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

LUIS ALBERTO JARAMILLO GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

SEMINARIO ESPECIALIZADO EQUIPOS ESTRATEGICOS CIBERSEGURIDAD

BOGOTA DC

2021

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

LUIS ALBERTO JARAMILLO GONZALEZ

Anteproyecto para optar por el título de

Diplomado especializado equipos estratégicos en ciberseguridad

JOHN FREDDY QUINTERO

Director de curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

SEMINARIO ESPECIALIZADO EQUIPOS ESTRATEGICOS CIBERSEGURIDAD

BOGOTA DC

2021

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá DC, 09 de Octubre de 2021

CONTENIDO

Ilustraciones

GLOSARIO

Ciberseguridad[1]: La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

Kali Linux[2]: Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar la antecesora de Kali Linux.

Redteam[3]: Un Red Team es un ejercicio, el cual consiste en simular un ataque dirigido a una organización, lo que se traduce que un grupo de personas internas o externas a la empresa, comprueban la posibilidad de tener acceso a los sistemas, comprometerlos y el impacto que esto podría tener en el negocio.

---

[1] ¿Que es la ciberseguridad? [Consultado el 09 de octubre 2021] Disponible en URL: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[2] Kali Linux [Consultado el 09 de octubre 2021] Disponible en URL: https://es.wikipedia.org/wiki/Kali_Linux

[3] ¿Que es RedTeam en ciberseguridad? [Consultado el 09 de octubre 2021] Disponible en URL: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

Blueteam[4]: Blue Team (seguridad defensiva): es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva.

Virtualbox[5]: VirtualBox es el software de virtualización de código abierto más popular. Con su ayuda, puedes ejecutar cualquier sistema operativo, por ejemplo, Windows, Linux, Mac, Android. El programa tiene una interfaz rápida y es fácil de usar.

Firewall[6]: Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Exploit[7]: Un exploit es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware. Por lo general, los exploits toman la forma de un programa de software o una secuencia de código previsto para hacerse con el control de los ordenadores o robar datos de red. En las páginas siguientes puede obtener información sobre la procedencia de los exploits, cómo funcionan y qué puede hacer para protegerse.

---

[4] RedTeam, BlueTeam y PurpleTeam, Cuales son sus funciones y diferencias? [Consultado el 09 de octubre de 2021] Disponible en URL: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[5] ¿Que es VirtualBox y para que sirve? [Consultado el 09 de octubre 2021] Disponible en URL: https://www.msn.com/es-es/noticias/tecnologia/qué-es-virtualbox-y-para-qué-sirve/ar-BB1f4nku

[6] ¿Que es un Firewall? [Consultado el 09 de octubre 2021] Disponible en URL: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

[7] Exploits: Todo lo que debes saber [Consultado el 09 de octubre 2021] Disponible en URL: https://www.avast.com/es-es/c-exploits

DDoS[8]: Un ataque de denegación de servicio distribuido, o DDoS, es el bombardeo de solicitudes de datos simultáneas a un servidor central. El atacante genera estas solicitudes desde múltiples sistemas comprometidos.

DMZ[9]: Una zona desmilitarizada (demilitarized zone, DMZ) es una red perimetral que protege la red de área local (local-area network, LAN) interna contra el tráfico no confiable. Un significado común para una DMZ es una subred que se encuentra entre la Internet pública y las redes privadas. Expone los servicios externos a redes no confiables y agrega una capa adicional de seguridad para proteger los datos confidenciales almacenados en redes internas, utilizando firewalls para filtrar el tráfico.

DNS[10]: El sistema de nombres de dominio (DNS) es el directorio telefónico de Internet. Las personas acceden a información en línea mediante nombres de dominio, como nytimes.com o espn.com. Los navegadores web interactúan mediante direcciones de protocolo de Internet (IP). El DNS traduce los nombres de dominio a direcciones IP para que los navegadores puedan cargar los recursos de Internet.

Integridad[11]: Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites

[8] ¿Que es un ataque DDoS? [Consultado el 09 de octubre 2021] Disponible URL: https://www.cisco.com/c/es_es/products/security/what-is-a-ddos-attack.html
[9] ¿Que es una red DMZ? [Consultado el 09 de octubre 2021] Disponible URL: https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz
[10] What is DNS? How DNS works [Consultado el 09 de octubre 2021] Disponible URL: https://www.cloudflare.com/es-es/learning/dns/what-is-dns/
[11] Integridad de la informacion [Consultado el 09 de octubre 2021] Disponible URL: https://marinajesusseguridadinformacion.wordpress.com/2018/05/14/integridad-de-la-informacion/

bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

Pentesting[12]: Es una abreviatura de las palabras inglesas “penetration” y “testing”, que significa test. Pentesting o Penetration Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.

[12] Que es el pentesting? [Consultado el 09 de octubre 2021] Disponible URL: https://openwebinars.net/blog/que-es-el-pentesting/

RESUMEN

El presente documento es el informe tecnico final donde se plasmara todo el proceso realizado paso a paso, los escenarios de pruebas que fueron tenidos en cuenta y cada una de las acciones que se realizaron desde las perspectivas de los dos equipos de Ingenieros de Ciberseguridad Red Teams y Blue Teams, estará tambien considerado el marco legal que fue tenido en cuenta durante el proceso de pruebas de acceso a los sistemas de información, como las recomendaciones de buenas practicas que debe implementar la empresa WhiteHouse Security para reforzar sus sistemas internos para prevenir posibles ataques en un futuro. Este documento contiene evidencias de las vulnerabilidades encontradas durante la ejecución de las pruebas, que software mal intencionado fue detectado al interior de la red de datos de WhiteHouse Security y como se realizo el proceso de contención de esta amenaza al interior de la red de la compañía.

INTRODUCCION

El presente documento se muestra con detalle el proceso realizado por los equipos de ciberseguridad Red Teams (Equipo rojo) y Blue Teams (Equipo Azul) durante el proceso de validación de la seguridad de la red interna de la empresa WhiteHouse Security, utilizando diferentes tipos de software y hardware para realizar todos los pasos que indica el PenTesting como lo son la planificación y preparación del pentesting, la investigación, el intento de penetración y explotación, el análisis y generación del informe, la limpieza y remediación y el retesteo de la red, generando este informe con el resumen de las vulnerabilidades encontradas en el análisis realizado sobre la red interna de la compañía y realizando unas recomendaciones de seguridad informática que se sugiere se apliquen al interior de la compañía para mejorar su seguridad y para evitar posibles futuros ataques o intentos de ataque sobre su red de datos o sobre sus sistemas de información como servidores, equipos de computo de usuarios dentro de la red o bases de datos donde pueda haber información sensible que no deba verse comprometida y deba cuidarse con mucho detalle.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Realizar un informe técnico donde se presente el paso a paso de la estrategia técnica utilizada para analizar, contener y mitigar una vulnerabilidad dentro de la red de WhiteHouse Security

1.2 OBJETIVOS ESPECÍFICOS

- Identificar la normatividad colombiana vigente con relación a los delitos informáticos y la protección de información personal
- Describir el proceso de identificación, mitigación y contención de las vulnerabilidades halladas en la red de datos de la empresa WhiteSecurity
- Presentar las herramientas utilizadas durante el proceso de pentesting
- Realizar recomendaciones desde la perspectiva de los equipos Rojo y Azul (RedTeam y BlueTeam)
- Realizar video de sustentación del trabajo en plataforma digital

2 JUSTIFICACIÓN

El desarrollo de esta actividad, esta motivado por una posible falla de seguridad en la red interna de la empresa WhiteHouse Security, donde la misma realiza una contratación a un equipo de seguridad para que diagnostique el problema utilizando la metodología de RedTeam y BlueTeam, validando cual es la causa de la filtración de información, identificando cuantos equipos de computo o servidores fueron comprometidos, y realizando un proceso de contención de los mismos dando recomendaciones de seguridad que pueden ser implementadas por la compañía para mejorar su seguridad en la red interna y evitar que este problema se vuelva a presentar dentro de su red de datos.

3 MARCO DE REFERENCIA

3.1 MARCO TEÓRICO

Identificar las posibles amenazas informáticas que se estén presentando en la empresa WhiteHouse Security proveyendo una solución tecnológica y de seguridad para mitigar los riesgos y controlar las fallas de seguridad al interior de la compañía.

3.2 MARCO LEGAL

En la actualidad, en nuestro país Colombia, se dio la mayor importancia a la información y a la evolución del uso diario de esta información sobre las infraestructuras tecnológicas, para así dar una mejor respuesta y realizar con mayor eficiencia los diferentes procesos que requieren las compañías privadas, publicas, mixtas o incluso las personas naturales; cuando se incluyo este componente, se tomo en cuenta las bases tecnológicas de almacenamiento y custodia de la información, por tanto es importante definir cuales son las herramientas jurídicas que puedan generar acciones de tipo legal en caso de presentarse algún delito informático o un uso no adecuado de los datos personales de los usuarios. Por lo tango se realizo la generación de 2 leyes que realizan adiciones a el código penal y adicionan una nueva sección sobre los delitos informáticos y un apartado adicional para el tratamiento de datos personales.

El desarrollo de este documento, esta basado en estas dos normativas, la primera la ley 1273 de 2009[13] y la Ley estatutaria 1581 de 2012[14].

[13] 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. [Consultado el 09 de octubre 2021] Disponible en URL: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

[14] Por la cual se dictan disposiciones generales para la protección de datos personales. [Consultado el 09 de octubre 2021] Disponible en URL: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Se detallará a continuación las leyes o los decretos que aplican en Colombia y que se encuentran vigentes para la aplicación de la seguridad informática:

Ley 1273 de 2009[15]: la presente ley dispuso la modificación del código penal reglamentando el "bien jurídico tutelable de la protección de la información y de los datos", dicho proceso se legislo por el incremento de uso de las tecnologías de la información y comunicación, viéndose cada día la implementación y tecnificación de procesos, pasando del resguardo de información sensible y confidencialidad en carpetas, archivadores o bodegas, a equipos de cómputo, infraestructura tecnológica o al modelo de cloud computing; por lo anterior se debió legislar de tal manera que si una persona natural o jurídica atenta contra la confidencialidad, integridad y disponibilidad de los datos de sistemas informáticos tal como el acceso a sistemas informáticos sin el debido permiso, obstaculización en el correcto funcionamiento de un sistema informático o red de comunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, suplantación de sitios web para la captura de datos personales tendría implicaciones legales y punitivas, de igual manera se definen como atentados informáticos u otras infracciones realizar algún proceso de captación de información sin autorización, intrusión a un sistema informático sin el debido permiso, robo de bienes intangibles a través de medios informáticos.

Ley 1581 de 2012[16]: la ley derogo lo que corresponde a la ley 1266 de 2008, dando un espectro más amplio y no limitado únicamente a la información de tipo financiero, crediticio, comercial, de servicios y lo proveniente de terceros países; la ley busco generalizar el concepto de protección de datos personales, manteniendo los

[15] 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. [Consultado el 09 de octubre 2021] Disponible en URL: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

[16] Por la cual se dictan disposiciones generales para la protección de datos personales. [Consultado el 09 de octubre 2021] Disponible en URL: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

principios rectores de la Ley 1266 de 2008 y anteriormente la ley 527 de 1999, en el cual se fundamenta el cumplimiento de tratamiento de datos personales, legalidad en materia de tratamiento de datos, uso para los fines dispuestos, libertad de aceptación y autorización del uso, veracidad de la información almacenada, transparencia, de acceso y circulación restringida, de seguridad y confidencialidad; un cambio respecto a las anteriores leyes es el hecho de categorizar los datos como datos sensibles y definición de que dato se puede considerar sensible, el tratamiento que se debe dar y disposiciones referente a la información de menores de edad. Se plantean los derechos y deberes en el proceso del tratamiento de datos personales por cada uno de los actores que resguarden este tipo de información. La SIC se mantiene como la entidad encargada de hacer cumplir las disposiciones de la presente ley y generar auditorias para la verificación del cumplimiento de lo dispuesto. Un punto importante de la ley 1581 de 2012 es la creación del Registro Nacional de Bases de Datos (RNBD), definiéndose como el directorio público en donde toda entidad que resguarde datos personales deberá realizar un registro de sus bases de datos y las políticas estipuladas a nivel interno para salvaguardar el cumplimiento de los datos personales.

Decreto 1377 de 2013[17]: por medio del cual se reglamenta de manera parcial la ley 1581 de 2012 y a través de la cual se estipula la disposiciones para el proceso de recolección de los datos personales, buscando dar cumplimiento a los principios rectores y hacer uso de la información únicamente para la finalidad por lo cual fue entregado, deberá existir una autorización explicita del titular de los datos personales para su tratamiento, teniendo el titular la capacidad de retirar la autorización y solicitar en cualquier momento las pruebas de dicha autorización. Uno de los elementos principales del presente decreto es la reglamentación de que toda entidad pública o privada que realice tratamiento de datos personales debe implementar una política de tratamiento de datos personales, divulgarla al interior de cada organización, darle cumplimiento, hacerlo parte de la cultura

[17] Decreto 1377 de 2013 [Consultado el 09 de octubre de 2021] Disponible en URL: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

organizacional, en la política debe estar contenido el proceso de tratamiento de datos personales, los derechos, los deberes y responsabilidades del tratador de los datos.

4 DISENO METODOLÓGICO

4.1 MÉTODO DOCUMENTAL

Para el desarrollo de este informe técnico, se va a utilizar la metodología documental, donde vamos a realizar el proceso de valoración de la red, recopilamos información, ejecutamos los procesos necesarios para realizar la contención y todas las evidencias las documentamos a modo de imágenes, conceptos y diagramas en el presente informe.

4.2 FUENTES Y TÉCNICAS DE RECOLECCION DE INFORMACION

Para recolectar la información correspondiente a este informe, nos basamos en la arquitectura con la que cuenta la empresa WhiteHouse Security, las copias de las maquinas virtuales que ellos nos entregaron para realizar los análisis y con los resultados que obtuvimos al ejecutar los análisis de seguridad, también nos basamos en recursos en línea sobre la ejecución de comandos de Kali Linux en la consola y la ejecución de un exploit de forma remota a un equipo Windows 7.

5 DESARROLLO DE LA PROPUESTA

5.1 DESARROLLO OBJETIVO ESPECÍFICO 1

Identificar la normatividad colombiana vigente con relación a los delitos informáticos y la protección de información personal

Leyes y decretos en Colombia

Dentro del marco legal en Colombia sobre delitos informáticos y protección de datos personales, se puede encontrar la ley 1273 de 2009 donde se normal los delitos informáticos en Colombia como lo son el acceso abusivo a sistema informático (articulo 269A), o la obstaculización ilegitima de sistema informático o red de telecomunicación (articulo 269B) o la interceptación de datos informáticos (articulo 269C) y muchos mas.

También podemos encontrar que en Colombia rige el decreto numero 1377 del 27 de junio del 2013 por la cual se dictan las disposiciones general es para la protección de datos personales en Colombia, la identificación y el tratamiento de los datos en el ámbito personal o domestico y en un ámbito empresarial, los avisos de privacidad que estarían dirigidos al titular para informarle que se realizaría con su información, la distinción y clasificación de lo que es un dato publico o un dato sensible.

Tenemos la ley estatutaria 1581 de 2012 por la cual el congreso de Colombia dicta las disposiciones generales para la protección de datos personales, definiendo (similar a la anterior) la autorización previo consentimiento expreso e informado del titular para realizar cualquier recopilación y tratamiento de su información personal, adicional se debe identificar y catalogar un dato personal y un dato publico, y se deben garantizar los principios que establece esta ley como lo son el principio de finalidad, principio de libertad, principio de veracidad o calidad, principio de

transparencia, principio de acceso y circulación restringida, principio de seguridad y el principio de confidencialidad.

Etapas de las pruebas de penetración o pentesting

Las pruebas de penetración o conocidas como pentesting, son pruebas que se realizan con herramientas informáticas avanzadas, para poder recopilar información de un objetivo (Sea una red de datos, un servidor, computador de escritorio, teléfono celular, entre otros) y poder explotar vulnerabilidades encontradas en la fase de recopilación de información, logrando accesos a zonas privadas donde pueden haber activos informáticos de valor para la compañía, siempre se debe recordar que este tipo de procedimientos se deben ejecutar con el previo consentimiento de la empresa o persona dueña de la información o del sistema de información que se desea testear, ya que en caso de no contar con una autorización explicita este tipo de acciones puede ser catalogada como un delito informático.

Para realizar este tipo de pruebas de penetración, existen una serie de pasos que se deben ejecutar en estricto orden para poder llevar una correcta secuencia y que la información recopilada sea de utilidad para la empresa que solicito los servicios, estos pasos son los siguientes:

Fase de recolección de información

Esta etapa es la primer etapa o la etapa de exploración, donde la persona que va a ejecutar la prueba, no tiene mucho conocimiento del sistema de información o de la configuración de la red que se desea validar, por tal motivo se utilizan herramientas tecnológicas como lo son NMap para realizar un mapeo de la red destino, donde podemos obtener un listado de todos las direcciones IP que están siendo utilizadas en la red informática, con un listado muy detallado de cuales puertos están

expuestos y que protocolos utilizan. En esta etapa es muy común encontrar puertos que utilizan protocolos inseguros y que pueden ser atacados en posteriores pasos para lograr encontrar vulnerabilidades, también se pueden encontrar puertos que estén abiertos en un servidor y no estén adecuadamente asegurados con claves lo suficientemente robustas para soportar un ataque de diccionario, también se pueden encontrar puertos que no se estén utilizando por el servicio que se esta exponiendo, por ejemplo un servidor de aplicación que tenga puertos diferente al 80 y al 443 expuestos, estos no deberían estarlo ya que no son necesarios para el tipo de servicio.

Fase de búsqueda de vulnerabilidades

Esta etapa es la segunda de la lista de pasos para realizar una prueba de penetración a un sistema informático, en esta fase, ya contamos con la información que obtuvimos del primer punto (Como puertos abiertos innecesarios, protocolos inseguros, entre otros), con esta información ya podemos nosotros trabajar para correr una herramienta de búsqueda de vulnerabilidades sobre los puntos que consideremos sean débiles en la red o en el servidor objetivo, para esta actividad, podemos utilizar la herramienta rkHunter, esta herramienta permite orientarla a una dirección IP puntual y esta herramienta busca las vulnerabilidades que encuentra y nos genera un log que podemos parametrizar para encontrar aquí mayor información de las vulnerabilidades encontradas en el objetivo.

Fase de explotación de vulnerabilidades

Esta es la tercera etapa de los pasos para realizar una correcta prueba de penetración a un sistema informático, es posiblemente la etapa favorita de todos ya que es la etapa donde realmente se corren herramientas informáticas como lo son

metasploit, herramienta que realiza el proceso de explotar la vulnerabilidad encontrada en los pasos anteriores y busca tener accesos que normalmente no estarían autorizados, tener acceso a archivos, a bases de datos, realizar suplantación de usuarios privilegiados o buscar acceder a web apis que normalmente no se tendrían acceso, esta fase igual que las anteriores, debe documentarse correctamente como parte del proceso del pentesting, que herramientas se utilizaron, que resultados se obtuvieron, entre otra información, y toda esta información recopilada debe quedar dentro del informe final.

Fase de post-explotación de vulnerabilidades

Esta es la cuarta etapa de los pasos del pentesting, en esta relacionada con la post-explotacion de las vulnerabilidades encontradas en los pasos anteriores, utilizando herramientas como lo son metaesploit, se busca en la base de datos de exploits disponibles para el tipo de vulnerabilidades encontradas y se ejecutan estos procedimientos sobre las vulnerabilidades, intentando obtener acceso a recursos privados, o escalando permisos de una forma no esperada por el administrador de la plataforma

Fase de informe de vulnerabilidades

Esta es la ultima etapa de la ejecución del procedimiento para pruebas de vulnerabilidades, y es la generación del informe de vulnerabilidades, en este informe debe quedar consolidado de forma integral el paso a paso que se utilizo durante los pasos anteriores, evidencias de las acciones que dieron resultados satisfactorios para lograr explotar vulnerabilidades en los sistemas de información, en este informe se debe reportar que herramientas fueron utilizadas, el proceso utilizado en

las pruebas de intrusión, y cuales fueron las vulnerabilidades encontradas, para que el administrador de la plataforma pueda solucionarlas.

5.2 DESARROLLO OBJETIVO ESPECÍFICO 2

Describir el proceso de identificación, mitigación y contención de las vulnerabilidades halladas en la red de datos de la empresa WhiteSecurity

Para el desarrollo de esta actividad, es necesario tener unas pre condiciones, estas son tener una maquina de Kali Linux instalada y una maquina de Windows 7 configuradas, para el desarrollo de esta actividad, utilice VirtualBox como herramienta de virtualización, cree una red NAT local con segmento 192.168.1.0/24, donde coloque ambas maquinas para que tuviera comunicación entre ellas, se descargaron las imágenes de los 2 sistemas operativos de la actividad 1 donde se entregan estos recursos por parte del tutor de este curso.

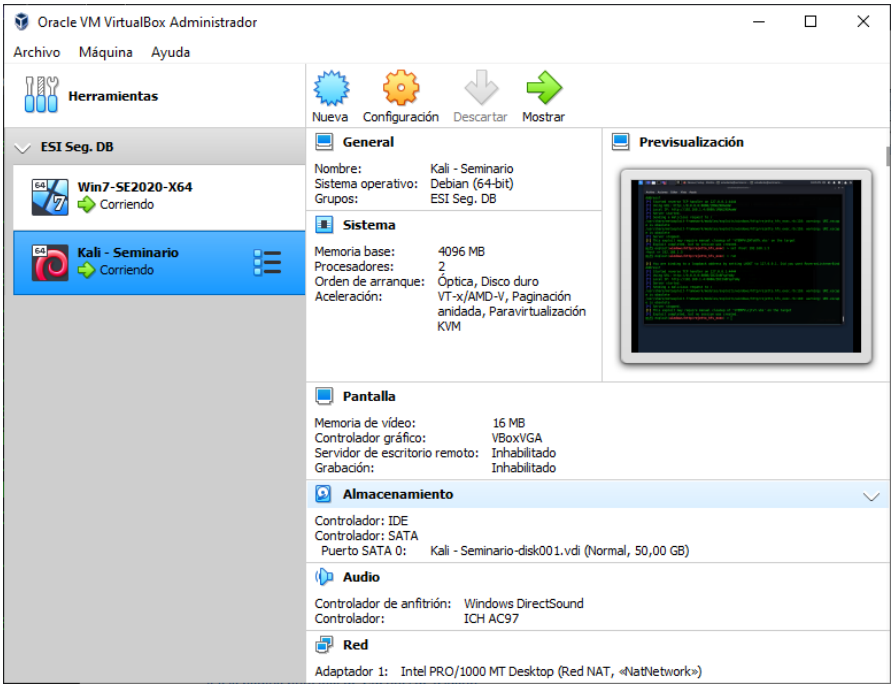

Ilustración 1 Configuracion VirtualBox como pre-requisito

Ahora nos enfocaremos en la maquina de Kali Linux, aquí debemos realizar una continuación del adaptador de red para que de manera fija tome una dirección IP del segmento de la configuración del NAT local (Que es 192.168.1.0/24), en este caso esto se hace por la interfaz grafica, se asigna una dirección IP del segmento y luego se ejecuta el comando sudo ifconfig para poder identificar cual es la dirección IP que fue asignada por la terminal corresponda con la asignada manualmente, para el caso de esta maquina virtual de Kali Linux, la IP es la 192.168.1.11

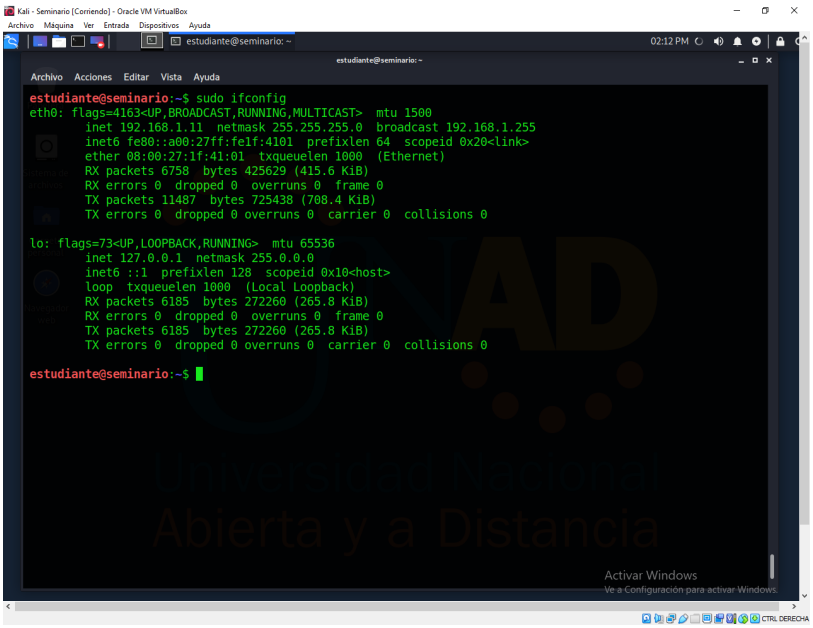

Ilustración 2 Configuracion de la direccion IP en Kali Linux

Ahora nos enfocaremos en la maquina de Windows 7 x64, aquí debemos realizar una continuación del adaptador de red para que de manera fija tome una dirección IP del segmento de la configuración del NAT local (Que es 192.168.1.0/24), en este caso esto se hace por la interfaz grafica, se asigna una dirección IP del segmento y luego se ejecuta el comando ipconfig para poder identificar cual es la dirección IP que fue asignada por la terminal corresponda con la asignada manualmente, para el caso de esta maquina virtual de Windows 7 x64, la IP es la 192.168.1.10

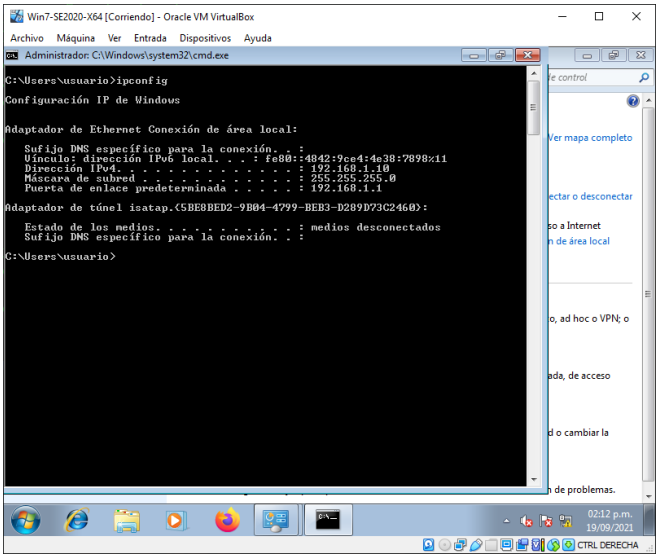

Ilustración 3 Configuracion de la direccion IP en Windows 7 x64

El siguiente paso que debemos realizar, es un proceso de escaneo de toda la red de área local (LAN), este paso hace parte del proceso de exploración de las etapas para realizar un pentesting, para esta etapa, deberemos ejecutar el comando nmap con los parámetros -sn y la dirección IP del host de destino, en este caso, queremos ejecutarlo a todo el segmento de direcciones IP de la NAT creada en VirtualBox en el paso numero 1, para esto, ejecutamos el comando con la IP 192.168.1.0/24

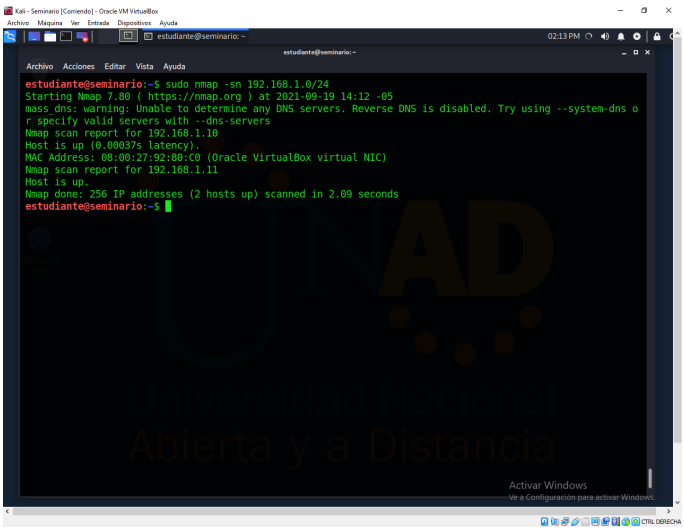

Ilustración 4 Comando NMAP a la red local

Podemos observar que se listan los dos nodos que están configurados correctamente en la red, la dirección 192.168.1.10 (El propio Kali Linux) y la 192.168.1.11 (El servidor Windows. 7)

Para ejecutar el siguiente paso, tenemos un pre-requisito que validar, debemos ir a nuestra maquina que va a ejecutar el rol de destino, y validar que tenga los sistemas perimetrales desactivados (Firewall abajo), para esto, entramos en la maquina de Windows 7 x64 y vamos a la configuración, luego vamos a firewall y validamos que la configuración este como se muestra en la siguiente imagen (Con el sistema perimetral desactivado):

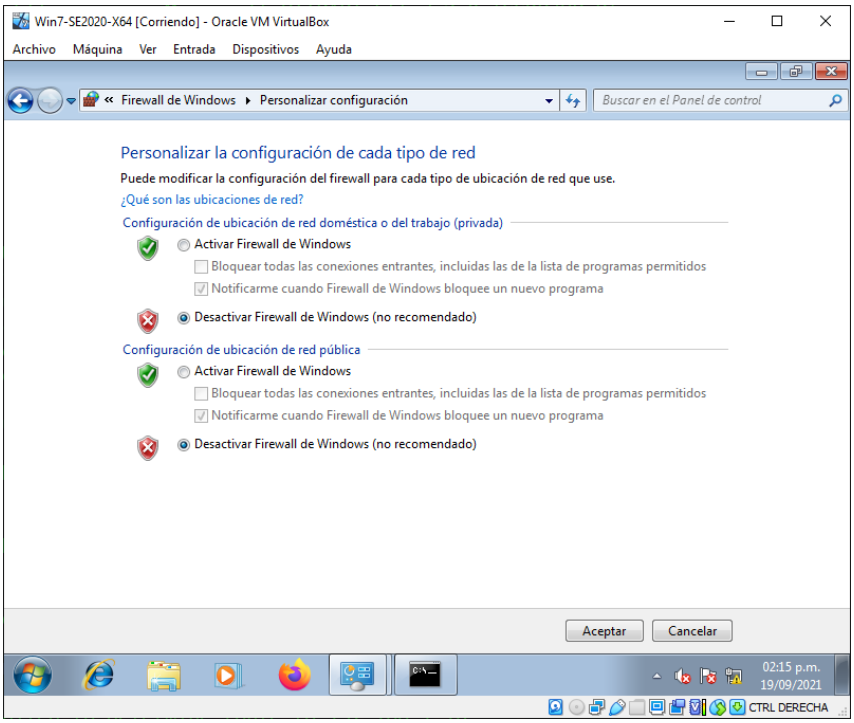

Ilustración 5 Configuracion del firewall de windows 7 x64 desactivado

Nota: Este es un pre-requisito para realizar el escaneo completo de los puertos del sistema operativo

Este paso es muy importante dentro del proceso que se va a realizar, aquí es donde podemos validar cuales son los puertos que tiene disponible el sistema operativo destino de Windows 7 x64 para realizar ataques a través de herramientas de Sploits (Que veremos en los siguientes puntos), para esto debemos hacer uso del comando de NMAP, este comando lo utilizamos en puntos anteriores pero esta vez no lo aplicaremos a todo el segmento de la red, sino que lo aplicaremos directamente a la IP del host destino que en nuestro caso es el sistema Windows 7 x64 a travez del comando sudo nmap -A 192.168.1.10:

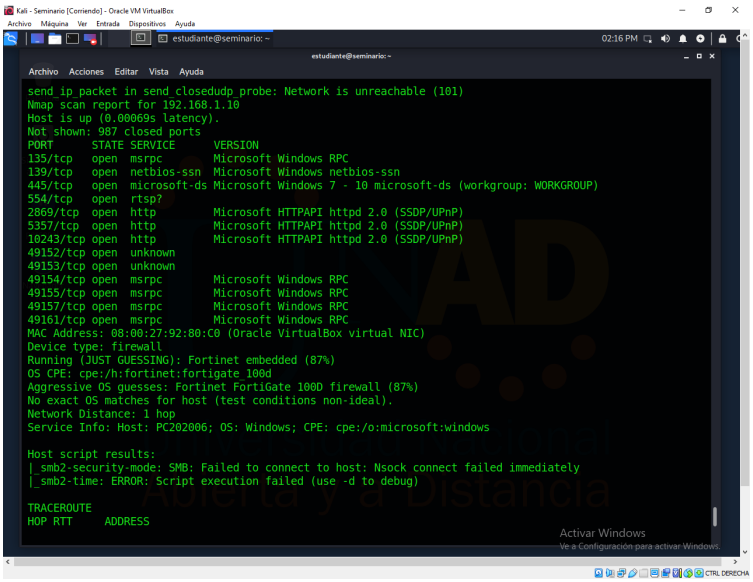

Ilustración 6 Ejecucion de escaneo de puertos para equipo Windows 7 x64

Este comando nos mostrara un listado con todos los puertos, el protocolo (tcp o udp), que servicio esta asociado a este puerto y cual es la versión que se esta ejecutando.

Para la ejecución de este siguiente punto, entramos a una nueva etapa del proceso de vulnerabilidades, estamos ahora en la fase de explotación de las vulnerabilidades, para esto, una de las herramientas mas útiles dentro de el sistema

operativo Kali Linux se llama Metasploit, esta herramienta se lanza con una instrucción de comando desde la terminal, y muestra una pestaña como la siguiente, aquí ya podemos hacer uso de las bases de datos de los sploits disponibles en la comunidad, esta base de datos es muy grande, por lo tanto esta herramienta es muy útil y muy conocida en el mundo del pentesting.

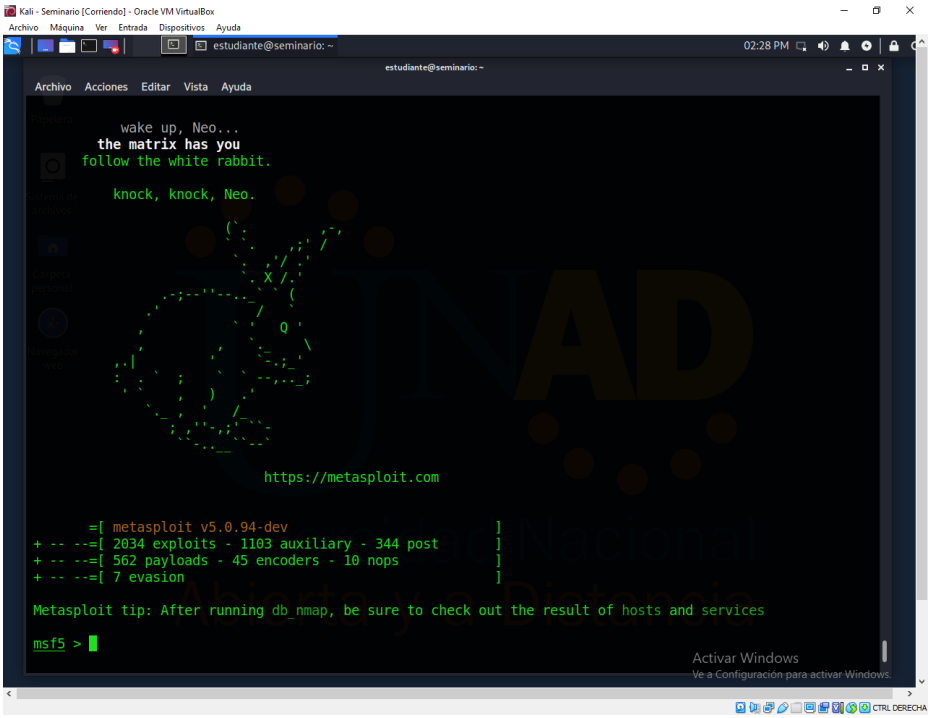

Ilustración 7 Herramienta metrasploit lanzamiento

Ahora debemos hacer uso de la herramienta rejetto dentro del Kali Linux en la herramienta de metasploit, esto nos permite abrir una ventana de comandos especial donde podemos realizar las configuraciones requeridas para la herramienta de rejetto y el host que queremos atacar.

Una posibilidad que tenemos en caso de no conocer todas las posibles configuraciones que debemos realizar en la herramienta, es utilizar la bandera de options, esta bandera nos listara todas las posibles propiedades que tiene la herramienta de rejetto disponibles para que nosotros utilicemos, esta información esta dividida en el nombre de la opción, el valor que actualmente tiene configurada,

si es una variable requerida o es una variable de carácter opcional, y una detallada descripción de que hace cada configuración.

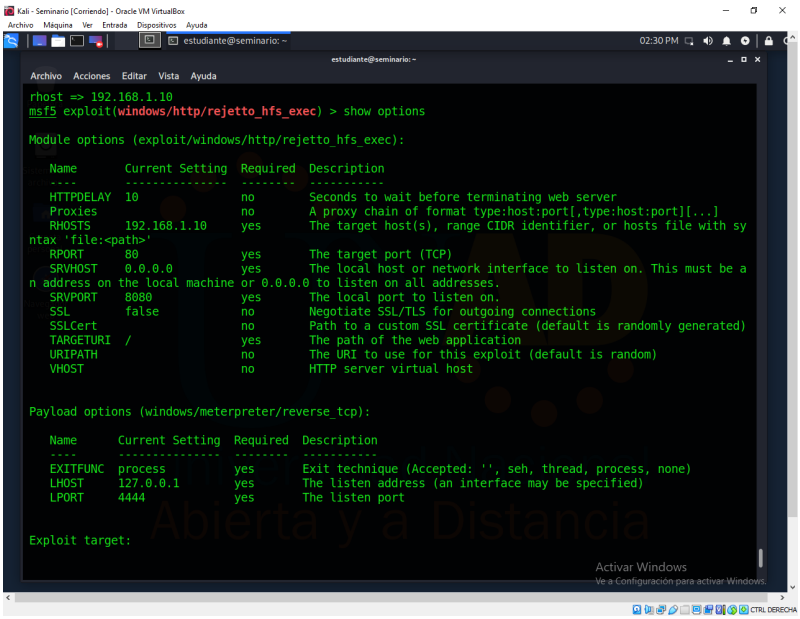

Ilustración 8 Rejetto listado de opciones

El paso siguiente es la configuración de la herramienta de rejetto, para esto se utilizaron dos parámetros, el primero es el payload que es el tipo de prueba que se va a realizar, en este caso, se va a utilizar una prueba llamada reverse_tcp, para esto debemos ejecutar el comando set payload Windows/meterpreter/reverse_tcp, la respuesta de este comando debe ser exitosa

El segundo paso es la configuración del host destino, para esto se debe utilizar la dirección IP del host que vamos a acceder, en nuestro caso es la 192.168.1.10, y debemos realizarlo mendiante el comando set rhost 192.168.1.10, se debe esperar una respuesta positiva en la interfaz.

Una vez esta configurado el sploit de rejetto, se debe proceder con la ejecución, para esto se pueden utilizar dos comandos, el primero puede ser run o el otro puede ser explot.

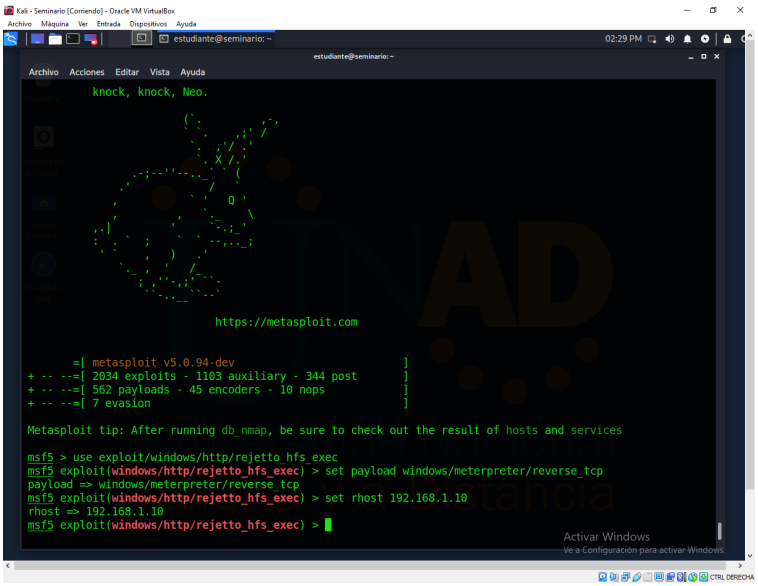

Ilustración 9 Configuracion de rejetto

Se instala la aplicación de HFS en el sistema Windows 7 x64 para realizar la prueba de transferencia de archivos de forma remota desde el sistema Kali Linux al sistema operativo Windows 7 x64:

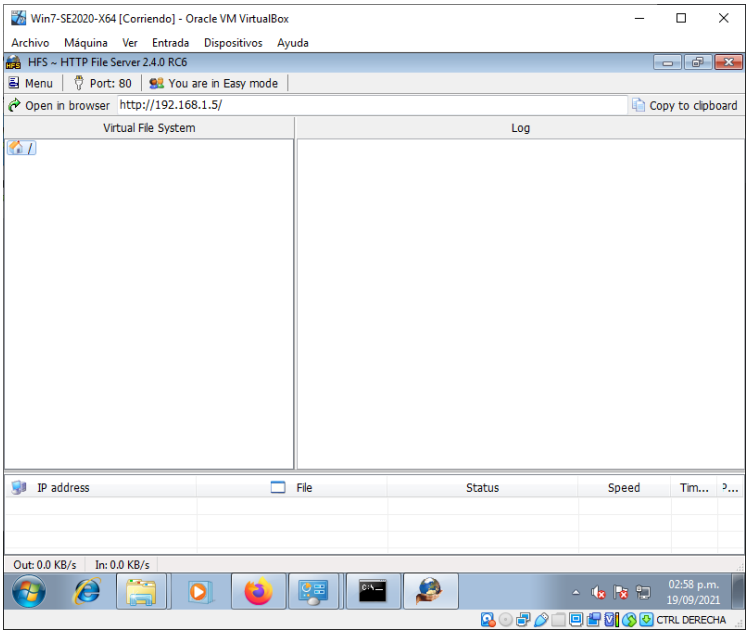

Ilustración 10 Herramienta HFS en Windows 7 x64

5.3 DESARROLLO OBJETIVO ESPECÍFICO 3

Presentar las herramientas utilizadas durante el proceso de pentesting

Metasploit

Es una herramienta que se utiliza para desarrollar nuestros propios sploits o ejecutar sploits propios o existentes en equipos remotos diferentes al nuestro, pueden estar en nuestra red o en redes externas también, es un software muy útil para realizar auditorias de seguridad, probar los sploits y desarrollar nuestros propios sploits.

Nmap

Esta es una herramienta muy importante para las primeras fases de la ejecución de pruebas de vulnerabilidades en los sistemas de información, es muy útil para realizar un mapeo de los ítems de red que están habilitados en la red, con esta herramienta se pueden realizar escaneos de puertos a una dirección ip especifica, o se puede correr sobre toda la red de datos y validar cuantos servidores hay disponibles y sobre estos, que puertos están habilitados, esta herramienta también informa si hay vulnerabilidades conocidas sobre estos puertos.

OpenVas

Es un software que se utiliza para escanear vulnerabilidades, con esta herramienta, se pueden encontrar diferentes tipos de problemas en una red de datos, se pueden encontrar tanto fallas de bajo impacto, medio como de alto impacto, esta empresa alimenta diariamente la base de datos de vulnerabilidades, convirtiendo esta herramienta en una de las mas completas, tiene una interfaz grafica para que el hecho de usarla y realizar con esta herramienta el escaneo, se convierta en una actividad mas fácil visualmente y cómoda para los usuarios finales que la usamos.

ExploitDB

Esta es una herramienta web que consta de una base de datos o directorio web donde muchas personas en todo el mundo publican vulnerabilidades, esta base de datos, a diferencia de la herramienta anterior, es alimentada diariamente pero no por una empresa privada sino por la comunidad, cualquiera puede reportar en esta base de datos una vulnerabilidad conocida a un software de información o aun sistema operativo.

CVE

Las vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures CVE) es una lista de vulnerabilidades de seguridad que son conocidas y que han sido reportadas en este sitio web, con una información detallada como la descripción de la vulnerabilidad, versiones de software que fueron afectadas, posible solución al fallo (En caso de que exista) o como de manera provisional, se puede configurar una forma de evitar que esta vulnerabilidad sea explotada en nuestras versiones de producto.

5.4 DESARROLLO OBJETIVO ESPECÍFICO 4

Realizar recomendaciones desde la perspectiva de los equipos Rojo y Azul (RedTeam y BlueTeam)

Una vez realizado todo el proceso de análisis en los servidores de la empresa WhiteHouse Security, como ingenieros de ciberseguridad realizamos algunas recomendaciones para que estas sean implementadas en el interior de la compañía, esto para fortalecer sus sistemas de seguridad internos y externos, garantizando asi que futuros ataques puedan ser identificados a tiempo o poniendo barreras para que, de forma preventiva, bloqueen cualquier tipo de ataque que pueda provenir del

exterior, incluso desde el interior de la misma compañía, estas son recomendaciones que se emiten con base a las evidencias recolectadas a lo largo del análisis, con base a nuestra experiencia y a las normativas vigentes en Colombia:

- Conformar al interior de la empresa, un equipo de seguridad informática donde puedan realizar las actividades que realizaría un equipo RedTeam y BlueTeam, ejecutando este tipo de actividades al menos dos veces al año, garantizando que los equipos están preparados y que estos cuentan con todos los equipos y con el conocimiento suficiente para enfrentarse a situaciones de seguridad.
- Realizar actualizaciones semestrales de las normatividades vigentes en el territorio nacional, buscando de manera activa cualquier cambio en la norma, nuevos requisitos sobre la protección de datos personales, nuevas leyes sobre los delitos informáticos y aplicar ese conocimiento nuevo sobre los equipos de seguridad informática, fortaleciendo así día con día el equipo ante posibles amenazas externas.
- Como ingenieros de sistemas, debemos dar total cumplimiento a el código de ética y de buena conducta para ingenieros establecida en el COPNIA
- Implementar las medidas de seguridad (proceso de hardenizacion) sobre los sistemas operativos, aplicaciones (Como Apache, Ngnix, Oracle, PostgreSQL, etc) antes de ponerlos productivos, o si algún servidor ya esta productivo sin haberle realizado este procedimiento, realizarlo con alta prioridad, bloqueando puertos, activando firewalls, y configurando los tiempos de respuesta de la forma mas optima posible
- Realizar pruebas de penetración de caja blanca y de caja negra en la red de la empresa al menos dos veces por año, esto para garantizar que una persona externa a la compañía pueda encontrar puntos de acceso que no se tenían contemplados por el equipo de seguridad.

5.5 DESARROLLO OBJETIVO ESPECÍFICO 5

Realizar video de sustentación del trabajo en plataforma digital

https://youtu.be/mjeids9786c

6 CONCLUSIONES

Una vez finalizado el proceso de validación de seguridad de la empresa de WhiteHouse Security se puede concluir que la empresa debe aplicar las recomendaciones de seguridad que se presentaran en el siguiente punto, esto por que se evidencia carencias en la implementación de las buenas practicas de seguridad, no se evidencian sistemas perimetrales como lo son los firewall configurados de forma apropiada, no se evidencian sistemas antivirus configurados en los servidores que contienen información critica para la organización y tampoco se evidencia dentro del área de seguridad de la compañía una implementación de los equipos rojos y equipos azules (RedTeams y BlueTeams), se concluye que la empresa tiene falencia en los procesos de contención de las vulnerabildiades que puedan ser encontradas, por tal motivo se concluye que ellos deben realizar una correcta segmentación de la red para tener una contención mayor en caso de vulnerabilidades reportadas.

7 RECOMENDACIONES

- Conformar al interior de la empresa, un equipo de seguridad informática donde puedan realizar las actividades que realizaría un equipo RedTeam y BlueTeam, ejecutando este tipo de actividades al menos dos veces al año, garantizando que los equipos están preparados y que estos cuentan con todos los equipos y con el conocimiento suficiente para enfrentarse a situaciones de seguridad.
- Realizar actualizaciones semestrales de las normatividades vigentes en el territorio nacional, buscando de manera activa cualquier cambio en la norma, nuevos requisitos sobre la protección de datos personales, nuevas leyes sobre los delitos informáticos y aplicar ese conocimiento nuevo sobre los equipos de seguridad informática, fortaleciendo así día con día el equipo ante posibles amenazas externas.
- Como ingenieros de sistemas, debemos dar total cumplimiento a el código de ética y de buena conducta para ingenieros establecida en el COPNIA
- Implementar las medidas de seguridad (proceso de hardenizacion) sobre los sistemas operativos, aplicaciones (Como Apache, Ngnix, Oracle, PostgreSQL, etc) antes de ponerlos productivos, o si algún servidor ya esta productivo sin haberle realizado este procedimiento, realizarlo con alta prioridad, bloqueando puertos, activando firewalls, y configurando los tiempos de respuesta de la forma mas optima posible
- Realizar pruebas de penetración de caja blanca y de caja negra en la red de la empresa al menos dos veces por año, esto para garantizar que una persona externa a la compañía pueda encontrar puntos de acceso que no se tenían contemplados por el equipo de seguridad.

BIBLIOGRAFÍA

¿Que es la ciberseguridad? [Consultado el 09 de octubre 2021] Disponible en URL: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kali Linux [Consultado el 09 de octubre 2021] Disponible en URL: https://es.wikipedia.org/wiki/Kali_Linux

¿Que es RedTeam en ciberseguridad? [Consultado el 09 de octubre 2021] Disponible en URL: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

Cybersecurity Red Team Versus Blue Team — Main Differences Explained [Consultado el 09 de octubre de 2021] Disponible en URL: https://securitytrails.com/blog/cybersecurity-red-blue-team

¿Que es VirtualBox y para que sirve? [Consultado el 09 de octubre 2021] Disponible en URL: https://www.msn.com/es-es/noticias/tecnologia/qué-es-virtualbox-y-para-qué-sirve/ar-BB1f4nku

What is a firewall? Firewalls explained and why you need one [Consultado el 09 de octubre 2021] Disponible en URL: https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html

Exploits: What You Need to Know [Consultado el 09 de octubre 2021] Disponible en URL: https://www.avast.com/c-exploits

¿Que es un ataque DDoS? [Consultado el 09 de octubre 2021] Disponible URL: https://www.cisco.com/c/es_es/products/security/what-is-a-ddos-attack.html

¿Que es una red DMZ? [Consultado el 09 de octubre 2021] Disponible URL: https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz

What is DNS? How DNS works [Consultado el 09 de octubre 2021] Disponible URL: https://www.cloudflare.com/es-es/learning/dns/what-is-dns/

Integridad de la informacion [Consultado el 09 de octubre 2021] Disponible URL: https://marinajesusseguridadinformacion.wordpress.com/2018/05/14/integridad-de-la-informacion/

¿Que es el pentesting? [Consultado el 09 de octubre 2021] Disponible URL: https://openwebinars.net/blog/que-es-el-pentesting/

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. [Consultado el 09 de octubre 2021] Disponible en URL: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Por la cual se dictan disposiciones generales para la protección de datos personales. [Consultado el 09 de octubre 2021] Disponible en URL: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Decreto 1377 de 2013 [Consultado el 09 de octubre de 2021] Disponible en URL: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646