copias de seguridad de la información de a empresa y guardada en sitios distintos para evitar perdida de la misma.

REFERENCIAS BIBLIOGRÁFICAS

Colombia, C. d. (05 de 01 de 2009). alcaldiabogota.gov.co. Obtenido de LAXMIKOWTA, A. S. et al. Analysis and Overview of Information Gathering & Tools for Pentesting. 2021 International Conference on Computer Communication and Informatics (ICCCI), Computer Communication and Informatics (ICCCI), 2021 International Conference on, [s. l.], p. 1–13, 2021. DOI 10.1109/ICCCI50826.2021.9457015. Disponível em: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edseee&AN=edseee.9457015&lang=es&site=eds-live&scope=site. Acesso em: 27 ago. 2021.

LOPEZ MOLINA, A. del P. Pentesting Web. [S. l.: s. n.]. Disponível em: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=ir00913a&AN=unad.10596.25188&lang=es&site=eds-live&scope=site. Acesso em: 27 ago. 2021.

CARDWELL, K. Building Virtual Pentesting Labs for Advanced Penetration Testing - Second Edition. Birmingham: Packt Publishing, 2016. v. Second editionISBN 9781785883491. Disponível em: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=1344064&lang=es&site=eds-live&scope=site. Acesso em: 27 ago. 2021.

Cardwell, Kevin. 2016. Building Virtual Pentesting Labs for Advanced Penetration Testing - Second Edition. Vol. Second edition. Community Experience Distilled. Birmingham: Packt Publishing. http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=1344064&lang=es&site=eds-live&scope=site.

Régimen de protección del secreto empresarial en Colombia https://www.uninorte.edu.co/documents/4368250/13180762/actualidad-juridica-10-45-53.pdf/39b77b50-83b0-44a5-8785-45bb188d3b1f#:~:text=El%20secreto%20industrial%20se%20encuentra,de%20transmitirse%20a%20un%20tercero.

Mecanismos alternativos de solución de conflictos https://www.asuntoslegales.com.co/consultorio/mecanismos-alternativos-de-solucion-de-conflictos-2834963

Cómo instalar Nessus en Kali Linux https://backtrackacademy.com/articulo/como-instalar-nessus-en-kali-linux

ALCALDÍA DE BOGOTÁ. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. {En línea}. {Consultado el 5 de febrero de 2021}. Disponible en: http://ticbogota.gov.co/sites/default/files/seguridad-de-lainformacion/ambito2.pdf

ALLEN, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). {En línea}. {Consultado el 3 de febrero de 2021}. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29) {En línea}. {Consultado el 3 de febrero de 2021}. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

CIS SECURITY. (2020). CIS Center for Internet Security. CIS Benchmarks. Recuperado de: https://www.cisecurity.org/cis-benchmarks/

COPNIA. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf/

PETTERS. Jeff. What is SIEM? A Beginner's Guide. En: Varonis. [sitio web]. [15, junio, 2020]. Disponible en: https://www.varonis.com/blog/what-is-siem/

RSI SECURITY. What is the Center for Internet Security (CIS)?. [Sitio Web]. [03, julio, 2020]. Disponible en: https://blog.rsisecurity.com/what-is-the-center-for-internet-security-cis/

William Khepri May 28, 2018·16 min read Las 25 mejores herramientas de Kali Linux https://medium.com/@williamkhepri/breve-introducci%C3%B3n-al-fingerprint-6daa5e0b3604

Fernando Tablado 5 abril, 2021 El Pentesting y su importancia en la ciberseguridad https://protecciondatos-lopd.com/empresas/pentesting/

Julio Prada 20 octubre, 2020 PENTESTING WIFI: HACKING ÉTICO DE REDES DOMÉSTICAS https://www.datio.com/security/pentesting-wifi-hacking-etico-de-redes-domesticas/