Capacidades técnicas. legales y de gestión para equipos Blue Team y Red Team

Wilman Alfonso Albarracin Ramírez

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2025

Resumen

La implementación de equipos Red Team y Blue Team en las empresas se convierte en un acierto para combatir las posibles vulnerabilidades que se presenten desde el exterior a los activos de información que pueden ser objeto de ataques por parte de la ciberdelincuencia, el conocimiento de estos equipos permiten consolidar un línea de defensa para la detección de intrusos, cerrar vulnerabilidades y mitigar los posibles ataques que se puedan presentar por medio de la explotación de vulnerabilidades ya evidenciadas en prueba de penetración y contención de los mismos.

A través de este informe técnico se pretende tener una visión de los aspectos legales que regulan los delitos informáticos, seguridad de la información, protección de datos que garantizan la confidencialidad de la información, comprender los alcances de los equipos de Red Team y Blue Team relacionadas con su capacidad de gestión frente a incidentes que se puedan presentar lograr mitigar, contener y asegurar la infraestructura de TI dentro de la empresa empleado estrategias de seguridad que permitan analizar el riego y las vulnerabilidades en la infraestructura TI logrando asegurar el activo más valioso de una empresa, como lo es su información.

Palabras clave: Blue Team, Ciberseguridad, Red Team, Hardening, Vulnerabilidad.

Abstract

The implementation of Red Team and Blue Team equipment in companies becomes a success to combat possible vulnerabilities that arise from the outside to information assets that can be subject to attacks by cybercrime, the knowledge of these equipment allows consolidating a line of defense for the detection of intruders, close vulnerabilities and mitigate possible attacks that may occur through the exploitation of vulnerabilities already evidenced in penetration and containment tests.

Through this technical report, it is intended to have a vision of the legal aspects that regulate computer crimes, information security, data protection that guarantee the confidentiality of information, understand the scope of the Red Team and Blue Team teams related to their management capacity in the face of incidents that may be mitigated, contain and secure the IT infrastructure within the company using security strategies that allow analyzing the risk and vulnerabilities in the IT infrastructure, ensuring the most valuable asset of a company, such as its information.

Keywords: Blue Team, Cybersecurity, Red Team, Hardening, Vulnerability.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Actualización

Evento que permite que el software descargue de la nube información con las ultimas correcciones en materia de seguridad.

Amenaza

Es aquella causa que permite materializar un incidente permitiendo causar daños a los activos de información de la empresa.

Antivirus

Software de seguridad que permite contrarrestar ataques logrando proteger el equipo donde se encuentra instalado eliminando las amenazas que se puedan presentar.

Firewall

Es un sistema de seguridad que puede ser software o hardware que permite administrar el tráfico de red en la empresa logrando mitigar ataques desde conexiones inseguras filtrando tráfico autorizado y no autorizado.

Hardening

Proceso mediante el cual se robustece o endurece la seguridad informática al interior de la empresa logrando con esto mitigar vulnerabilidades que puedan existir.

NMAP

Software de código abierto que permite rastrear puestos abiertos en un quipo o red objetivo logrando con esto recopilar información para posibles ataques de vulnerabilidades.

Payload

Es un sistema modular que permite ejecutar la explotación encontrada logrando aprovechar la vulnerabilidad accediendo al equipo víctima y accediendo a su información.

Introducción

Con el presente trabajo se pretende adquirir y profundizar conocimientos frente a los test de penetración denominados pentesting o Etikal Haking aplicando sus diferentes fases y ejecución de herramientas para lograr minimizar las vulnerabilidades en las organizaciones y permitan establecer una correcta ejecución de los niveles de seguridad informática evitando perdida de información, llevando estas pruebas a la práctica con diferentes pruebas de penetración por medio de escenarios tecnológicos controlados.

Se profundiza frente a las acciones de los equipos Red Team & Blue Team por medio de estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI de acuerdo a los conocimiento adquiridos como equipos Blue Team en la aplicación componente practico para la contención de ataques informáticos, siempre aplicando el marco ético y legales, la normatividad vigente que regula los delitos informáticos, a su vez el código de ética profesional como marco legal en las actuaciones que enaltecen el ejercicio de las funciones de la profesión de ingeniero ya que permite analizar la conduta profesional en sus actuaciones dentro de la legalidad y transparencia.

Finalmente se abordará la importancia de la aplicación de medidas de hardenización que impidan ataques a los activos de información de la empresa mitigando y conteniendo su propagación.

Objetivos

Objetivos General

Elaborar un informe técnico que permita implementar las estrategias propuestas por los equipos Red Team y Blue Team en desarrollo de los escenarios propuestos en la empresa CyberFort Technologies enmarcado dentro de la normatividad legal colombiana de ciberseguridad y delitos informáticos.

Objetivos Específicos

Ejecutar las herramientas de ciberseguridad que permitan ejecutar las fases del pentesting logrando llegar a este informe observando las estrategias que permitan remediar posibles vulnerabilidades en el marco ético y legal.

Formular a través de los equipos Red Team y Blue Team estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

Aplicar medidas de hardenización que minimicen los riesgos de ataque a los activos de información de la empresa o que se repitan este tipo de ataques.

Marco Legal

Actualmente, Colombia tiene regulaciones vigentes sobre delitos informáticos y protección de datos personales, además del código de ética profesional fundamental para la carrera en ingeniería. A continuación, se describirá cada una de estas Leyes.

Ley 842 de 2003

"Por el cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones" (Pública E. F., 2023) con esta ley se buscó la reglamentación del desarrollo de la Ingeniería, A su vez como profesionales estamos sujetos al código de Ética que establece las conductas profesionales que debemos ejercer, por tal razón el Consejo Profesional Nacional de Ingeniería COPNIA plasmo lo contenido en la Ley 842 en su Código de Ética (Copnia, 2015) que permite validar el comportamiento profesional exigible y de cumplimiento obligatorio, al igual este documento nos ilustra frente a los deberes, prohibiciones y sanciones para los ingenieros.

Ley 1273 de 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" (Pública F. , Ley 1273 de 2009, 2009), la finalidad de esta ley es definir de manera clara los delitos informáticos, a fin que se puedan judicializar de manera efectiva por los organismos judiciales dentro de las investigaciones que se realicen cuando se tipifiquen esta clase de delitos contra los sistemas informáticos y la información de los colombianos, dejando clara las penas a las que se ven expuestos los ciberdelincuentes, con la

entrada en vigencia la presente ley el estado colombiano promueve la protección de la infraestructura digital y la seguridad de la información de los ciudadanos. Esta ley fue un gran acierto del estado colombiano ya que permite modificar el código penal dando herramientas al aparato judicial para investigar, sindicar, juzgar y judicializar a los ciberdelincuentes que cometan estos delitos informáticos a través de la tipificación de ellos con penas claras en cada caso que se presente, ya que debido a la acelerada evolución de la tecnología, el gran aumento de los sistemas de información a través de internet, se han expuesto día a día los internautas a la ciberdelincuencia que no descansa para cometer sus delitos informáticos, estos no solo atacan a un ciudadano en común sino que también atacan la infraestructura tecnológica de empresas gubernamentales públicas, la empresa privada, causando grandes pérdidas de información y afectando su economía y llegado el caso afectar la defensa y seguridad del estado.

Ley 599 de 2000

"Por la cual se expide el Código Penal." (Pública F. , Ley 599 de 2000, 2000) sufre una modificación adicionando el Titulo VII BIS "De la protección de la información y de los datos" en esta Ley, una vez promulgada la ley 1273 de 2009 (Pública F. , Ley 1273 de 2009, 2009) que contiene los siguientes Capítulos donde encontramos los diferentes artículos con la definición pena y multa del delito, que modifican y se aplican al Código Penal así:

Capítulo I "De los atentados contra la confidencialidad, la integridad y la disposición de los datos y de los sistemas informáticos que enmarca los siguientes delitos informáticos:

Tabla 1

Delitos Informáticos Ley 1273 de 2009

Articulo	Delito	Pena	Multa
269ª	Acceso abusivo a un sistema informático	Pena de prisión de 48 a 96 meses	De 100 a 1.000 SMLMV
269B	Obstaculización ilegítima de sistema informático o red de telecomunicación	Pena de prisión de 48 a 96 meses	De 100 a 1.000 SMLMV
269C	Interceptación de datos informáticos	Pena de prisión de 36 a 72 meses	No lo Establece
269D	Daño Informático	Pena de prisión de 48 a 96 meses	De 100 a 1.000 SMLMV
269E	Uso de software malicioso	Pena de prisión de 48 a 96 meses	De 100 a 1.000 SMLMV
269F	Violación de datos personales	Pena de prisión de 48 a 96 meses	De 100 a 1.000 SMLMV
269G	Suplantación de sitios web para capturar datos personales	Pena de prisión de 48 a 96 meses*	De 100 a 1.000 SMLMV **
*	La pena señalada se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.		
**	Siempre que la conducta no constituya delito sancionado con pena más grave.		

Nota. Autoría propia.

En relación con el Articulo 269H: Circunstancias de agravación punitiva, se pueden agravar las penas de la mitad a las tres cuartas partes de los artículos antes descritos si la conducta se comete con los siguientes agravantes:

Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

Por servidor público en ejercicio de sus funciones.

Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

Revelando o dando a conocer el contenido de la información en perjuicio de otro.

Obteniendo provecho para sí o para un tercero.

Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

Utilizando como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales. (Pública F. , Ley 1273 de 2009, 2009)

Capítulo II “De los atentados informáticos y otras infracciones que enmarca los siguientes delitos informáticos:

Tabla 2

Delitos Informáticos Capítulo II Ley 1273 de 2009

Articulo	Delito	Pena	Multa
269I	Hurto por medios informáticos y semejantes. conducta señalada en el artículo 239 Código Penal,	Penas señaladas en el artículo 240 Código Penal	
269J	Transferencia no consentida de activos.	Pena de prisión de 48 a 120 meses	Multa de 200 a 1.500 SMLV
Si la conducta tuviere una cuantía superior a 200 SLMV, la sanción se incrementa en la mitad.			

Nota. Autoría propia.

La Ley 1273 de 2009, adiciona al artículo 37 del Código de Procedimiento Penal dando la potestad de conocer de los delitos contenidos en el Titulo VII Bis a los Jueces Penales Municipales y deroga el texto del artículo 195 del código penal relacionado con el Acceso abusivo a un sistema informático. Así las cosas, esta Ley permite al aparato investigativo y judicial proponer una lucha frontal contra la ciberdelincuencia.

Ley 1581 de 2012

"Por la cual se dictan disposiciones generales para la protección de datos personales" (Colombia, 2012) reglamentada parcialmente a través del Decreto 1377 de 2013 emanado por el Presidente de la República, esta Ley tiene como objeto ejercer el derecho constitucional que tiene todo ciudadano a la protección de sus datos personales, conocer, actualizar y modificar la información recaudada en bases de datos o archivos por parte de terceros, salvaguardar la misma y evitar vulneraciones a sus derechos y garantías constitucionales, a su vez regula el derecho constitucional a la información, con su implementación se busca garantizar que el titular de la

información conozca sus derechos, las políticas de tratamiento y las definiciones que se le aplican, las autorizaciones y responsabilidades.

Decreto 338 de 2022

"Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones" (Pública F. , Decreto 338 de 2022, 2022)este decreto permite al País generar líneas de fortalecimiento desde el Gobierno dirigida a las autoridades que hacen parte de la Administración Pública del estado colombiano aplicando los principios de coordinación y colaboración armónica entre las instituciones en materia de seguridad digital, permite validar e identificar infraestructura criticas cibernéticas, servicios esenciales, gestionar riesgos de ciberseguridad y dar respuesta de manera oportuna a los incidentes de seguridad digital que se presenten.

Pruebas de Penetración o Pentesting

¿Vamos a iniciar con la definición de que es Pentesting? es una prueba (testing) de penetración (penetration) que permite detectar posibles fallas o vulnerabilidades de seguridad en un sistema informático, el alcance y las posibles contingencias que permitan mitigarlo, a través de una simulación de un ataque cibernético, ejecutando pruebas controladas que permiten evadir la seguridad aplicada a los sistemas, a fin de auditar la infraestructura de red, los sistemas y las diferentes aplicaciones de software instalados en la organización como resultado de estas pruebas de penetración se pueden tomar medidas que permitan reforzar y mejorando la ciberseguridad, logrando con esto blindar la organización de intrusiones o ataques de los ciberdelincuentes.

Encontramos que el Pentesting se puede clasificar en tres tipos atendiendo la cantidad de información que se tiene sobre la organización o los sistemas informáticos que se pretenda aplicar la prueba de penetración así:

Pentesting de Caja Blanca

Para la ejecución de esta prueba el testeador hace parte de la organización o a través de una fuente interna conoce toda la infraestructura tecnológica frente al software y hardware que se dispone.

Pentesting de Caja Negra

Para la ejecución de esta prueba el testeador hace su análisis partiendo de cero, sin ningún tipo de información de la organización ni de los sistemas a testear.

Pentesting de Caja Gris

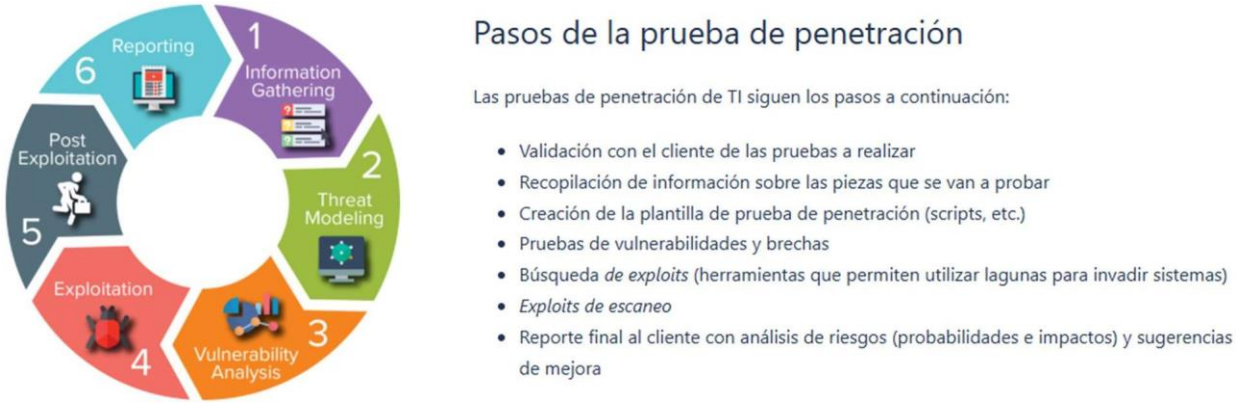
Para la ejecución de esta prueba el testeador conoce apartes de información de la organización, y a su vez desconoce gran parte de su información, este tipo de Pentesting es un hibrido entre el la caja blanca y la caja negra.

Fases del Pentesting

Dando aplicación a las siguientes fases de las pruebas de penetración, permitirá establecer el nivel de vulnerabilidad de la organización y tomar las acciones para remediar posibles ataques informáticos a los sistemas de información:

Figura 1

Prueba de Penetración



Nota. Imagen que representa los pasos de las pruebas de penetración. Tomado de. Cybergo.com. PenTest: Pruebas de penetración.2020. https://cybergo.com.br/pentest-testes-de-penetracao/

Recopilación de Información (Information Gathering)

Esta fase se accede y recolecta la información pública que se puede acceder del objetivo. Se puede aplicar reconocimiento activo, pasivo o ambos.

El Reconocimiento pasivo no permite dejar huella digital al momento de recolectar la información sobre un objetivo. Conocido como **footprinting**, su principal característica es la no interacción del sistema, se utilizan herramientas que permitan recopilar dominios y subdominios, DNS como WHOIS, descubrimiento de tecnologías utilizadas a través de Wappalyzer, BuiltWith, recolección de inteligencia por medio de fuentes abiertas como OSINT, Motores de

Búsqueda Activos (Shodan, Netlas) que nos valida servicios y versiones en ejecución, MetaDatos de archivos en la red (Google Hacking, GooFuzz, FOCA).

El Reconocimiento activo puede dejar huella digital, su interacción es directa con el objetivo que se analiza. Conocido como fingerprinting y, se requiere un permiso para hacer este tipo de análisis, se utilizan las siguientes herramientas que permiten el escaneo de puertos en los dominios relevantes (Nmap o RustScan), búsqueda de directorios y recursos (BurpSuite, OWASP ZAP, Feroxbuster o ffuf)

Modelado de Amenazas (Threat Modeling)

Culminada la fase anterior y recauda toda la información se procede a generar la estrategia que se va aplicar para e modelado de las posibles amenazas comparando la defensa del sistema y lograr definir cada una de las vulnerabilidades detectadas que nos permitirá explotarlas en las siguiente fase.

Analisis de Vulnerabilidades (Vulnerability Analysis)

Como ya se tienen el modelado de amenazas y con el fin de descubrir los activos de la infraestructura, sistemas y aplicaciones versiones y servicios de uso se aplican las siguientes herramientas avanzadas que permiten la identificación de vulnerabilidades como Nmap, Nessus, Acunetix, WPScan o SQLMap

Explotación (Exploitation)

Esta es la fase se ejecutan las vulnerabilidades encontradas en la fase anterior, se definen cuáles son amenazas reales y explotables, para determinar su impacto, su complejidad, su nivel de acceso, la cantidad de datos expuestos, su sensibilidad y su afectación en la disponibilidad, integridad y confiabilidad, en este punto se aplican una metodología como OWASP (Open Web

Aplication Security Project), la cual permite aplicar acciones y buenas prácticas de mitigación para las vulnerabilidades encontradas.

Explotación Posterior (Post Exploitation)

En base a las vulnerabilidades reales y que fueron explotadas y remediadas, se debe persistir en el sistema para volver a acceder al mismo toda vez que se abren nuevos servicios ocultos que también podrían ser explotados, por eso la importancia de continuar con una explotación posterior más a profundidad que nos permita extraer nueva información de posibles vulnerabilidades en busca de soluciones de los fallos de seguridad y lograr mitigarlos.

Reporte (Reporting)

En esta última fase del Pentesting, se centra en generar un informe estructurados que evidencie los fallos de seguridad que se encontraron, las amenazas de ciberseguridad existentes, las soluciones de mitigación y las acciones de mejora en la seguridad de la organización.

Es importante que el informe sea comprensible por parte del personal técnico y no técnico de la empresa en todos sus niveles deben generarse informes técnicos y ejecutivos destinado para la toma de decisiones que permita a la organización tomar las medidas de asegurabilidad de sus sistemas de ciberseguridad.

Herramientas de Ciberseguridad

Las herramientas de ciberseguridad están encaminadas a ejecutar análisis de vulnerabilidades dentro de las más utilizadas se profundizará en:

Metasploit

Esta Herramienta permite realizar pruebas de penetración o hacking ético, es un software de código abierto inicialmente creado en lenguaje Perl y luego traducido a Ruby que le permitió mayor eficiencia por tal razón es la herramienta más popular entre los profesionales de la seguridad informática, cuenta con una colección de más de 1677 exploits (CIBERSEGURIDAD, 2024) que permiten probar las vulnerabilidades de los sistemas informáticos, sus principales funciones se encuentran:

Escanear y recopilar información

Identificar y explorar vulnerabilidades

Escalada de privilegios

Instalar Backdoors

Hacer Fuzzing

Evasión de antivirus

Módulos posteriores a la exploración

Eliminación de rastros

Ingeniería Social

Entre otras.

Busca mejorar la conciencia sobre seguridad y ayuda a los equipos de seguridad en la defensa de las vulnerabilidades.

Cuenta con cuatro interfases disponibles dentro de las cuales se encuentran:

MSFConsole: la más utilizada la cual permite acceder a través de una línea de comando interactiva.

MSFWeb: permite acceder al marco de Metasploit a través de una interfaz basada en navegador.

Armitage: Interfaz gráfica basada en Java colaborativa entre equipos de seguridad donde se comparten host comprometidos.

RPC: permite su manejo mediante programación con servicios de llamada a procedimientos remoto basado en HTTP, puede operar con otros lenguajes como Java, Python y C.

Metasploit cuenta con tres bibliotecas (REX, MSF Core y Base de MSF) que ayudan en la ejecución de los sploits en la interacción de los usuarios sin necesidad de escribir código adicional.

Metasploit Framework para realizar diferentes tareas de escaneo y explotación de objetivos usa un software denominado módulos que se clasifican en cinco módulos principales (CIBERSEGURIDAD, 2024) así:

Cargas útiles: las cargas útiles son códigos de shell que realizan las acciones previstas por el usuario una vez que un exploit ha comprometido un sistema objetivo. Se pueden usar para abrir Meterpreters o comandos de shells. Los Meterpreters son cargas útiles sofisticadas que se utilizan durante un ciberataque para ejecutar código y realizar más tareas exploratorias. (CIBERSEGURIDAD, 2024)

Exploits: ejecuta secuencias de comandos para aprovechar las debilidades del sistema o de la aplicación y obtener acceso a los sistemas de destino. (CIBERSEGURIDAD, 2024)

Publicaciones (módulos posteriores a la explotación): las publicaciones permiten a los usuarios realizar una recopilación de información más profunda e infiltrarse aún más en un sistema de destino después de la explotación. Por ejemplo, las publicaciones se pueden utilizar para realizar la enumeración de servicios. (CIBERSEGURIDAD, 2024)

Codificadores: los codificadores ocultan las cargas útiles en tránsito para garantizar que se entreguen correctamente al sistema de destino y eviten la detección del software antivirus, los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS). (CIBERSEGURIDAD, 2024)

NOP (No Operation): los generadores NOP crean secuencias aleatorias de bytes para evitar los sistemas de detección y prevención de intrusiones. (CIBERSEGURIDAD, 2024)

Auxiliares: los módulos auxiliares incluyen escaneo de vulnerabilidades, escaneo de puertos, fuzzers, sniffers y otras herramientas de explotación. (CIBERSEGURIDAD, 2024)

Encontramos que Metasploit integra otras herramientas de ciberseguridad, como Nmap, Nessus y Nexpose robusteciendo su capacidad.

Dentro de la gran lista de comando utilizados en metasploit vamos a relacionar algunos comandos básicos (school, 2024)

Msfconsole: ejecuta el Metaspoit en la consola de comando

search <name>: Buscar cualquier Herramienta

use <module name> (***Auxiliary, Exploits, Payloads, Posts, Encoders, Nops***): para hacer uso del módulo solicitado.

set <variable> <value>: para conocer las variables requeridas n el modulo

info: desplegara una tabla con los requerimientos obligatorios para ejecutar

show options: para conocer las funciones de una herramienta o exploit

Nmap

Es una herramienta que permite escanear puertos y validación de los equipos disponibles en la red sus sistemas operativos, los servicios se encuentran activos, los paquetes que se envían en la red, adicionalmente permiten ejecutar script para detectar vulnerabilidades, es un software de código abierto para exploración de red, inventarios de equipos, planificación de actualizaciones, monitoreo del tiempo de los servicios activos que finalmente permiten aplicar una auditoría de seguridad.

Genera un listado de objetivos analizados que permite recibir gran información detallada frente a cada uno de los equipos escaneados en la red que incluye los puertos, protocolos, servicios, versión de la aplicación, DNS, sistemas operativos, tipo de dispositivos y direcciones MAC.

Su comando de ejecución es nmap con la siguiente sintaxis:

nmap [<Tipo de sondeo> ...] [<Opciones>] { <especificación de objetivo> }

Cuando se ejecuta solo el comando nmap sin parámetros genera el resumen de opciones o una ayuda que nos permite validar y conocer la parametrización para ejecutar este programa o abriendo el siguiente link https://nmap.org/data/nmap.usage.txt para que nos muestre la última versión (NMAP.ORG, Guía de referencia de Nmap, 2024)

En la documentación consultada nos presentan los siguientes ejemplos del uso de la herramienta (NMAP.ORG, Ejemplos, 2024)

nmap -v scanme.nmap.org Esta opción sondea todos los puertos TCP reservados en el servidor scanme.nmap.org. La opción -v activa el modo detallado (también llamado verboso). (NMAP.ORG, Ejemplos, 2024)

nmap -sS -O scanme.nmap.org/24 Lanza un sondeo de tipo SYN sigiloso contra cada una de las 255 máquinas en la “clase C” de la red donde está el sistema "analizame". También intenta determinar cuál es el sistema operativo que se ejecuta en cada máquina que esté encendida. Esto requiere permisos de root por la opción de sondeo SYN y por la de detección de sistema operativo. (NMAP.ORG, Ejemplos, 2024)

nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127

Lanza una enumeración de equipos y un sondeo TCP a cada uno de la primera mitad de las 255 posibles subredes de 8 bit en la red de clase B 198.116. Esto probará si los sistemas están ejecutando sshd, DNS, pop3d, imapd o tienen un servidor en el puerto 4564. Para cualquier puerto que se encuentre abierto, se realizará una detección de versión para determinar qué aplicación se está ejecutando. (NMAP.ORG, Ejemplos, 2024)

nmap -v -iR 100000 -P0 -p 80

Solicita a Nmap que elija 100.000 sistemas aleatoriamente y los sondee buscando servidores web (puerto 80). La enumeración de sistemas se deshabilita con -P0 ya que es un desperdicio enviar un par de pruebas para determinar si el sistema debe ser analizado cuando de todas maneras sólo se va a analizar un puerto. (NMAP.ORG, Ejemplos, 2024)

nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20

Esto sondea 4096 IPs para buscar cualquier servidor web (sin enviar sondas ICMP) y guarda la salida en formato para grep y en XML. (NMAP.ORG, Ejemplos, 2024)

OpenVas

OpenVAS (Open Vulnerability Assessment Scanner, originalmente conocido como GNessUs) es el componente de escaneo de Greenbone Vulnerability Management (GVM), un

marco de software de varios servicios y herramientas que ofrecen escaneo y gestión de vulnerabilidades informáticas. (WIKIPEDIA.ORG, 2024)

Es un software libre con licencia GNU (GLP) Los complementos para Greenbone Vulnerability Management escritos en Nessus Attack Scripting Language, NASL. Presenta una actualización continua no inferior a 24 horas es la herramienta principal de OSSIM. (WIKIPEDIA.ORG, 2024)

Esta herramienta de escaneo de vulnerabilidades presenta las siguientes funciones

Pruebas autenticadas.

Pruebas no autenticadas.

Cuenta con protocolos industriales y de Internet de alto y bajo nivel.

Ajustes personalizados de rendimiento para exploraciones a gran escala.

Desarrollado en un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad.

Dentro de su característica principal encontramos que ofrece explotación de vulnerabilidades y su gestión por medio de los servicios y utilidades en su gran documentación, ejecución desde líneas de comandos o en modo grafico con una interfaz muy completa que permite la generación de informes de interés y sin dejar a un lado que a través de su comunidad presta apoyo en el momento de explotar vulnerabilidades en su web o en los foros como Reddit.

ExploitDB

Esta aplicación web denominada ExploitDB es un proyecto sin ánimo de lucro que fue desarrollado por la compañía Offensive Security, que también es la creadora del sistema operativo Kali Linux. (School, 2024)

Encontramos que es una aplicación web que consolidad bases de datos públicas con ayuda de los usuarios con exploits para vulnerabilidades conocidas, los cuales son utilizador por los pentester de todo el mundo gratuitamente logrando con esto que las auditorias de ciberseguridad se realicen de mayor calidad toda vez que estas consultas son fuentes adicionales de consulta de la existencia de exploits para las vulnerabilidades de los sistemas.

CVE

El fin del Programa CVE es identificar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas públicamente. Generando un registro CVE para cada una de ellas y son cargadas en el catálogo. Cada vez que las vulnerabilidades son descubiertas, se asignan y publican por organizaciones a nivel mundial para que todos los puedan ver, los socios del programa CVE publican registros CVE para comunicar descripciones coherentes de las vulnerabilidades. Los profesionales T.I. y la ciberseguridad utilizan los registros CVE para asegurarse de que están hablando del mismo problema y para aunar sus esfuerzos en priorizar y abordar las vulnerabilidades. (CVE.ORG, 2024)

Instalación Banco de Trabajo

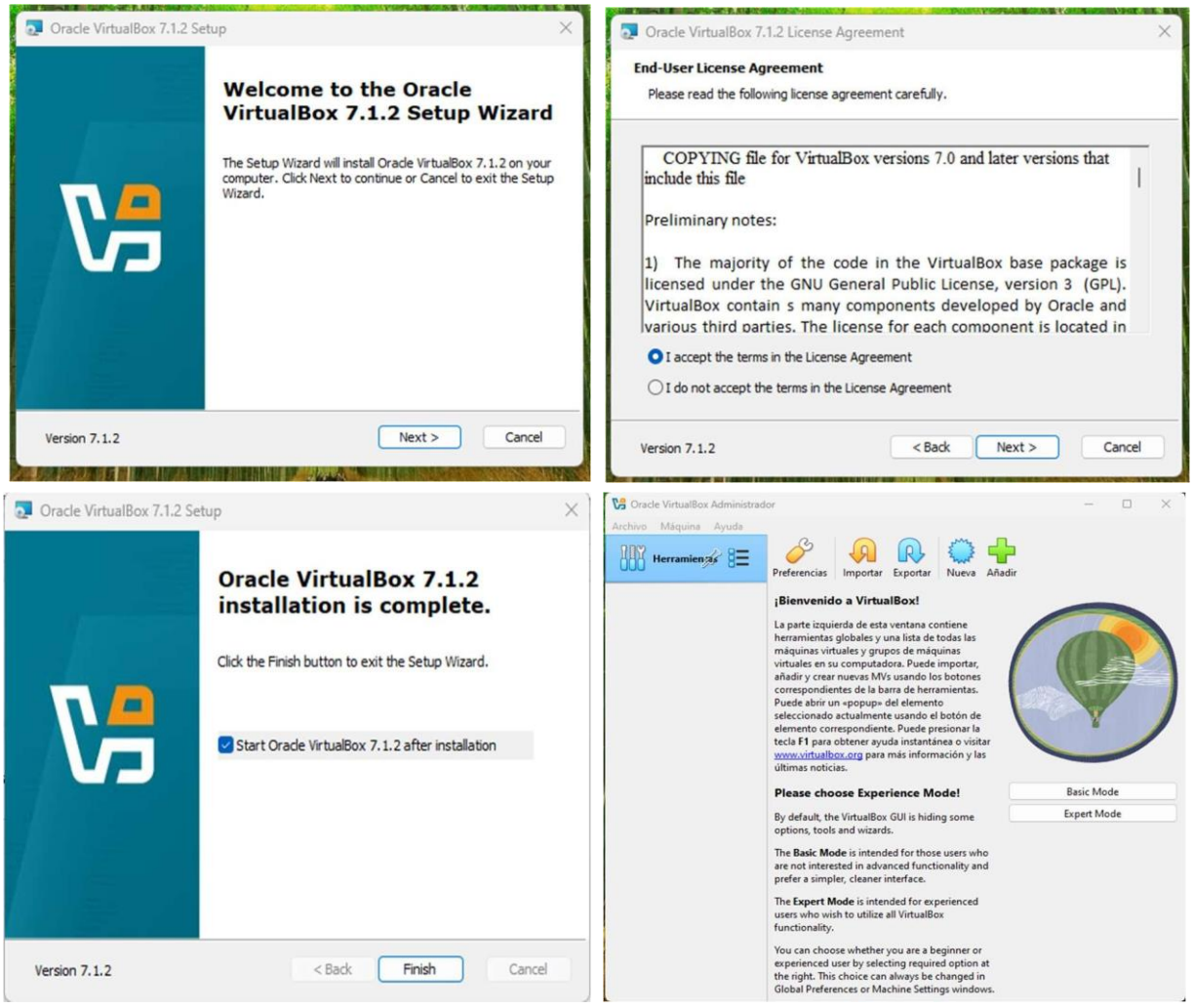
Atendiendo las indicaciones del tutor y en desarrollo de la guía de actividades se procede hacer la el respectivo en los siguientes términos:

Instalación VirtualBox (Máquina Virtual)

Paso A: Descargar VirtualBox desde la página oficial Downloads – Oracle VirtualBox una vez finalizada la descarga se procede con su instalación.

Figura 2

Proceso de Instalación VirtualBox (Maquina Virtual)



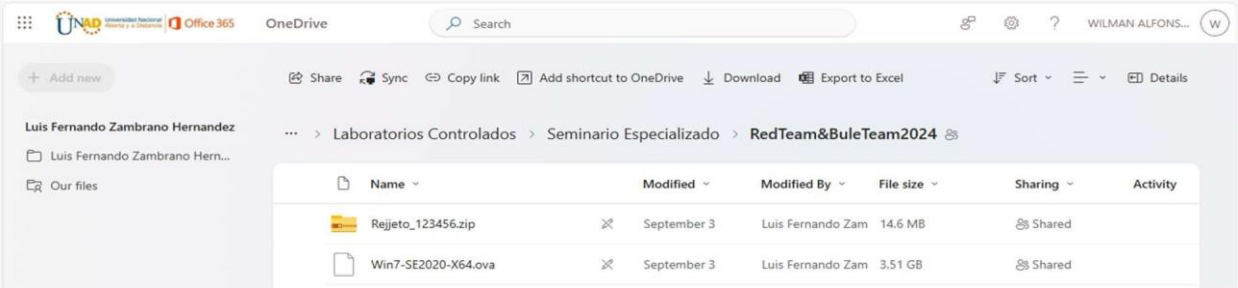
Nota. Representación paso a paso del proceso de instalación Máquina Virtual.

Paso B: Se hace la descarga de los archivos compartido a través del enlace de descarga suministrado en el Foro para el desarrollo de la actividad en el enlace

https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/luis_zambrano_unad_edu_co/EkdfOBYMt0tDh-vNUeGND5QBlfEmt6nCQG0fsWnuXr8E9Q?e=cN102a

Figura 3

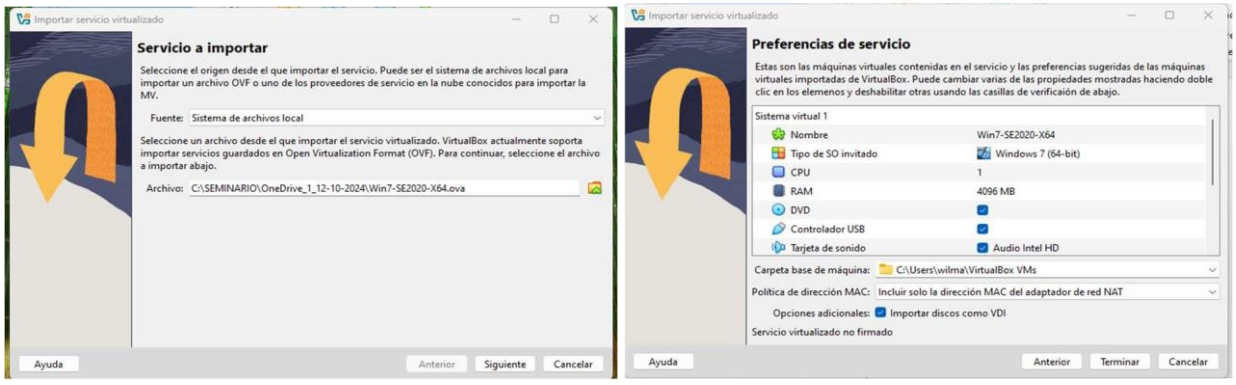
Ilustración Carpeta Compartida Laboratorio Seminario Especializado



Nota. Recurso compartido archivos para el laboratorio RedTeams&BlueTeams 2024.

Figura 4

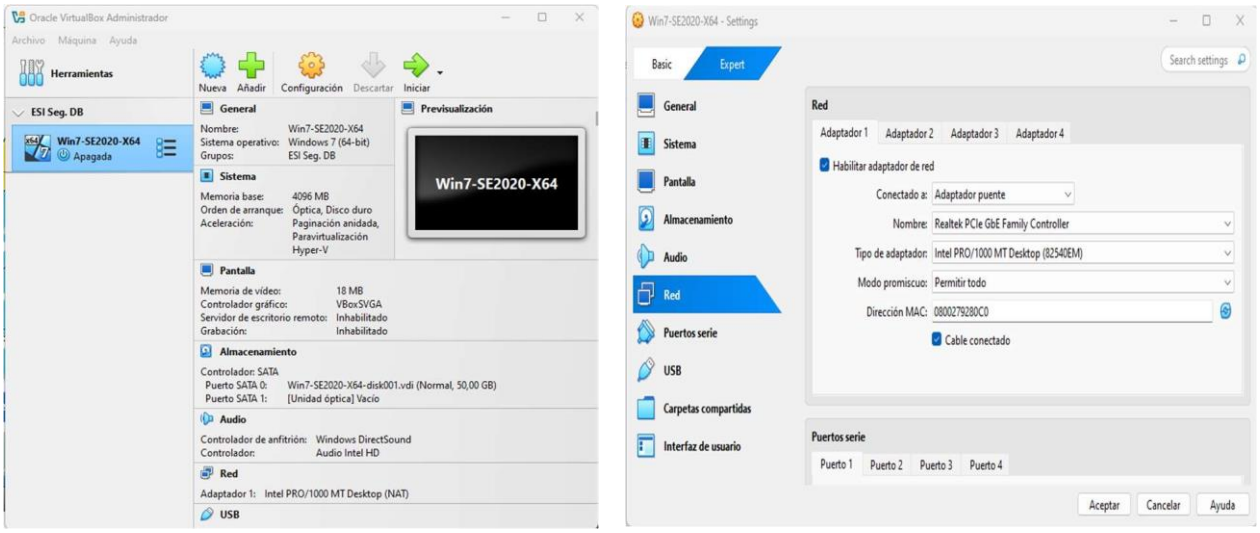
Cargue Imagen SO Win7 al VirtualBox



Nota. Se procede con la importación de sistema operativo Windows 7 en el VirtualBox.

Figura 5

Cambio Tipo Adaptador en la Virtualbox



Nota. Se cambia el tipo de adaptador de red por adaptador de puente que nos permite lograr la conexión entre las maquinas.

Instalación Kali Linux

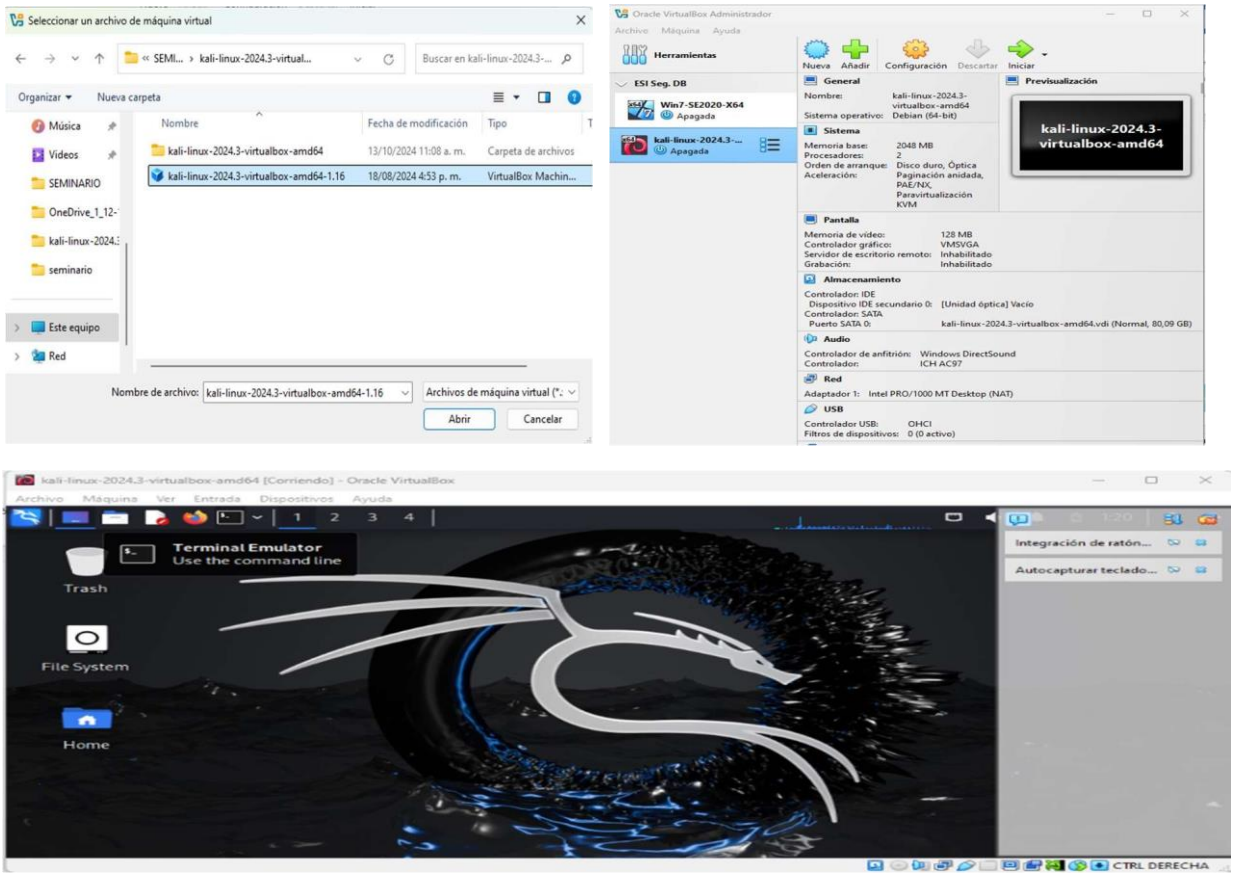
Figura 6

Descarga Kali Linux

Nota. Se procede a realizar la descarga de la página oficial en la siguiente url https://www.kali.org/get-kali/#kali-virtual-machines .

Figura *7*

Descarga Kali Linux



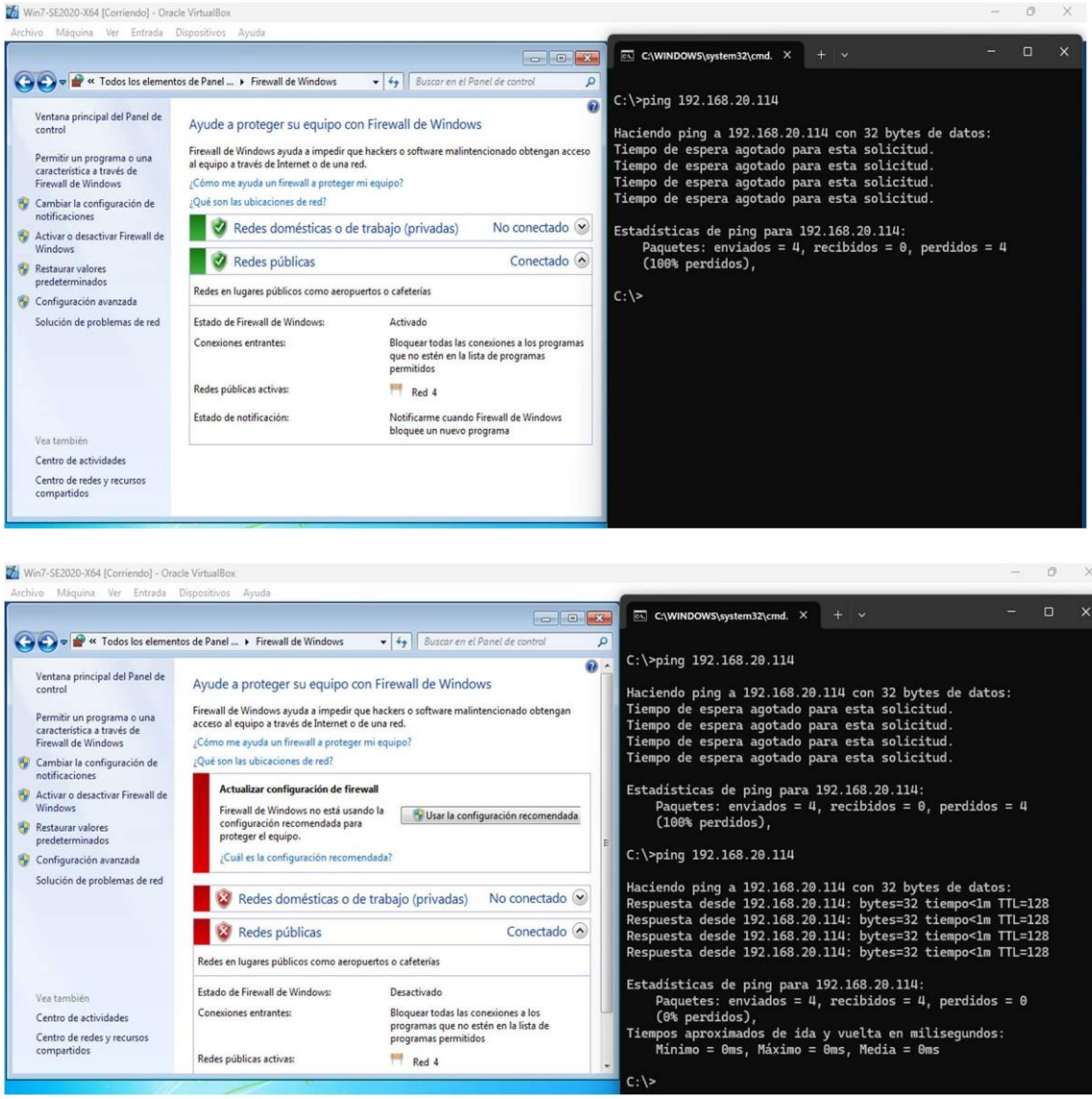
Nota. Se descargada la imagen de Kali Linux se procede con la instalación en VirtualBox

Paso C: se procede con la validación de la conectividad en los sistemas operativos instalados que hacen parte del banco de trabajo

Inicio con el encendido de la máquina virtual con win 7 para ejecutar la prueba de conectividad desde la maquina host hacia el Win 7, obteniendo como resultado pérdida total de los paquetes debido a que se encuentra habilitado el firewall de Windows que impide la conexión.

Figura 8

Validación Negativa Conectividad Entre Equipos Host Win 7

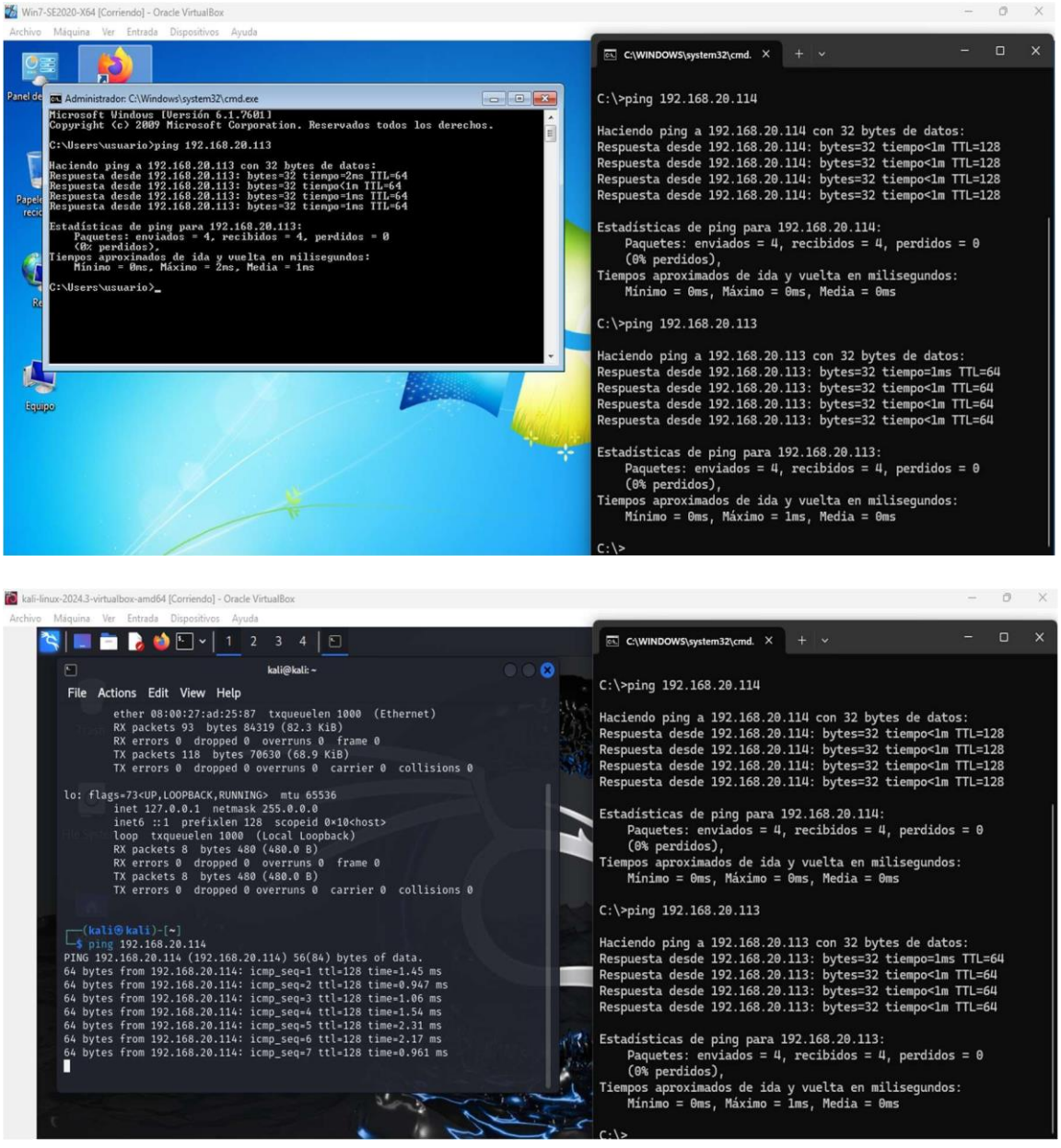


Nota. Se deshabita el Firewall de Windows nuevamente se ejecuta el comando ping logrando establecer la conexión con el host y el sistema operativo Windows 7.

Ahora se procede al encendido de la máquina virtual Kali Linux

Figura 9

Validación Positiva Conectividad Entre Equipos Host Win 7 y Kali Linux



Nota. Dando como resultado positivo de conectividad entre el host y las máquinas virtuales.

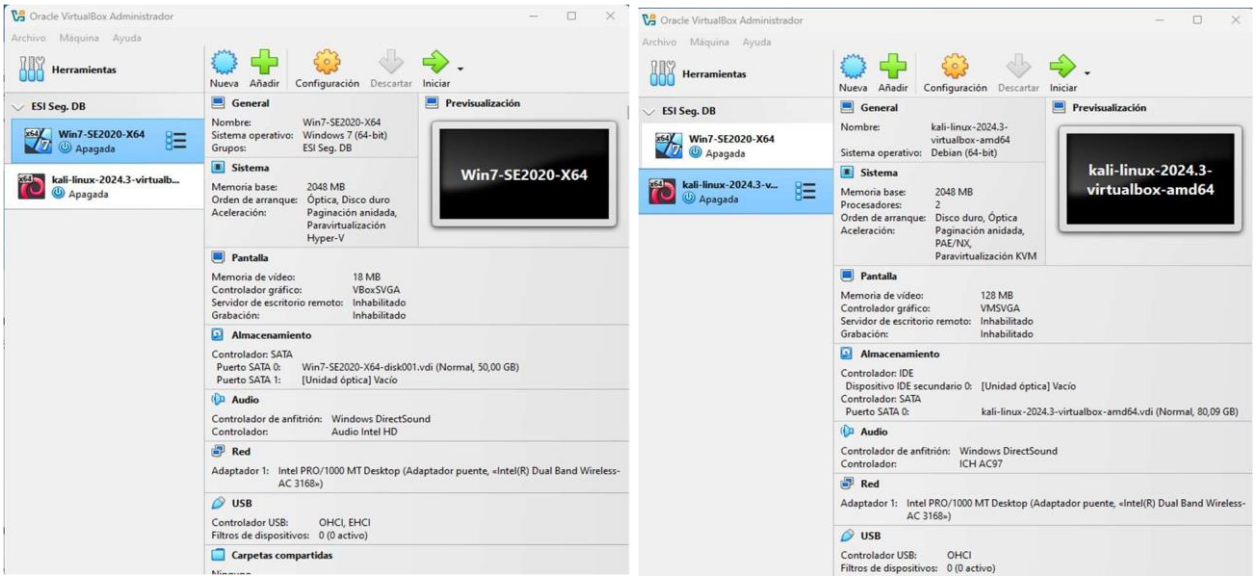
Se valida conectividad entre el Win 7 IP 192.168.20.114 con Kali Linux IP 192.168.20.113 y desde el equipo Host hacia las dos máquinas virtuales. hacemos lo mismo

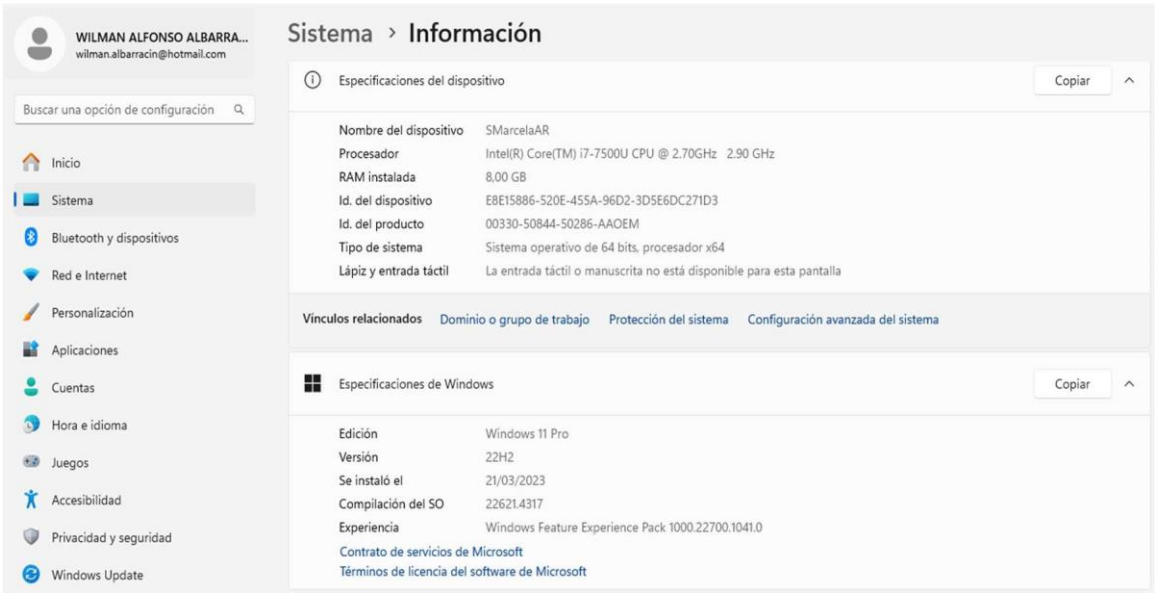
desde la máquina de Kali Linux IP 192.168.20.113 hacia la maquina Win7 IP 192.168.20.114 y desde el equipo Host hacia las dos máquinas virtuales.

Paso D: Se capturan los printscreen del montaje realizado y las características de Hardware de las máquinas virtuales

Figura 10

Pantallazos Montajes Máquinas virtuales Win 7 y Kali Linux





Nota. Se observa la configuración y características de Hardware instado máquinas virtuales.

Análisis Legal y Ético Empresa CyberFort Technologieses

Frente a la primera pregunta ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo?, se puede evidenciar efectivamente que en el análisis legal la organización CyberFort Technologieses, en razón a su gran experiencia en asesoría en Ciberseguridad y Ciberdefensa requiere de un equipo Red Team y Blue Team para aumentar los niveles y protocolos de seguridad internamente

En relación con el contrato elaborado por el abogado presenta varias inconsistencias las cuales podrían traer situaciones como investigaciones judiciales que traerían consecuencias penales para la compañía y para el profesional que firma el acuerdo como se observa en el primera clausula la cual reza:

"Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de CyberFort Technologies no podrán ser divulgados."

Se denota con el solo objetivo del acuerdo de confidencialidad que la empresa CyberFort Technologieses, realiza procesos ilegales lo cual implicaría una responsabilidad por el profesional que suscriba este acuerdo ya que aceptaría las condiciones del objetivo del acuerdo entre las partes.

Ahora revisemos la segunda clausula en especial lo que se enuncia en su punto 2 así:

"Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:

Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos…”.

Aquí encontramos otra situación que es comprometedora tanto para la empresa como para el profesional que piense ser contratado por la empresa, puesto aceptan prácticas delictivas como son la interceptación de información, acceso abusivo a sistemas informáticos que los incriminaría donde se presente una inspección judicial por denuncias que se puedan presentar por estas malas prácticas que comete la empresa.

En relación con la tercera clausula no se encuentra ninguna observación y esta ajustada, sin embargo, al dar lectura de la cuarta clausula se encuentra reparos en las obligaciones 3, 4, 8 y 9 que igualmente que las observaciones anteriores aquí el directamente responsables es el profesional así:

“Cuarta. Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:”

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

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

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

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 CyberFort Technologies."

Se evidencia que la empresa en el presente acuerdo de confidencialidad no tiene obligación alguna zafándose de responsabilidades contractuales y de responsabilidad penal alguna como se observa en la cláusula quinta y octava del acuerdo y como si fuera poco el profesional deberá asumir de manea privada su defensa y exonera la empresa CyberFort Technologieses de cualquier tipo de responsabilidad legal y penal.

Frente a la segunda pregunta Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 – Acuerdo: acuerdo, deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

Una vez consultada la ley se pudo establecer que de acuerdo con lo manifestado en el punto anterior y dando respuesta a este se logra llegar a la conclusión que los siguientes artículos de la Ley se infringen con el acuerdo de confidencialidad presentado por la empresa empresa CyberFort Technologieses.

Para lo encontrado en el numeral 2 de la cláusula segunda Definición de información confidencial que reza;

"2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"

Claramente podemos ver que se enmarca las siguientes vulneraciones de los artículos de la Ley 1273 de 2009, toda vez que se atenta contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, así:

Artículo 269A: Acceso abusivo a un sistema informático. Porque según su acuerdo al suscribirse se acepta la responsabilidad al definir la información confidencial de la empresa incluyen datos secretos accesos abusivos a sistemas informáticos para obtener la información que les permita sacar provecho de manera ilícita.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. En Colombia una "chuzada" es la interceptación ilegal de las comunicaciones de alguien y como se menciona como datos de chuzadas, se hace uso de red de telecomunicación para llevar a cabo este fin, lo cual trasgrede el presente artículo.

Artículo 269C: Interceptación de datos informáticos, este articulo también se menciona como dato secreto interceptación de información, ya que se hace de manera ilegal sin ningún tipo de orden judicial que les permita capturara información reservada para darle usos indebidos.

Artículo 269F: Violación de datos personales, desde mi punto de vista este articulo también se infringe toda vez que al hacer uso de la información obtenida fraudulentamente saque provecho de la información recopilada.

En cuanto a la Clausula Cuarta. Obligaciones de la parte receptora en su obligación descrita en el numeral 3. "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros". Se podría verse envuelta la empresa en una investigación penal de acuerdo con el ARTÍCULO 463 del código penal Ley 599 de 2000 que tipifica el Espionaje, así: El que indebidamente obtenga, emplee o revele secreto político, económico o militar relacionado con la

seguridad del Estado y el profesional se vería incurso en una investigación por omisión de un acto punible.

Frente a la tercera pregunta ¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo, ¿usted como experto en ciberseguridad aplicaría a este trabajo en CyberFort Technologies, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros.

Una vez valoradas las implicaciones legales a las cuales me veo como experto de ciberseguridad como profesional en caso de firmar este contrato, he tomado la decisión de no aceptar la propuesta que hace la empresa CyberFort Technologieses por tal razón la rechazo de manera tajante, no firmare ningún tipo de contrato ni mucho menos ese acuerdo de confidencialidad en el que se manifiesta y se acepta por la empresa llevar a cabo situaciones que van en contra de la legislación y las leyes de la República de Colombia.

Además, que como profesional estaría faltando a la ética profesional del COPNIA, código mediante el cual estoy sujeto a poner en práctica buenas conductas profesionales en el desarrollo de mi profesión como ingeniero de sistemas, con este código puedo validar el comportamiento profesional exigible y le doy cumplimiento obligatorio, a mis deberes, prohibiciones y sanciones en los que puedo incurrir al firmar este tipo de contratos, a continuación expondré las violaciones al código de ética profesional que pudiera cometer al suscribir este acuerdo de confidencialidad y las sanciones a las cuales me vería abocado.

La violación comprobada a los deberes y prohibiciones dispuestos en el Código de Ética Profesional para este ejercicio claramente son las siguientes:

En cuanto a los Deberes Generales nos encontramos faltas a la letra f) denunciar los delitos lo cual no podríamos hacer si se firma el acuerdo de confidencialidad.

En relación con las prohibiciones generales tenemos la letra b) Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones.

Ahora se faltaría a la prohibición especial frente a la sociedad contemplada en el artículo 34 inciso a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación.

Igualmente se faltaría a los deberes para con la dignidad de sus profesiones contemplada en el artículo 35 inciso b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.

Según las violaciones antes descritas me conllevará la imposición de la máxima sanción por tratarse de una FALTA GRAVISIMA ya que la actuación como profesional al firmar este acuerdo de confidencialidad se encuentra descrita en el artículo 53 de la ley 842 de 2003, inciso e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares, lo que me ocasionaría como sanción la cancelación de la Matrícula Profesional.

Frente a la cuarta pregunta Deberá analizar el caso problema “Ciberespionaje y Ética en CyberFort Technologies” (Anexo 7 - Escenario 2), redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar y dar respuesta los siguientes interrogantes:

En relación al incidente se pueden observar que en cumplimiento de su función legal la empresa CyberFort Technologies, mitigo la amenaza y elimino el malware de los sistemas infectados, sin embargo la empresa se ha visto afectada con las decisiones tomadas por los expertos que acudieron al llamado del gobierno vecino a realizar la auditoria, ya que a cuenta propia sin autorización de la empresa causando un daño reputacional y utilizando la herramientas de análisis forense accedieron a comunicaciones sensibles y documentos estratégicos relacionados con temas de defensa, política exterior y negociaciones comerciales, faltado a la ética profesional por la violación de los deberes y prohibiciones dispuestos en el Código de Ética Profesional que conlleva a catalogarse como una FALTA GRAVISIMA toda vez que estaría violando las prohibiciones contempladas en el artículo 32 en el incisos b) Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley. Al igual podemos observar también se viola la prohibición del artículo 39 deberes de los profesionales para con sus clientes y el público en general en especial el inciso a). Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo.

En cuanto al ámbito jurídico aplicando las normas colombianas tenemos la violación del Artículo 269A: Acceso abusivo a un sistema informático, el Artículo 269C: Interceptación de datos informáticos, el Artículo 269E: Uso de software malicioso, el Artículo 269F: Violación de datos personales, adicionalmente a las penas contempladas en la Ley 1273 de 2009, que van desde los 36 o 48 meses hasta los 96 meses de prisión y multas de 100 a 1000 SMMLV se ven abocados al incremento de las mismas debido al Artículo 269H: Circunstancias de agravación punitiva: porque la conducta se cometió sobre redes o sistemas o de comunicaciones estatales u oficiales del sector financiero, nacionales o extranjeros por tal razón se aumentarán de la mitad a

las tres cuartas partes, dando como país Colombia donde se hizo la intervención por parte de la empresa CyberFort Technologies, se vincularía en un proceso penal donde se puede condenar a la empresa y a sus expertos ya que las versiones con las cuales justificaron sus acciones no fueron autorizadas por el gobierno lo que se convirtió un acto de ciberespionaje sin consentimiento y serán procesados por este incidente ocurrido en el mes de enero de 2024, claro que no solo podrán ser juzgados en Colombia sino que también se podrá solicitar por parte del gobierno a través de la Cancillería se inicie un proceso de cooperación internacional establecido en el convenio de ciberdelincuencia firmado en Budapets en el año 2001, para que a través de un proceso legal en el vecino País Chile puedan ser procesados bajo la Ley 21459 del 9 de junio de 2022, la cual "Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest" que contempla en su Artículo 1°.- Ataque a la integridad de un sistema informático. Artículo 2°.- Acceso ilícito. Artículo 3°.- Interceptación ilícita. Artículo 4°.- Ataque a la integridad de los datos informáticos. Artículo 6°.- Receptación de datos informáticos. Artículo 7°.- Fraude informático.

a) ¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

No debería de tener acceso a información privilegiada puesto que se presta para lograr acceso donde pueden expertos sacar provecho como se observa en el anexo 7 Escenario 2 por tal razón las empresas de ciberseguridad inicialmente para este tipo de auditoria deberán definir el alcance y los objetivos de la auditoria acordar controles de acceso con cero privilegios, desarrollar las pruebas de Ethical Hacking, gestionar el cierre de vulnerabilidades.

b) ¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Implementación de nuevas tecnologías como Zero Trust Network Access (ZTNA), también conocido como perímetro definido por software (SDP) que permita tener acceso remoto seguro a las aplicaciones internas con el menor privilegio.

Implementación actualización de las matrices de acceso

Implementar revisiones periódicas de los procesos y procedimientos de Ciberseguridad

Implementar políticas de supresión de usuarios administrador

Implementación de matrices de roles y responsabilidades según el cargo

Monitoreo de actividades y comportamiento del software de la empresa en especial las herramientas de ciberseguridad

Implementar mapas de riegos por procesos

Implementar un SOC y Herramientas de monitoreo y comportamiento de red NDR

Aplicando estas herramientas y controles por parte de las empresas de ciberseguridad se logrará minimizar los riesgos que puedan surgir de manera indebidos sobres las herramientas

c) ¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente?

Iniciar las acciones legales ante la Justicia para que sean Judicializados y se de aplicación a las leyes y normas vigentes que con este trabajo se han abordado lo cual permiten proteger la información y los datos informáticos de delitos informáticos y ciberespionaje.

Las medidas que se podrían implementar serian endurecer y aumentar las penas en relación a los delitos informáticos los cuales no deberían ser excarcelables, a fin que estos ciberdelincuentes sigan delinquiendo, lo mismo que se judicialicen en una mayor brevedad ya que el tiempo pasa y los delincuentes quedan en libertad por vencimiento de términos y siguen delinquiendo.

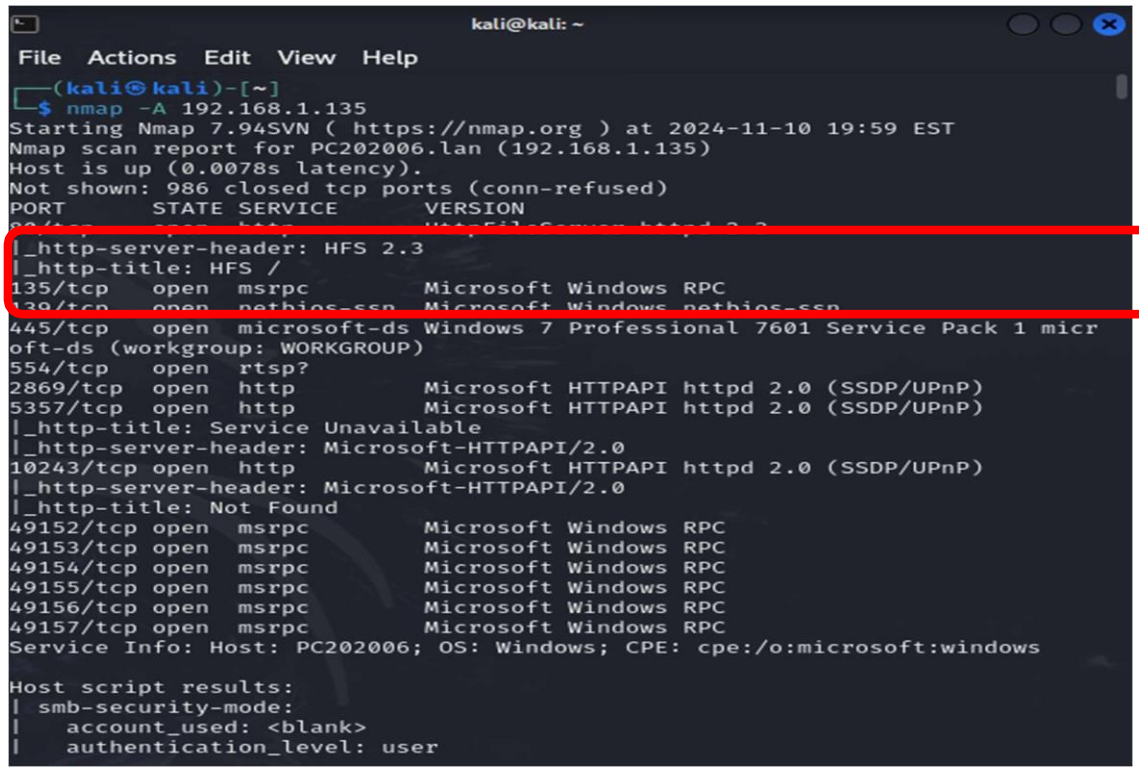
Herramientas de Software Red Team

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.

En la primera fase del Pentesting se hizo reconocimiento activo ya que se conocía la IP del equipo para analizar logrando una interacción directa con el objetivo en esta fase se hace uso de la herramienta Nmap por medio de la cual podemos escanear los diferentes puertos que se encuentran abiertos y pueden utilizarse debido algún nivel de vulnerabilidad desde la maquina Kali Linux.

Figura 11

Ejecución del Comando Nmap -A

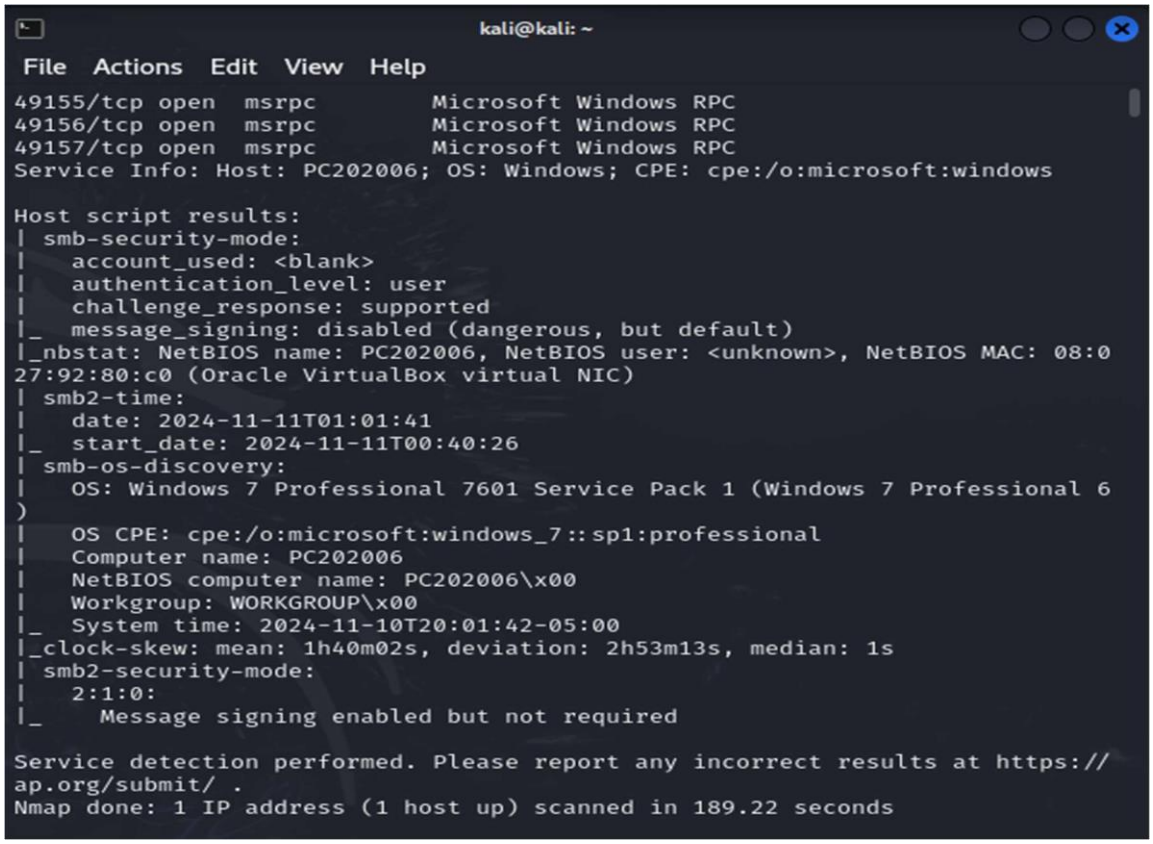


Nota: Se observa la ejecución del comando nmap -A desde la consola de Kali Linux.

Como se observa en la imagen evidenciamos que a través del puerto 80 se conecta la aplicación HFS la cual presenta una vulnerabilidad la cual puede ser explotable y tomar la máquina de manera remota.

Figura 12

Vulnerabilidad explotable puerto 80



Nota: Se conecta a través de la aplicación HFS logrando acceder a la máquina.

Adicionalmente nos muestra información importante del sistema operativo al cual estamos accediendo, dando información que permite ejecutar la explotación de una manera mas fácil, durante la recolección de información se logra obtener:

La MAC 08:27:92:80:c0. Donde se encuentra instalado: Oracle VirtualBox Virtual NIC OS CPE que corresponde a Windows7 profesional sp1, Nombre del Equipo: PC202006, El grupo de Trabajo: WORKGROUP.

Con toda la información que se recolecto en la fase 1 procedemos a iniciar nuestra fase 2 que corresponde al modelado de amenazas aquí se procede con utilizamos la herramienta METASPLOID ya que nos permite validar las posibles vulnerabilidades y llegar a explotarlas aquí se comprueba la defensa del sistema que se va a intervenir y cuáles son las vulnerabilidades detectadas que nos permitirá explotarlas en las siguiente fase. A través de Kali Linux con el comando msfconsole abrimos la aplicación la consola de metasploit así:

Figura 13

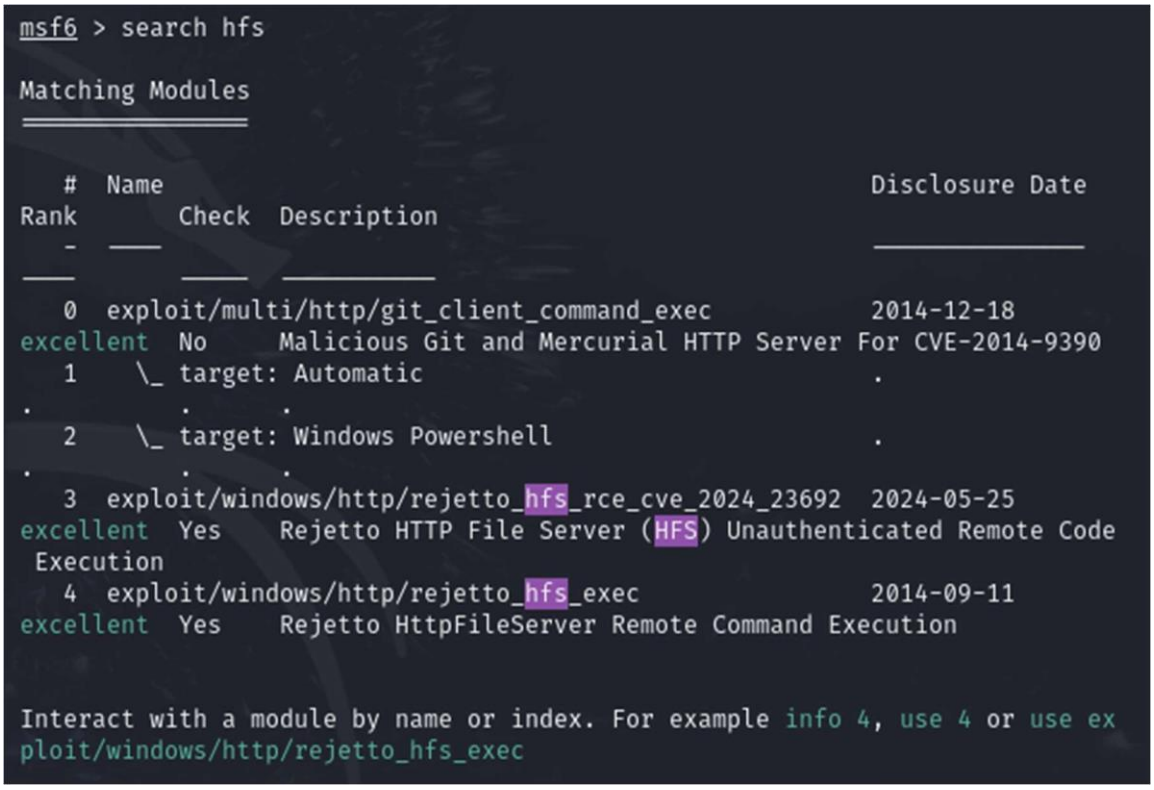
Acceso Consola de Metasploit

Nota: Se conecta a través de la aplicación HFS logrando acceder a la máquina.

Una vez cargada la consola de metasploit y con la información recopilada con el nmap en relación a la vulnerabilidad observada del programa HFS se procede con nuestra tercera fase del pentesting que corresponde al análisis de vulnerabilidades se hace una búsqueda a través del comando search hfs y encontramos que se puede hacer una explotación a través del exploit a través de la aplicación detectada con la herramienta nmap en su escaneo de puertos.

Figura 14

Ejecución Comando Search hfs



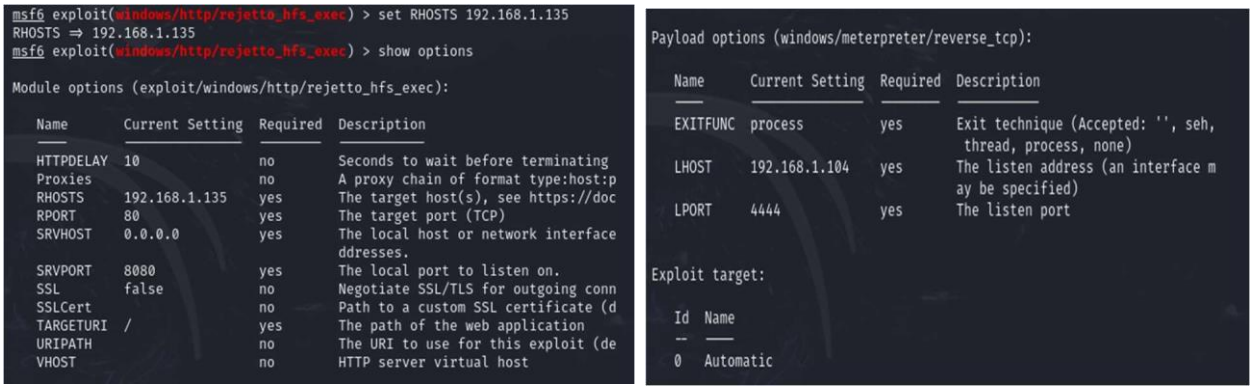
Nota: Se ejecuta el comando search hfs para detectar el exploit y explotar la vulnerabilidad.

Una vez definida el exploit por el cual se realizará la explotación procedemos con la cuarta fase que corresponde a la explotación seleccionamos el numero 4 de las opciones listadas ejecutando el exploit.

Una vez ejecutamos el exploid requiere que sea configurada razón por la cual se ejecuta el comando show options en los campos RHOST RPORT

Figura 15

Ejecución Comando Show Options



Nota: Se configuran las diferentes opciones del exploit.

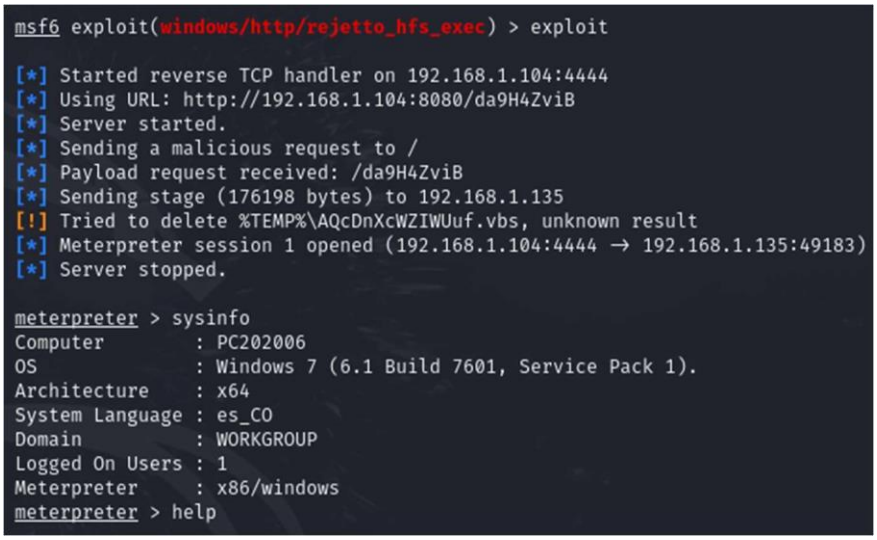
Se configura el RHOST que corresponde a la IP de la maquina victima Windows 7 en cuanto al RPORT por defecto estaba configurado en el puerto 80 que corresponde al puesto abierto

En las opciones igualmente nos muestra el playload que se utilizara la cual por defecto cargo la información del maquina Kali Linux en relación con LHOST y LPORT en este caso maquina atacante

Se procede a ejecutar el exploit como se observa a continuación una vez se conecta a la maquina W7 a través de una sesión de meterpreter se conoce más información de con el comando sysinfo.

Figura 16

Ejecución del Exploit y Sysinfo

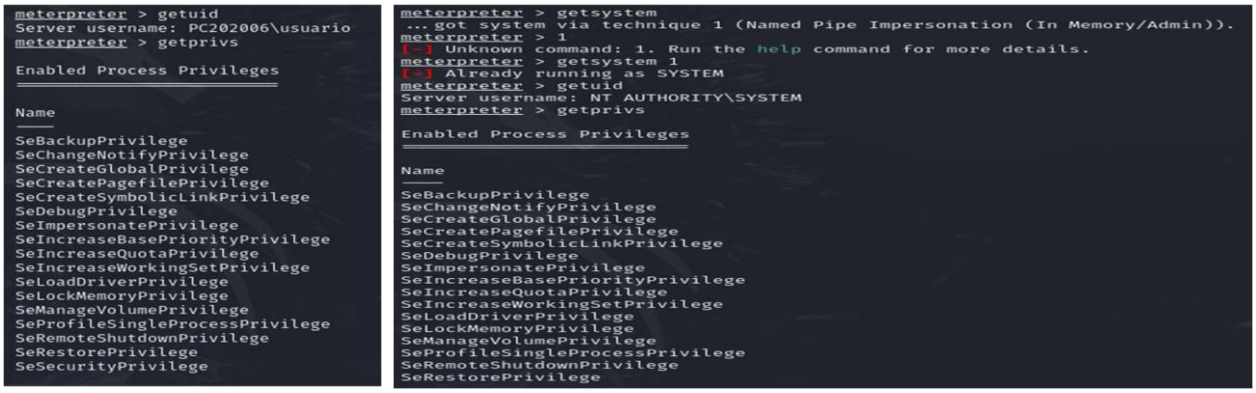


Nota: Se accede al equipo victima desde el equipo atacante a través de una sesión meterpreter.

Para conocer más acerca de meterpreter podemos utilizar el comando help para ver los comandos que podemos utilizar para acceder a los diferentes recursos de la maquina a través del meterpreter como el usuario a través del comando getuid y sus privilegios a través del comando getprivs como observamos a continuación el usuario no tiene privilegios de administrador.

Figura 17

Elevación de Privilegios

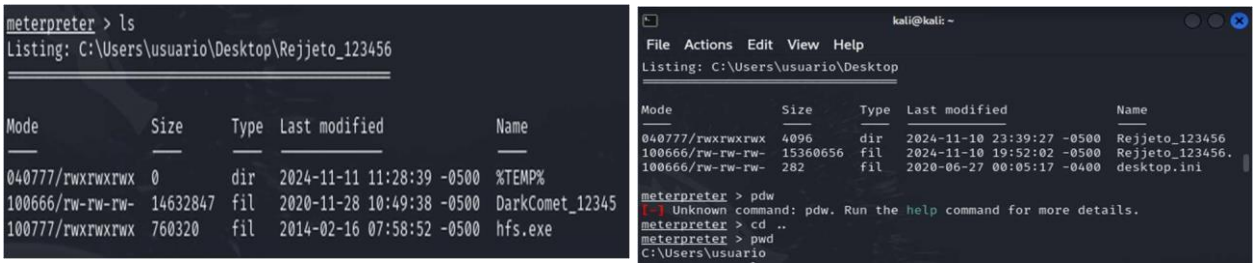


Nota: Se elevan privilegios en el equipo victima para tener control total de la máquina.

Con el comando getsystem se puede elevar privilegios al usuario dejándolo como NT AUTHORITY\SYSTEM antes se encontraba como Server username: PC202006\usuario con el comando ls podemos listar los archivos contenidos en las carpetas, y los demás comandos como cd para retroceder en las carpetas, cd para abrir carpetas y pwd vemos en que directorio nos encontramos.

Figura 18

Acceso a directorios y archivos



Nota: Comandos que permiten acceder a información confidencial permitiendo robarla.

También podemos acceder desde el powershell y ejecutar muchas opciones desde línea de comandos que también permiten verificar información adicional como lo es el comando net user que permite ver cuantas de usuario creadas en el sistema.

Figura *19*

Uso de Powershell

Nota: Con este comando logramos acceder a información de la máquina.

Para la fase de post explotación una vez encontradas las vulnerabilidades reales y que fueron explotadas y remediadas, se debe persistir en el sistema para volver a acceder al mismo toda vez que se abren nuevos servicios ocultos que también podrían ser explotados, por eso la importancia de continuar con una explotación posterior más a profundidad que nos permita extraer nueva información de posibles vulnerabilidades en busca de soluciones de los fallos de seguridad y lograr mitigarlos.

Reporte (Reporting) En esta última fase del Pentesting, se centra en generar un informe estructurados que evidencie los fallos de seguridad que se encontraron, las amenazas de ciberseguridad existentes, las soluciones de mitigación y las acciones de mejora en la seguridad de la organización.

Es importante que el informe sea comprensible por parte del personal técnico y no técnico de la empresa en todos sus niveles deben generarse informes técnicos y ejecutivos destinado para la toma de decisiones que permita a la organización tomar las medidas de asegurabilidad de sus sistemas de ciberseguridad.

2. A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows.

La primera misión del equipo Red Team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. 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 vulnerable bajo un windows; esta aplicación al parecer tiene asociado un exploit que puede terminar en un acceso a través de Shell, escalación de privilegios u otro tipo de ataque.

Dentro de la indagación, también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

Con esta información suministrada en el anexo se logra evidenciar que la organización se encuentra expuesta a un ataque por medio de la vulneración que se evidencio durante el ejercicio

3. ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows”? ¿Qué puerto abre la aplicación específica en el anexo?

Las herramientas utilizadas durante el desarrollo del ejercicio fueron:

Una maquina con Kali Linux

La aplicación nmap para escanear los puertos abiertos vulnerables y la información del sistema operativo victima

La consola de Metasploit que nos permite buscar exploit de la vulnerabilidad encontrada con nmap y ejecutarla para tomar el control de las maquinas

Sesión de meterprter

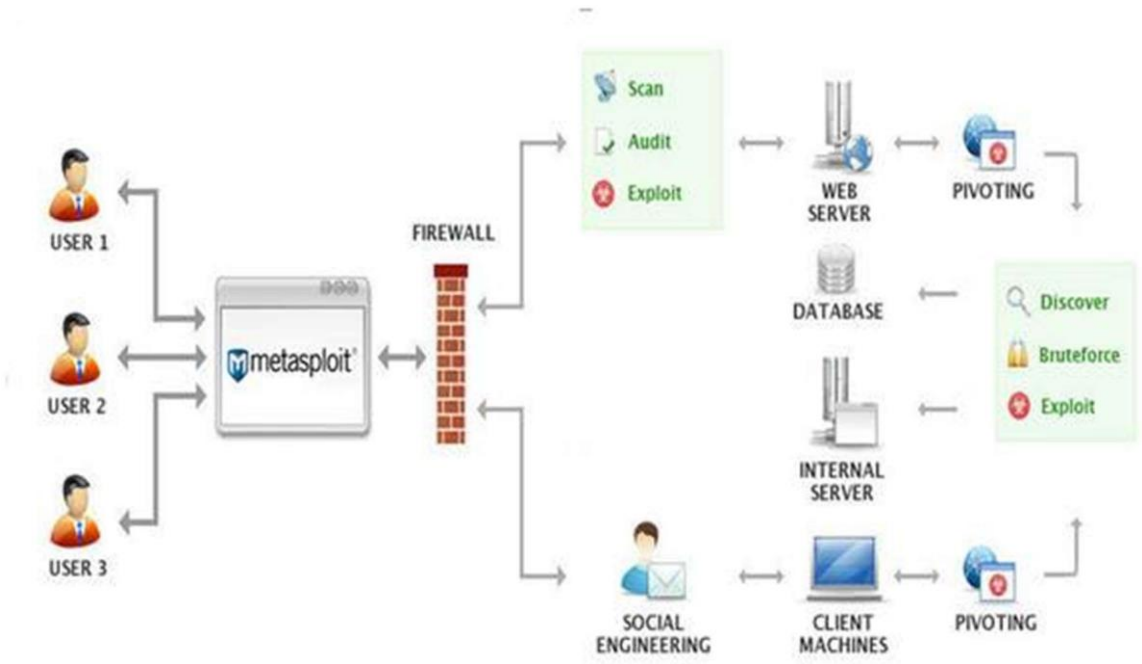
Powershell

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

El ataque a la maquina Windows puso en riego la información de la empresa toda vez que accedieron con privilegios de administrador elevándolos, logrando tener el control total de la maquina logrando desde esa maquina hacer pivoting escala de privilegios pueden hacer movimientos laterales y persistencia para que siempre continúen accediendo a los recursos e información de la organización.

Figura *20*

Diagrama del Ataque



Nota: Se observa el diagrama del ataque presentado a la maquina víctima.

Contención de Ataques Equipo Blue Team

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real?

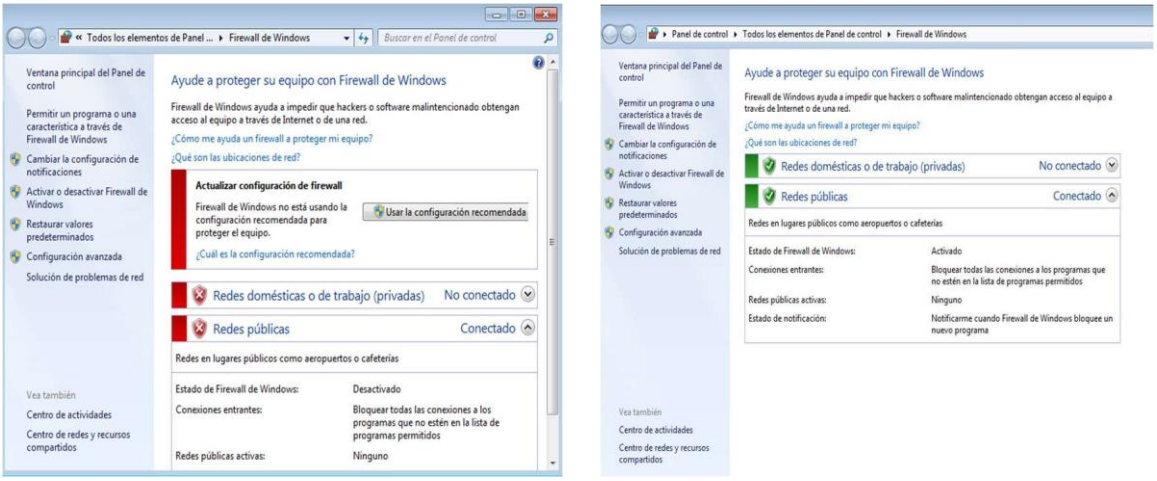
En caso de encontrarme con un ataque en tiempo real se debe indagar inicialmente con el equipo Red Team el tipo de ataque que se está sometiendo la empresa, con el fin de tomar las decisiones más acertadas frente a este activo de información determinando su alcance, impacto y vulnerabilidades explotadas para mitigar el riesgo en los demás activos de la empresa, por tal razón con la indagación preliminar se procede:

Aislar de manera inmediata el equipo de la red, con el fin contener el ataque y evitar su propagación en la red de la empresa. Se procede a la desconexión del punto de red inhabilitando el acceso al equipo para evitar que sea atacado o accedido de manera remota.

Revisar que el firewall se encuentre activo y configurado con altos niveles de seguridad una vez validado en el win7 se observa a continuación que esta desactivado por tal razón se procede a su activación.

Figura *21*

Desprotección y Protección Firewall

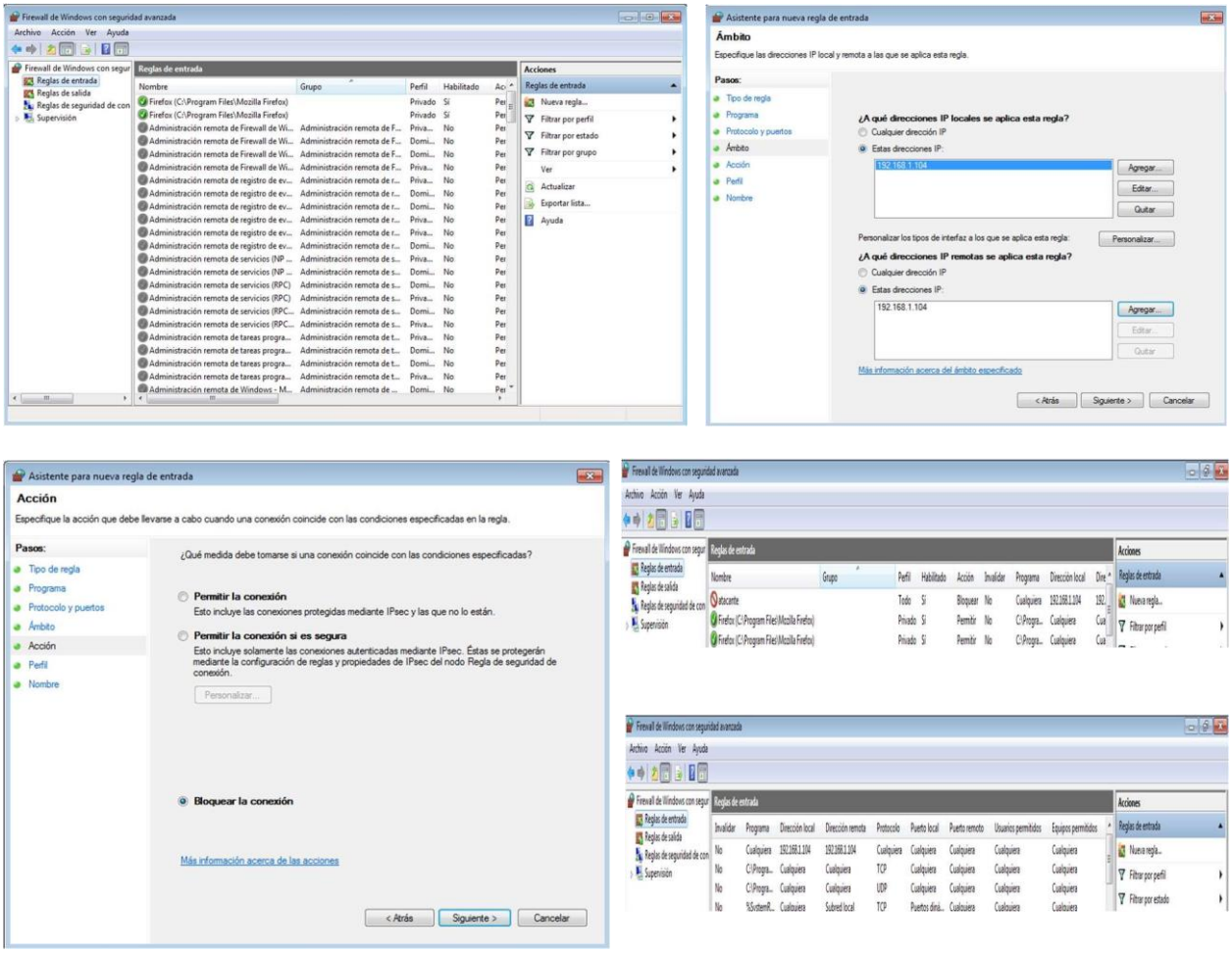


Nota: Se observa que el Firewall se encontraba desactivado y se activa.

Bloquear las direcciones IP origen del ataque: a través del firewall procedemos a bloquear la ip atacante en este caso la maquina Kali Linux ubicada en al IP 192.168.1.104 aplicando una nueva regla bloqueando la conexión

Figura *22*

Bloqueo de Direcciones IP a través de Reglas.



Nota: Con esta configuración y despliegue de reglas se bloquea el acceso a la máquina por la IP.

Revisar las Log de la máquina, el administrador de tareas, el visor de eventos a fin de evidenciar ejecución de procesos, tareas, eventos de seguridad, aplicaciones y demás ejecuciones que sean no comunes que se ejecuten desde el activo de información víctima del ataque, como no

se tiene implementado en la empresa un SIEM que nos permita evaluar estos tipos de hallazgos a través del monitoreo en tiempo real, lo debemos hacer de manera manual.

Validar el sistema operativo atacado si este cuenta con el soporte del fabricante que garantice aplicar las actualizaciones en seguridad periódicamente, evitando el uso de vulnerabilidades ya descubiertas, detectadas y resultas por el fabricante si no se actualiza el activo de información. En este caso encontramos que el sistema operativo tiene una copia sin licenciar además no cuanta con soporte del fabricante lo cual lo hace más vulnerable debido a que no se pueden correr las actualizaciones por tal razón se recomienda actualizar el sistema operativo a uno superior para este activo de información.

Revisar que el antivirus se encuentre actualizado a su última versión de actualización, se observa que no cuenta con un antivirus instalado por tal razón continúa siendo más vulnerable.

Medidas de Hardenización

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

Para minimizar los riesgos de ataque a los activos de información de la empresa a continuación relacionare las medidas de hardenización que se deben aplicar para evitar que se materialicen o se repitan este tipo de ataques:

Instalar actualizaciones de seguridad a través de políticas por medio de un cronograma que permita de manera regular la instalación de las actualizaciones al sistema operativo y antivirus logrando con esto reducir posibles vulnerabilidades, aplicando buenas prácticas.

Para nuestro ejercicio vemos que el equipo Windows 7 se encuentran las actualizaciones desactivadas, se hace imposible su actualización ya que no es una copia original Windows.

Validar reglas de firewall las cuales pueden estar muy genéricas y con un bajo nivel de seguridad para el sistema operativo como lo ocurrió con la maquina victima donde el firewall se encuentra desactivado. Se activa y se bloquea las IP atacantes.

Validar que las herramientas antivirus instaladas se encuentren actualizados además de herramientas perimetrales que permitan ampliar la protección del firewall bloqueando tráfico anormal, también se pueden utilizar otra herramienta que permiten mitigar riegos de seguridad pro ataques informáticos conocida como IPS sistemas de prevención e intrusiones que permite monitorear y analizar tráfico en la red en tiempo real para detectar comportamientos maliciosos o anómalos que permiten sospechar razón por la cual despliega una seria de mediadas que le permite bloquear proviniendo la amenaza causando un intento fallido de ataque, mientras que los IDS sistemas de detección de intrusiones solo se usa para alertar de la presencia de posibles amenazas al líder de seguridad estas herramientas permiten garantizar la integridad y

confidencialidad de la información sensible. Se procede a la instalación y actualización del antivirus protegiendo el equipo de virus y malware.

Aplicar controles de acceso fortaleciendo el uso de contraseñas robustas y autenticación segura como lo es el doble factor de autenticación, deshabilitar el uso de usuarios genéricos por default.

Robustecer el servidor de hfs con cabeceras de contenido seguro, CSP, protección de tipo de contenido nosniff, del mismo modo para evitar el clicjacking se utiliza la cabecera de xframeoptions opción sabe origen como se muestra a continuación. Lo que nos permite proteger ataques de ciberdelincuencia cerrando las posibilidades de ataques que afecten los activos de la empresa.

Figura *23*

Cabezas de contenido seguro.

```
### Configuracion Encabezados de Respuesta ###
# Politica de Contenido Seguro
add_header Content-Security-Policy "default-src https: data: 'unsafe-inline' 'unsafe-eval'" always;
#  Desactivar Ataques MIME sniffing sobre el sitio web
add_header X-Content-Type-Options nosniff;
# Previene el riesgos de ataques de clickJacking
add_header X-Frame-Options SAMEORIGIN;
# Bloquear Stague de Cross-site scripting (XSS) sobre el sitio web
add_header X-XSS-Protection "1; mode=block";
# Fortalecer y redicionar cuando detacta trafico inseguro
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
#Secure flag for Cookies
add_header Set-Cookie "Path=/; HttpOnly; Secure";
```

Nota: Con esta configuración se evitan ataques de ciberdelincuentes.

Reducir el campo de acción para los atacantes por medio de la aplicación de políticas procedimientos y buenas prácticas, que conlleven a deshabilitar servicios que no se usan en las máquinas, eliminando las posibles vulnerabilidades.

Implementar copias de seguridad a fin de salvaguardar los activos de información salvaguardando la información en su integridad.

Adicionalmente se pueden instalar balanceadores de red para distribuir y controlar el tráfico de la red a través de varios servidores además de la configuración de una DMZ que proporciona un bufer entre internet y la red privada evitando que los atacantes puedan hacer el reconocimiento para obtener información de los activos de la empresa.

Instalar herramientas de seguridad que prevengan intrusiones en el sistema detectando tráfico anormal o maliciosos como fail2ban la cual bloquea IPs que intentan acceso con contraseñas erradas, conexiones remotas por fuerza bruta.

Realizar pruebas de seguridad para identificar las posibles brechas de seguridad a través de los controles de acceso, firewall y sistemas de detección de intrusos con herramientas como Nexus la cual cuenta con plantillas de aseguramiento la cual nos dan recomendaciones o buenas prácticas y como implementarlo.

Diferencias Entre Un Equipo Blueteam y Un Equipo de Respuesta a Incidentes Informáticos

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

El equipo Blueteam tiene como competencia detectar prevenir y mitigar cualquier tipo de amenaza o ataque informático antes que se presenten, por tal razón este equipo debe constantemente monitorear la infraestructura de los activos de información de la empresa, a través de pruebas de vulnerabilidad las cuales planifica desarrolla y genera informes de los resultados que permite evidenciar los ataques, análisis de ciberseguridad, al igual descubrimiento de los vectores de ataque, lo cual conduce a la aplicación de políticas, procesos y procedimientos de seguridad, a su vez mediadas de seguridad y hardenizacion como las comentadas en el punto anterior, aplicando un rol defensivo y proactivo en la seguridad informática de la empresa.

En cuanto al equipo de respuesta de incidentes (CSIRT-CERT) su competencia es atender y responder a los incidentes informáticos de seguridad cuando se materializa, es el encargado de minimizar el incidente, restaurando la operatividad de los sistemas afectado, se encarga de investigar las causas del incidente, recopilación de las pruebas que permita socializarlo al comité de crisis de la empresa a más alto nivel, posteriormente divúlgalo a las autoridades para que se apliquen todo el protocolo de seguridad en las demás empresas o aliados para evitar esta clase de ataques, esto equipos aplican un rol reactivo en la seguridad informática de la empresa.

CIS “Center For Internet Security”

¿Si dentro de un equipo Blue Team le indican que debe trabajar con CIS “Center For Internet Security”, usted lo utilizaría para qué fin?

Inicialmente debemos conocer más a fondo el CIS Centro de Seguridad en Internet, reconocido a nivel mundial como el principal estándar de configuración segura, a su vez desarrolla checklist de verificación que permiten identificar y mitigar las vulnerabilidades en materia de seguridad, posee un banco de información relacionada con la ciberseguridad que se utiliza para mitigar y prevenir ser víctima de hurto y fuga de información.

Así como se puede validar la importancia del CIS a nivel mundial efectivamente lo utilizaría dentro de mi equipo Blue Team puesto que la información que nos suministra permitiría a la empresa identificar y mitigar posibles vulnerabilidades en temas de seguridad aplicando los recursos y herramientas de verificación que CIS tiene a disposición minimizando los riesgos de seguridad que se puedan presentar hasta su contención y/o eliminación garantizando que el grupo de Blue Team altos niveles de seguridad mejorando en detección prevención de las amenazas informáticas que se puedan presentar

Funciones y Características Principales de lo Que Es Un SIEM.

SIEM (Security Information and evento Management) Sistema de gestión de eventos e información de seguridad, este sistema tiene el control sobre la seguridad informática de la empresa toda vez que es un correlacionador de eventos que centraliza sus Logs para detectar tendencias y patrones fuera de lo normal está en la capacidad de detectar responder y neutralizar las amenazas informáticas antes que se materialicen gracias a su sistema central que proporcionando una visión global de la seguridad de la tecnología de la información SIEM es la combinación de SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad). Esta unión genera una recuperación más ágil de los eventos de seguridad a través de su identificación y análisis

Funciones del SIEM

Realiza recopilación de forma centralizada de datos de todos los dispositivos de seguridad y los de red.

Realiza correlación de todos los eventos para detectar diferentes patrones de comportamiento.

Realiza el análisis de comportamiento de toda la información recopilada y correlacionada de las diferentes fuentes para normalizar a través de algoritmos con el fin de identificar con análisis estadísticos comportamientos anómalos en la red o en los dispositivos de seguridad.

Detección de amenazas, en base a los resultados del análisis se pueden detectar errores de seguridad que se pueden materializar y convertirse en una amenaza de seguridad, razón por la cual se hace uso de patrones y anomalías en la red para identificarlas.

Respuesta a incidentes, una vez detectada la amenaza su puede proveer información minuciosa de la amenaza y su contexto para que los equipos de respuesta a incidentes para que pueda tomar decisiones al respecto.

Características del SIEM

Recolectar información de diferentes dispositivos de seguridad o de red de las diferentes fuentes de datos (logs del sistema, log de aplicaciones, registros de eventos, registros de seguridad, vulnerabilidades) y demás que puedan ayudar.

Normalizar la información recolectada que contenga la misma fecha y hora permitiendo hacer búsquedas y análisis de la información recolectada.

Análisis de información y correlacionamiento permite validar el comportamiento a través de algoritmos y análisis detectando anomalías que se puedan convertir en alertas y/o riesgos de seguridad.

Módulo de gestión o Dashboard donde podamos administrar la solución y visualizar en tiempo real las alertas analizadas a traves del monitoreo por medio de tableros de información y mediante generación de informes del estado de seguridad de la red.

Integración de funciones avanzadas que permitan integra con otros sistemas de seguridad.

Dentro del mercado se encuentran los siguientes SIEMS, Open Source: OSSIM de Alien Vault, Wazuh, Sagan, OSSEC que son gratuitos, aunque este último posee una versión premium.

Herramientas de Contención de 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.

Firewalls

Son una herramienta indispensable para evitar ataques de internet actúa como una barrera protectora que filtra el paso de trafico de red validando si se trata una amenaza o no permite dividir la red internar con la red exterior, son parametrizables y se encuentran de 2 tipos. Los firewalls de software que se instalan en las maquinas no tangibles y los firewalls de hardware que corresponden a dispositivos físicos tangibles instalados separando la conexión interna y el internet

Software Antivirus y Anti Spyware

Son programas diseñados para detectar, prevenir y eliminar software malicioso y que los equipos de cómputo, redes y demás dispositivos permanezcas a salvo de ataques informáticos (ciberataques) o malware.

Sistemas de Prevención de Intrusiones (IPS)

Herramienta de contención de ataques informáticos que se utiliza para monitorear el tráfico de red en busca de actividades sospechosas o maliciosas. Estos sistemas utilizan una combinación de técnicas de detección de intrusiones y análisis de tráfico para identificar y bloquear posibles amenazas antes de que puedan causar daño. Los IPS pueden ser hardware o software, y pueden ser configurados para bloquear automáticamente el tráfico de red malicioso o enviar alertas a los equipos de seguridad para una respuesta manual.

HONEYPOT

Sistema de trampa y señuelo que evita un posible ataque a los sistemas informáticos de la empresa su función es detectar y obtener información del atacante haciendo creer que ingreso al sistema real cuando está dentro de la simulación logrando engañar al ciberdelincuente y observando lo que hacen y que vulnerabilidades está atacando.

OSSIM de Alien Vault

Open Source Security Information Management corresponde a una colección de herramientas bajo la licencia GPL, que permite detectar intrusos prevenir ataques dentro de la red.

Recomendaciones

Como recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización se deben tener en cuenta la implementación de políticas de seguridad informática la cual se debe dar a conocer a todos los miembros de la empresa desde el cargo menor hasta el nivel directivo, por medio de esta política la cual debe ir alineada con el Sistema de Gestión de la Seguridad de la Información (SGSI) dando aplicación a la norma ISO/IEC 27001.

Dentro de aspectos relevantes a tener en cuenta para lograr endurecer los aspectos de seguridad se debe implementar buenas prácticas a nivel de seguridad informática como son:

Correcta activación y configuración de los firewalls que garanticen un tráfico estable en la red a través de filtrado de peticiones y rechazo de spam.

Restringir el permiso de instalación de aplicaciones y mucho menos de aplicaciones de acceso remoto que puedan contener vulnerabilidades, esta tarea dede ser de uso explusivo del área TI de la empresa.

Eliminar el uso de usuarios con privilegios de administrador que puedan generar vectores de ataques por desconocimiento.

Aplicar políticas de cambio de contraseñas de manera periódica a todos los usuarios

Aplicar políticas de actualización de sistema operativo, antivirus y todos los aplicativos que requieran.

Gestionar tareas de backups de la información.

Aplicar políticas de correo no deseado que contenga archivos de extensión desconocida

Mantener actualizado el software antivirus.

Aplicar tareas de los grupos Red Team y Blue Team de manera periódica con Nmap para revisar puertos y servicios en los equipos de cómputo y equipos activos de red logrando cerrar puertos y servicios innecesarios.

Implementar herramientas de seguridad perimetral DMZ, UTM, logrando proteger de manera efectiva la red interna de la externa mitigando cualquier tipo de ataque

Implementar las políticas de seguridad informática alineadas con el SGSI aplicando la norma ISO 27001.

Implementar planes de capacitación a los miembros de la empresa socializando los diferentes tipos de ataques a los cuales se pueden ver expuestos aplicando ingeniería social.

Conclusiones

Se hace necesario que los equipos de ciberseguridad, garantizar la seguridad de la información adelantando los procesos de pentesting, con el fin de mitigar las vulnerabilidades y la explotación de los fallos de seguridad que se puedan evidenciar durante las diferentes fases de las pruebas de penetración haciendo uso de las herramientas gratuitas que ofrece el mercado logrando así evaluar la infraestructura tecnológica y evitando posibles ciberataques que atenten contra la confidencialidad, la integridad y la disposición de los datos y de los sistemas informáticos.

Los delitos informáticos y la protección de datos personales se encuentran regulados por la normatividad vigente logrando que el aparato investigativo y judicial puedan judicializar a los ciberdelincuentes que actualmente están al acecho debido al crecimiento en materia tecnológica que el país ha venido desarrollando en los últimos años.

El uso de herramientas tecnológicas de ciberseguridad ayuda a cerrar las brechas de seguridad de las organizaciones cuando se establecen bajo procedimiento de Ethical Hacking y no como delincuentes cibernéticos.

Con la aplicación de herramientas de contención y detección los equipos Blue Team lograr desarrollar un buen trabajo a nivel de ciberseguridad, garantizar la seguridad de la información apliquen las diferentes herramientas que se encuentran disponibles en el mercado.

La ejecución del SIEM permite gestión de eventos de manera centralizada con toda la información de seguridad de red, este sistema tiene el control sobre la seguridad informática de la empresa lograr detectar y minimizar las vulneraciones al interior de las organizaciones.

Bibliografía

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Congreso Colombia. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

MINTIC. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas de- Privacidad-y-Condiciones-de-Uso

OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Policía. (2009). Ley 1273 [LEY_1273_2009].Policía. (pp. 1-4). https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Zuluaga Mateus. (2017). Hacking Ético Basado En La Metodología Abierta De Testeo De Seguridad – Osstmm, Aplicado A La Rama Judicial, Seccional

ARMENIA. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/17410

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). 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

Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information, 14(11), 587. https://doi.org/10.3390/info14110587

CIBERSEGURIDAD. (2024). Qué es Metasploit Framework y cómo funciona. Obtenido de https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

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

Colombia, C. (2012). Ley 1581 de 2012. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general . Obtenido de https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CVE.ORG. (2024). Acerca del programa CVE. Obtenido de https://www.cve.org/About/Overview cybergo. (2020). PenTest: testes de penetração. Obtenido de https://cybergo.com.br/pentest-testes-de-penetracao/

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

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

NMAP.ORG. (2024). Ejemplos. Obtenido de https://nmap.org/man/es/man-examples.html NMAP.ORG. (2024). Guía de referencia de Nmap. Obtenido de https://nmap.org/man/es/index.html#man-description Pública, E. F. (09 de 10 de 2023). Ley 842 de 2003. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=40907 Pública, F. (2000). Ley 599 de 2000. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388#VIIBIS

Pública, F. (2009). Ley 1273 de 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Pública, F. (2022). Decreto 338 de 2022 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285-288. https://doi.org/10.1109/ICCD.2011.6081410

school, k. t. (2024). Comandos de Metasploit. Obtenido de https://keepcoding.io/blog/comandos-de-metasploit/

School, K. T. (2024). Qué es ExploitDB. Obtenido de https://keepcoding.io/blog/que-es-exploitdb/

WIKIPEDIA.ORG. (2024). OpenVAS. https://es.wikipedia.org/wiki/OpenVAS#Caracter%C3%ADsticas_principales Zambrano Hernández, Peña Hidalgo, H. J., & Cardenas Corral. (2024). Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Apéndices

Apéndice A

Link Video Sustentación

https://youtu.be/x-clzkA2nSI