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

SERGIO ENRIQUE VALERO PEÑARANDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
2023

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

SERGIO ENRIQUE VALERO PEÑARANDA

Curso: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team - (202337164A_1435)

M.Sc. John Freddy Quintero Tamayo
Director de curso.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
2023

TABLA DE CONTENIDO

Pág.

TABLA DE ILUSTRACIONES

Pág.

RESUMEN

El presente documento es un informe técnico que describe el proceso paso a paso que realiza un equipo a Blue Team y Red Team que inicia con el reconocimiento e implementación de un banco de trabajo en una máquina virtual en Virtualbox para generar un ataque informático controlado en una de las maquinas del banco de trabajo, identificando las vulnerabilidades a través de pruebas de penetración, para luego implementar metodologías de hardenización utilizando buenas prácticas en software y hardware para el desarrollo de acciones en seguridad informática y de la información y de esta forma minimizar o controlar los ataques cibernéticos en una organización

Palabras clave: Equipos red team y blue team, pentesting, Hardening

GLOSARIO

Seguridad Informática: Es el conjunto de medidas y prácticas destinadas a proteger los sistemas informáticos, la información almacenada en ellos y la privacidad de los usuarios de estos sistemas.

Sistema Operativo: "Conjunto de programas que permite manejar la memoria, disco, medios de almacenamiento de información y los diferentes periféricos o recursos de nuestra computadora."[1] Algunos de estos sistemas operativos son Windows, Linux, Mac Os y DOS.

Ataque Informático: "Un ataque informático es un intento de acceder a tus equipos informáticos o servidores, mediante la introducción de virus o archivos malware, para alterar su funcionamiento, producir daños o sustraer información sensible para tu empresa." [2].

Amenaza Informática: "Se entiende como amenaza informática toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático." [3].

Confidencialidad de la información: "acceso a la información solo mediante autorización y de forma controlada." [4].

Integridad de la información: "modificación de la información solo mediante autorización."

---

[1] Euroinnova (2023). *El sistema operativo*. Recuperado de https://www.euroinnova.co/sistema-operativo

[2] Caser.es (n.d.). *Ataque informático*. Recuperado de https://www.caser.es/glosario-seguros/comercio/ataque-informatico

[3] Ambit (2020). Amenzas informáticas. Recuperado de https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

[4] Elvira Mifsud (2012) *MONOGRÁFICO: Introducción a la seguridad informática - Seguridad de la información / Seguridad informática.* Recuperado de http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1#:~:text=Confidencialidad%3A%20acceso%20a%20la%20informaci%C3%B3n,debe%20permanecer%20accesible%20mediante%20autorizaci%C3%B3n.

Disponibilidad de la información: “la información del sistema debe permanecer accesible mediante autorización.” [4]

Equipo Red Team: Es un equipo de atacantes simulados que trabaja para explotar vulnerabilidades y debilidades en un sistema o red, simulando una intrusión real.

Equipo Blue Team: Es un equipo de defensa que trabaja para proteger el sistema o red de intrusiones simuladas.

Pentesting: “El Pentesting es una abreviatura formada por dos palabras “penetration” y “testing” y es una práctica/técnica que consiste en atacar diferentes entornos o sistemas con la finalidad de encontrar y prevenir posibles fallos en el mismo.” [5]

Ciberseguridad: “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.” [6]

Hackspaces: “Son lugares físicos operados por la comunidad, donde las personas comparten su interés por jugar con la tecnología, se reúnen y trabajan en sus proyectos, y aprenden unos de otros.” [7]

[5] Campus Internacional CIBERSEGURIDAD (2023) *¿Qué es el Pentesting?.* Recuperado de https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting
[6] Kaspersky. (n.d.) *¿Que es la ciberseguridad?* Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
[7] Hackerspaces. (n.d.) Hackerspaces. Recuperado de https://hackerspaces.org/

INTRODUCCIÓN

La seguridad informática es una disciplina encargada de salvaguardar los sistemas informáticos, redes y datos ante posibles intrusiones y amenazas e incluye protección de la privacidad, integridad y disponibilidad de la información, así como protección contra la interrupción o mal uso de los sistemas informáticos.

La seguridad informática es crítica en un mundo cada vez más digital, ya que la mayoría de las organizaciones dependen de los sistemas informáticos para sus operaciones diarias. Además, los ataques informáticos pueden tener consecuencias graves, incluyendo pérdida de datos confidenciales, interrupción del negocio y daño a la reputación de la organización.

Para garantizar la seguridad informática, es importante adoptar medidas preventivas, como la implementación de políticas de seguridad sólidas, educación de los usuarios, contratar expertos en seguridad informática, así como el constante monitoreo de los sistemas informáticos para detectar y actuar ofensivamente o preventivamente ante amenazas a la seguridad de la información.

En general, la seguridad informática es un aspecto crítico de la gestión de la información, y requiere un enfoque proactivo y constante para garantizar la protección de los sistemas informáticos, redes y datos de las organizaciones.

Expuesto lo anterior desarrollaremos en cuatro fases un informe técnico de las capacidades técnicas, legales y de gestión desarrollado en el seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

- A través de un informe técnico evaluar e implementar acciones a partir del uso de metodologías y técnicas de intrusión y vulnerabilidades en seguridad informática aplicadas por los equipos Blue Team y Read Team, dentro de un marco de criterios éticos y legales, para la contención de ataques informáticos en una organización.

1.2 OBJETIVOS ESPECÍFICOS

- Analizar la legislación Colombia con relación a delitos informáticos.
- Analizar y evaluar las vulnerabilidades y debilidades en la seguridad de un sistema o aplicación informática
- Analizar los métodos de contención en un ataque informático en tiempo real.
- Implementar acciones de hardenización para minimizar ataques a la seguridad informática.
- Explicar las diferentes herramientas y servicios utilizados en ciberseguridad.
- Reconocer herramientas utilizadas en la contención de ataques informáticos.
- Implementar y configurar un “banco de trabajo” en un entorno local.
- Analizar un acuerdo de confidencialidad desde el punto de vista legal y no ético con referencia a la violación de la ley 1273 de 2009.
- Analizar una propuesta de trabajo para seleccionar el personal de los equipos Red team y Blue team, desde el punto de vista legal y ético.

2. DESARROLLO DEL INFORME

A continuación, se desarrollará la Etapa 1 - Conceptos equipos de Seguridad, el cual será la primera fase del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

2.1 CONCEPTOS Y LEGISLACIÓN SOBRE DELITOS INFORMÁTICOS

2.1.1 Legislación actual sobre delitos informáticos en Colombia.

El aumento de los ataques informáticos en el mundo y en Colombia es un reflejo de la creciente dependencia de la tecnología y la información en la sociedad moderna.

Con la adopción masiva de tecnologías de la información y las comunicaciones, se han creado nuevos canales para que los ciberdelincuentes perpetren ataques informáticos con el objetivo de obtener ganancias económicas, acceder a información confidencial o causar daños a la infraestructura informática.

En Colombia, el aumento de los ataques informáticos se ha visto impulsado por la falta de medidas preventivas adecuadas y la falta de conocimiento sobre lo realmente importante que es la seguridad informática. Además, los servicios encargados de analizar, investigar y perseguir estos hechos tienen limitaciones en cuanto a recursos y capacitación, lo que hace más difícil combatir estos ataques.

En el mundo, el aumento de los ataques informáticos se ha acelerado debido a la pandemia de COVID-19, que ha llevado a un aumento del trabajo remoto y la dependencia de las tecnologías de la información y las comunicaciones. Esto ha creado nuevos puntos de entrada para los atacantes, incluyendo la explotación de la tecnología obsoleta o la falta de medidas de seguridad adecuadas.

Así como las conductas delictivas convencionales o tradicionales se encuentran tipificados en leyes explícitamente creadas para su penalización, de igual forma para la judicialización de los delitos informáticos se crearon nuevas legislaciones relacionados con vulnerabilidades contra el acceso y la protección de la información y de los datos en Colombia, los cuales permiten condenas a través de penas con privación de la libertad y/o multas y se citarán a continuación:

Ley 1273 de 2009[8] sobre Delitos Informáticos: Esta ley establece las sanciones penales para los delitos informáticos cometidos en Colombia, incluyendo el acceso no autorizado a sistemas informáticos, la manipulación de información, la interceptación ilegal de comunicaciones, entre otros.

Decreto 1377 de 2013[9] sobre Protección de Datos Personales: Este decreto establece las normas para la protección de datos personales en Colombia, incluyendo los derechos de las personas sobre su información personal y las responsabilidades de las empresas y entidades en su recolección, almacenamiento y uso.

Ley 1581 de 2012[10] sobre Protección de Datos Personales: Esta ley establece los derechos de los titulares de la información y las obligaciones de los responsables y encargados del tratamiento de datos personales, y regula el registro, uso y protección de los datos personales.
En general, estas leyes tienen como objetivo proteger los derechos de las personas en relación a su información personal y prevenir los delitos informáticos.

2.1.2 Pentesting

Penetration Testing (Prueba de penetración o "pentesting" en español) es una técnica de seguridad informática utilizada para evaluar la seguridad de un sistema o aplicación informática. El objetivo del pentesting es evidenciar vulnerabilidades y debilidades en la seguridad de los sistemas y proporcionar recomendaciones para solucionarlas antes de que puedan ser explotadas por un atacante malintencionado.

En un pentest, un equipo de expertos en seguridad informática simula un ataque realista para evaluar la eficacia de las medidas de seguridad actuales. Esto se hace mediante la aplicación de herramientas y técnicas de hacking ético en busca de vulnerabilidades en el sistema y obtener acceso no autorizado a los datos y recursos, siendo esta una parte importante de la gestión de la seguridad de la información y mejoras en la seguridad de un sistema antes de un ataque real. Este proceso de pentesting debe ser llevado ejecutado por profesionales expertos

[8] Secretaría del Senado. (2022) Ley 1273 de 2009. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/arbol/1000.html
[9] Función Pública. (n.d.) Decreto 1377 de 2013. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646#:~:text=Se%C3%B1ala%20lo%20relacionado%20con%20el,al%20tratamiento%20de%20datos%20personales
[10] Función Pública. (n.d.) Ley 1581 de 2012. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

capacitados y autorizados, ya que una mala implementación o interpretación puede causar daños adicionales a los sistemas evaluados.

El pentesting es un proceso que consta de varias etapas y su objetivo es evaluar la seguridad de un sistema informático.

A continuación, se describirá cada una de las etapas y se cita un ejemplo:

- Planificación: En esta etapa, se establecen los objetivos y los alcances del pentesting, así como se determinan los recursos y las restricciones necesarias para llevar a cabo el proceso. Por ejemplo, se puede establecer un objetivo de evaluar la seguridad de un sitio web y se definen las restricciones para no causar daños al sistema.

- Recopilación de información: En esta etapa, se recopila información sobre el sistema y la infraestructura que se va a evaluar. Por ejemplo, se pueden buscar detalles sobre la topología de la red, las tecnologías utilizadas y la presencia de sistemas externos que interactúan con el sistema objetivo. Herramientas utilizadas Dnsmap, Dnsrecon, Nmap, Recon-ng, SubFinder entre otras.

- Análisis de vulnerabilidades: En esta etapa, se analizan las vulnerabilidades potenciales del sistema y se determinan los puntos de ataque. Por ejemplo, se pueden buscar vulnerabilidades en el software utilizado, en la configuración de la red o en las políticas de seguridad. Herramientas utilizadas Nessus, OWASP Zap Proxy, BugBounty Recon, Vega, BurpSuite entre otras.

- Explotación: En esta etapa, se lleva a cabo la explotación de las vulnerabilidades identificadas. Por ejemplo, se pueden utilizar herramientas de pentesting para acceder a un sistema o para causar daños a la infraestructura. Herramientas utilizadas OpenVAS, Nessus, BeEF, Metasploit Framework, Routersploit, PowerSploit, SPARTA, Xarp, SQLMap, BurpSuite entre otras.

- Evaluación: En esta etapa, se evalúan los resultados del pentesting y se determinan las recomendaciones para corregir las vulnerabilidades

identificadas. Por ejemplo, se pueden recomendar cambios en la configuración de la red o en el software utilizado para mejorar la seguridad del sistema.

- Informe: Finalmente, se prepara un informe con los resultados del pentesting y se proporcionan las recomendaciones para corregir las vulnerabilidades identificadas. Por ejemplo, se puede presentar un informe con detalles sobre las vulnerabilidades encontradas, las explotaciones realizadas y las recomendaciones para corregir las vulnerabilidades. Herramientas utilizadas Dradis, Faraday, Simple Vulnerability Manager.

2.2 HERRAMIENTAS DE CIBERSEGURIDAD

Las herramientas de ciberseguridad son software y hardware diseñados para ayudar a proteger sistemas informáticos y redes contra ataques cibernéticos y amenazas en línea, siendo estas de gran ayuda para detectar, prevenir y mitigar riesgos de seguridad.

Algunos de los tipos más comunes de herramientas de ciberseguridad son:

- Firewalls: son dispositivos o software que controlan el tráfico entrante y saliente en una red y bloquean las conexiones no autorizadas. Estos ayudan a proteger los sistemas de ataques externos como los virus o malware.
- Antivirus y antimalware: estas herramientas protegen los sistemas contra virus, malware, spyware y otras amenazas informáticas. Realizan análisis en tiempo real y escaneos regulares para detectar y eliminar software malicioso.
- Herramientas de detección y respuesta a incidentes (IDS/IPS): estas herramientas monitorean continuamente la actividad en una red y alertan en caso de detectar comportamientos anómalos o amenazas.
- Soluciones de gestión de seguridad de la información (SIEM): estas herramientas combinan información de varios puntos de la red y proporcionan una visión global de la seguridad. A menudo incluyen análisis en tiempo real y generación de informes para ayudar a los administradores a detectar y responder a las amenazas.
- Encriptación de datos: las herramientas de cifrado protegen la confidencialidad de los datos al aplicar una capa de seguridad a los datos sensibles.

- Es importante tener en cuenta que, aunque las herramientas de ciberseguridad son útiles, estas no garantizan la protección total contra todas las amenazas que existen actualmente y que día a día crecen por lo cual es importante implementar medidas de seguridad en diferentes capas y mantener las herramientas actualizadas y los profesionales especializados para asegurarse de contar con la máxima protección contra amenazas en línea y fuera de línea.

A continuación, se enuncian algunas herramientas de ciberseguridad y servicios en línea:

METASPLOIT

Metasploit es una plataforma de seguridad de código abierto utilizada para realizar pruebas de penetración (pentesting) en sistemas y redes. Fue desarrollada por HD Moore y actualmente es mantenida por la empresa de seguridad informática Rapid7.

Metasploit permite a los profesionales de seguridad probar la seguridad de los sistemas y aplicaciones para identificar vulnerabilidades y debilidades. La plataforma incluye una amplia biblioteca de exploits, herramientas y módulos que facilitan la identificación y explotación de las vulnerabilidades. Además, Metasploit permite automatizar pruebas de penetración y personalizar ataques para adaptarse a las necesidades específicas de cada organización.

Metasploit es ampliamente utilizado por profesionales de seguridad y empresas para evaluar la seguridad de sus sistemas y aplicaciones. Sin embargo, también es utilizado por atacantes malintencionados para realizar ataques y explotar vulnerabilidades en sistemas y redes. Por lo tanto, es importante utilizar Metasploit de manera ética y responsable para proteger los sistemas y los datos sensibles.

Para más información acceder a la siguiente URL https://www.metasploit.com/

Nmap.

Nmap es una herramienta de escaneo de puertos y seguridad de código abierto utilizada para explorar redes y dispositivos. Fue desarrollada por Gordon Lyon y es ampliamente utilizada por profesionales de seguridad informática, administradores de sistemas y desarrolladores de software.

Nmap permite a los usuarios escanear dispositivos en una red para identificar los servicios y puertos que están activos, así como la información sobre el sistema operativo, las versiones de software y otros detalles técnicos. Además, Nmap puede utilizarse para identificar vulnerabilidades y debilidades en los sistemas y aplicaciones, y para investigar ataques e intrusiones.

Nmap es una herramienta poderosa que puede ser utilizada tanto para fines legítimos como ilegítimos. Por lo tanto, es importante utilizar Nmap de manera ética y respetar las políticas de seguridad y privacidad de las redes y dispositivos que se escanean. Nmap es una herramienta valiosa para profesionales de seguridad y administradores de sistemas que buscan mejorar la seguridad de sus redes y dispositivos.

Para más información acceder a la siguiente URL https://nmap.org/

OpenVas

OpenVAS es un sistema de gestión de seguridad de código abierto el cual permite realizar escaneos de vulnerabilidades en sistemas y aplicaciones. Es una solución completa para la gestión de la seguridad de la información que incluye herramientas para la detección, análisis y solución de problemas de seguridad.

OpenVAS utiliza una amplia variedad de herramientas de escaneo de vulnerabilidades, incluyendo escaneos de puertos, análisis de aplicaciones web, detección de software malicioso y mucho más. La plataforma también ofrece informes detallados que pueden ser personalizados para adaptarse a las necesidades de cada organización.

OpenVAS es una herramienta valiosa para profesionales de seguridad informática y administradores de sistemas que buscan mejorar la seguridad de sus redes y aplicaciones. La plataforma es fácil de usar y se integra fácilmente con otras soluciones de seguridad, lo que la hace ideal para organizaciones de todos los tamaños. Sin embargo, es importante utilizar OpenVAS de manera ética y respetar las políticas de seguridad y privacidad de las redes y dispositivos que se escanean.

Para más información acceder a la siguiente URL https://www.openvas.org/

ExploitDB

ExploitDB Base de exploits de código abierto que recopila información sobre vulnerabilidades y explotaciones conocidas. Fue creada para ser una fuente confiable de información sobre seguridad para profesionales de seguridad informática e investigadores.

ExploitDB incluye información sobre una amplia variedad de sistemas y aplicaciones, desde sistemas operativos hasta software de aplicaciones web y de servidores. La base de datos se actualiza regularmente con nuevos exploits y se puede utilizar para investigar y detectar vulnerabilidades en los sistemas y aplicaciones.

ExploitDB es una herramienta valiosa para profesionales de seguridad informática y administradores de sistemas que buscan mantenerse informados sobre las últimas vulnerabilidades y explotaciones conocidas. La BD es de acceso libre y se puede utilizar para ayudar en la seguridad de los SO y aplicaciones, pero es importante utilizarla de manera ética y respetar las políticas de seguridad informática y confidencialidad y privacidad de los sistemas y aplicaciones que se investigan.

Para más información acceder a la siguiente URL https://www.exploit-db.com/

CVE

CVE (Common Vulnerabilities and Exposures) es un sistema de identificación estándar para vulnerabilidades informáticas. Fue creado por MITRE Corporation con el objetivo de proporcionar una base de datos centralizada y unificada para describir y clasificar vulnerabilidades informáticas.

Cada vulnerabilidad en el sistema CVE se identifica con un número único, conocido como identificador CVE, que permite a los profesionales de seguridad informática y a los investigadores de seguridad rastrear y rastrear fácilmente las vulnerabilidades. La información sobre las vulnerabilidades se actualiza regularmente en la base de datos de CVE para proporcionar información precisa y actualizada.

CVE es una herramienta valiosa para profesionales de seguridad informática y administradores de sistemas que buscan mantenerse informados sobre las últimas

vulnerabilidades conocidas. La base de datos es de acceso gratuito y se puede utilizar para mejorar la seguridad de los sistemas y aplicaciones, pero es importante utilizarla de manera ética y respetar las políticas de seguridad y privacidad de los sistemas y aplicaciones que se investigan.

Para más información acceder a la siguiente URL https://cve.mitre.org/

2.3 CONFIGURACIÓN DEL "BANCO DE TRABAJO"

Se hace la aclaración que se procede a configurar el banco de trabajo con las OVA de Windows 7 X86 y Windows 7 X64 no oficiales suministradas por el curso del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team - (202337164A_1435) para poder cumplir con la actividad.

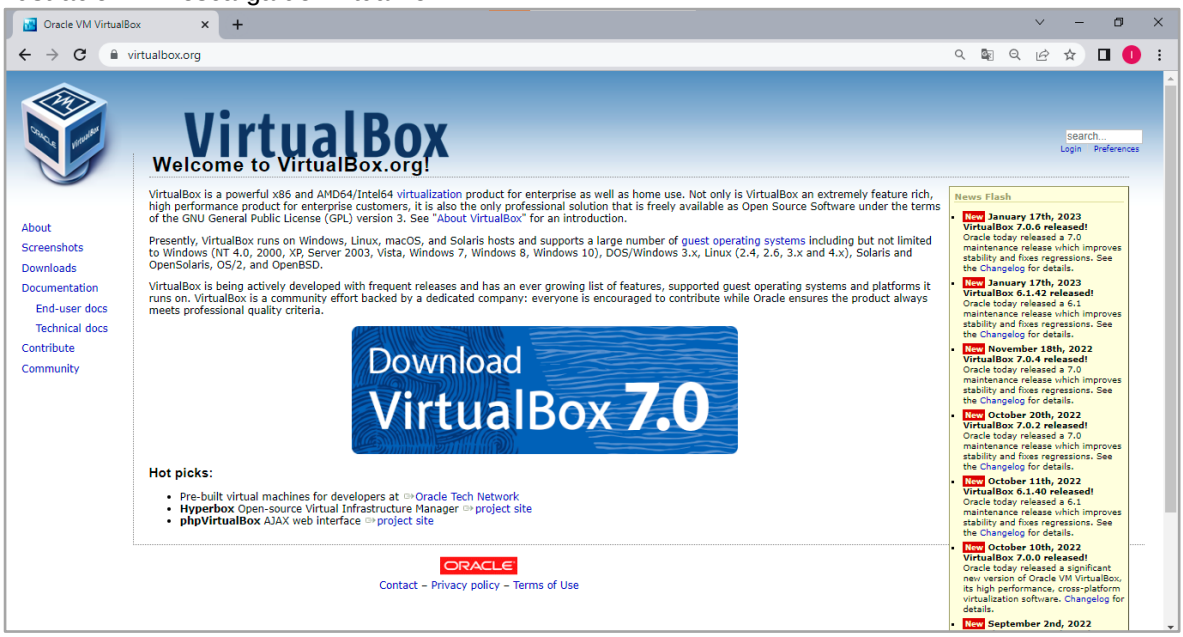
2.3.1 Instalación Virtualbox

VirtualBox es un programa de virtualización de sistemas operativos gratuito y de código abierto que permite ejecutar múltiples sistemas operativos en una sola máquina física. Esto permite a los usuarios probar y experimentar con diferentes sistemas operativos y aplicaciones sin tener que realizar cambios permanentes en su sistema operativo principal. Además, VirtualBox es útil para desarrolladores que desean probar su software en diferentes entornos sin tener que configurar múltiples máquinas físicas.

VirtualBox es compatible con una amplia variedad de sistemas operativos, incluyendo Windows, macOS, Linux y Solaris, y es fácil de usar, con una interfaz de usuario amigable y herramientas de configuración avanzadas.

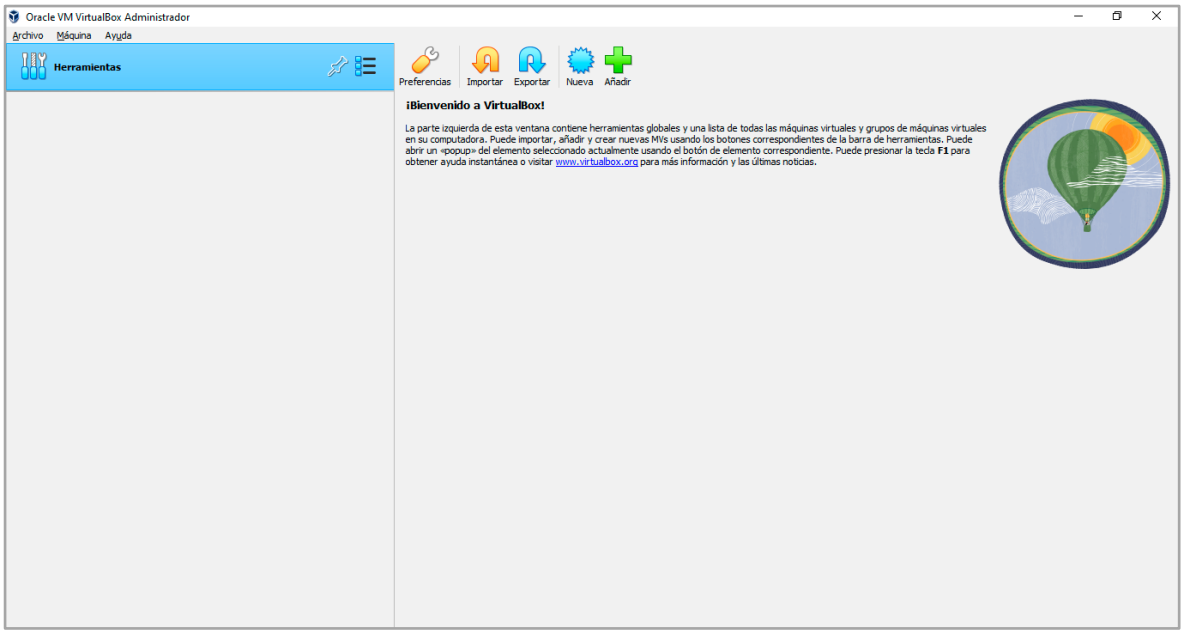
A continuación, se ejecuta la descarga de VirtualBox de la página oficial

Ilustración 1. Descarga de VirtualBox



Fuente: Propia (2023)

Ilustración 2. Instalación VirtualBox



Fuente: Propia (2023)

2.3.2 Instalación Windows 7 X86 Win7-SE2020 (Win7 32 bits)

Windows 7 es un sistema operativo desarrollado por Microsoft que fue lanzado en octubre de 2009. X86 se refiere a la arquitectura de 32 bits.

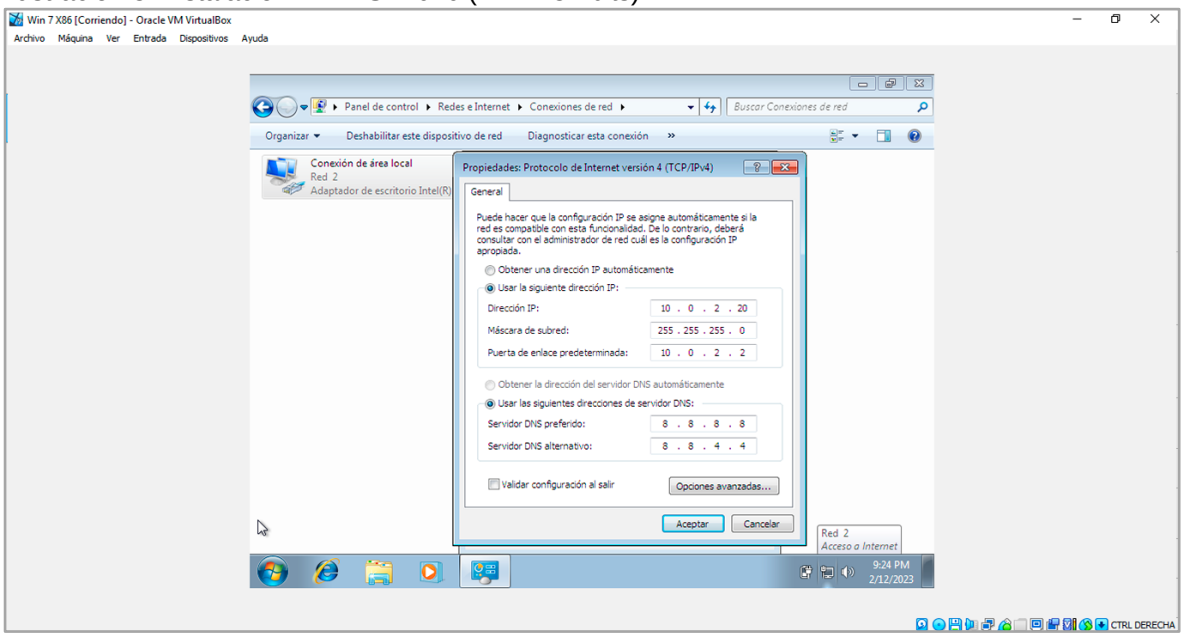
Windows 7 es un SO el cual cuenta con un entorno gráfico rediseñada y más intuitiva, con una barra de tareas más organizada y nuevas funciones de gestión de ventanas. También ofrece una mayor compatibilidad con hardware y software, una mejor seguridad y un rendimiento más rápido en comparación con su predecesor, Windows Vista.

Windows 7 incluye una amplia gama de características, incluyendo el Asistente para resolución de problemas, la recuperación de sistemas, la compatibilidad con múltiples monitores, la compatibilidad con touch, la reproducción de medios mejorada y la posibilidad de crear perfiles de usuario para diferentes miembros de una familia o empresa.

Aunque Microsoft ha dejado de dar soporte técnico a Windows 7 desde enero de 2020, todavía es un sistema operativo popular y ampliamente utilizado en todo el mundo. Sin embargo, se recomienda a los usuarios actualizar a un sistema operativo más reciente como Windows 11 para obtener las últimas características de seguridad y rendimiento.

Se configura la dirección IP: 10.0.2.20 en la máquina Windows 7 32 bits

Ilustración 3. Instalación Win7-SE2020 (Win 7 32 bits)



Fuente: Propia (2023)

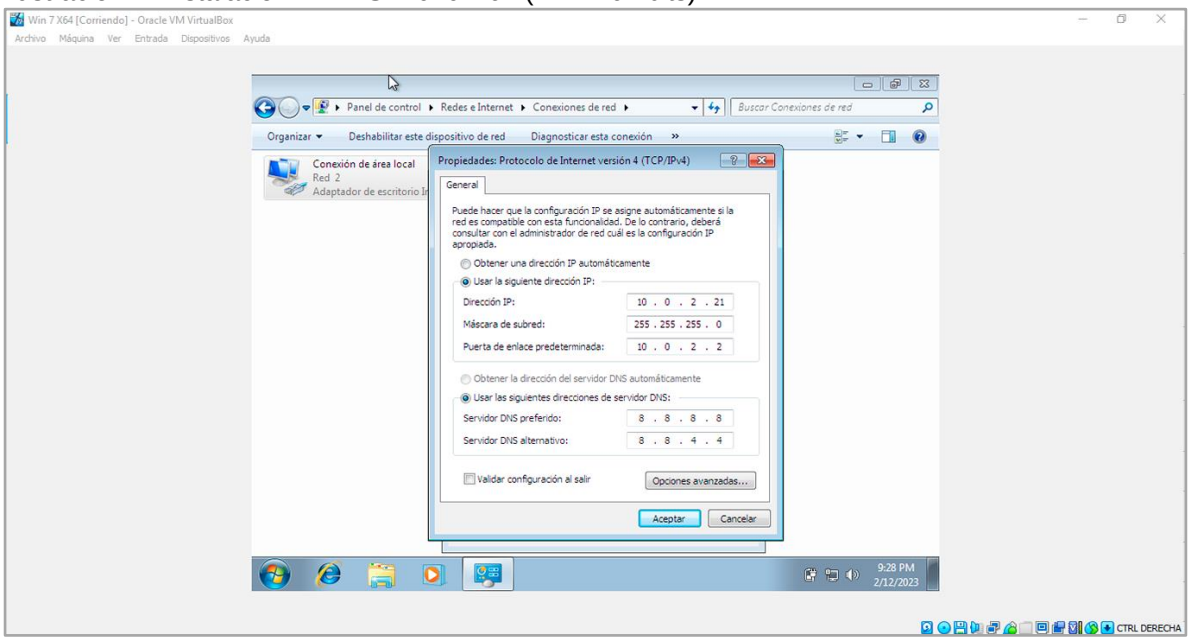
2.3.3 Instalación Windows 7 X64 Win7-SE2020-X64 (Win7 64 bits)

Windows 7 x64 Versión de 64 bits del SO Win 7. La principal diferencia entre la versión x86 y x64 de Windows 7 es la cantidad de memoria RAM que puede utilizar. La versión x64 permite una cantidad mayor de memoria RAM, lo que a su vez permite un rendimiento más rápido y una mayor capacidad para ejecutar aplicaciones más exigentes.

Además de esta diferencia, Windows 7 x64 ofrece las mismas características y funciones que la versión x86 de Windows 7, incluyendo una interfaz gráfica de usuario mejorada, compatibilidad con múltiples monitores, compatibilidad con touch, mejor reproducción de medios, posibilidad de crear perfiles de usuario y más. Sin embargo, es importante tener en cuenta que la versión x64 de Windows 7 solo es compatible con hardware y software de 64 bits. Si el computador está equipado con un procesador de 32 bits, no podrá instalar Windows 7 x64.

Se configura la Dirección IP: 10.0.2.21 en la máquina Windows 7 64 bits

Ilustración 4. Instalación Win7-SE2020-X64 (Win 7 64 bits)



Fuente: Propia (2023)

2.3.4 KALI LINUX

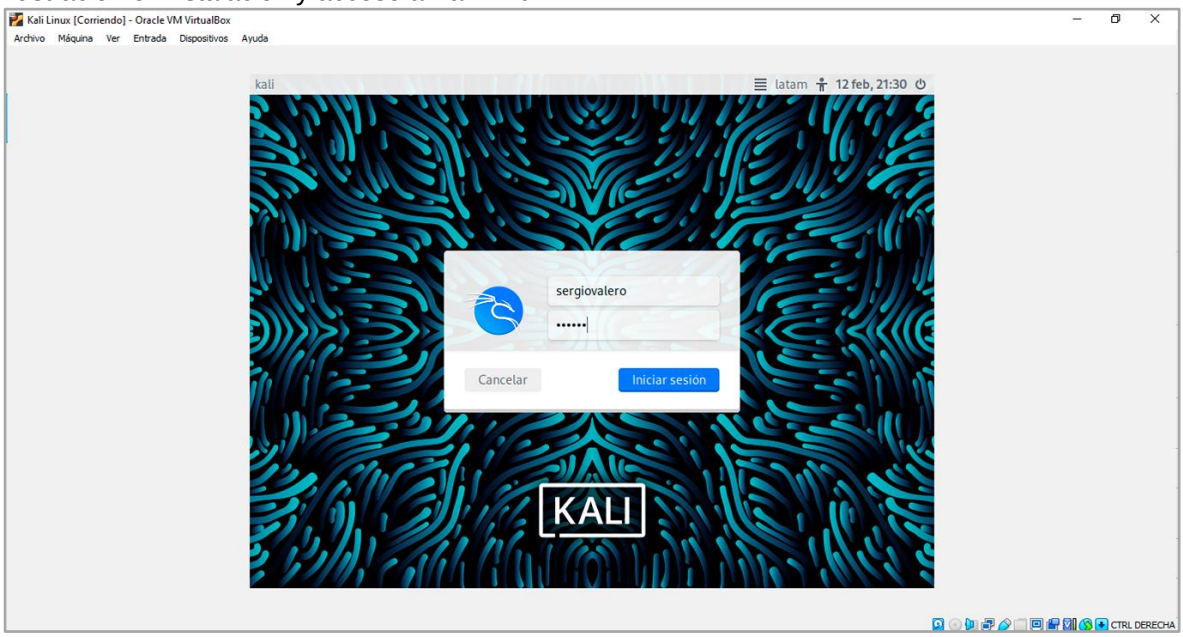
Sistema operativo diseñado para pruebas de penetración y seguridad informática. Desarrollado por Offensive Security y ampliamente utilizado por profesionales de la seguridad informática, investigadores de seguridad y entusiastas de la tecnología.

Algunas de las características y ventajas de Kali Linux incluyen:

- Amplia selección de herramientas de seguridad: Incluye más de 600 herramientas de seguridad, incluyendo Nmap, Metasploit, Aircrack-ng, etc.
- Personalización: Kali Linux permite a los usuarios personalizar y adaptar el sistema operativo a sus necesidades específicas.
- Documentación y comunidad en línea: Cuenta con una gran comunidad de usuarios y amplia documentación en línea que puede ayudar a los usuarios a resolver problemas y obtener más información sobre el sistema operativo.
- Actualizaciones frecuentes: Sistema operativo en constante desarrollo, con actualizaciones que incluyen nuevas herramientas y mejoras de seguridad.
- Gratuito y de código abierto: Es un sistema operativo de código abierto y gratuito, se puede descargar, usar y modificar el código fuente.

Se configura la Dirección IP: 10.0.2.22 en la máquina Kali Linux

Ilustración 5. Instalación y acceso a Kali Linux

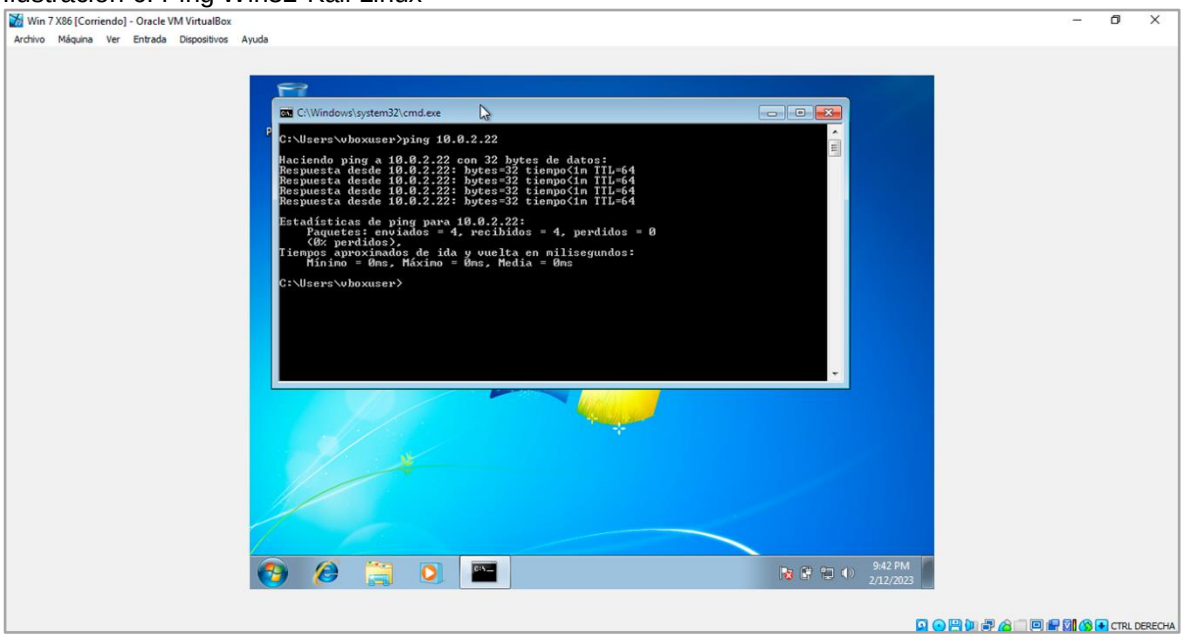


Fuente: Propia (2023)

2.3.5 Comunicación entre las maquinas del banco de trabajo

Se hace ping de la máquina Windows 7-32 Bits a Kali Linux.

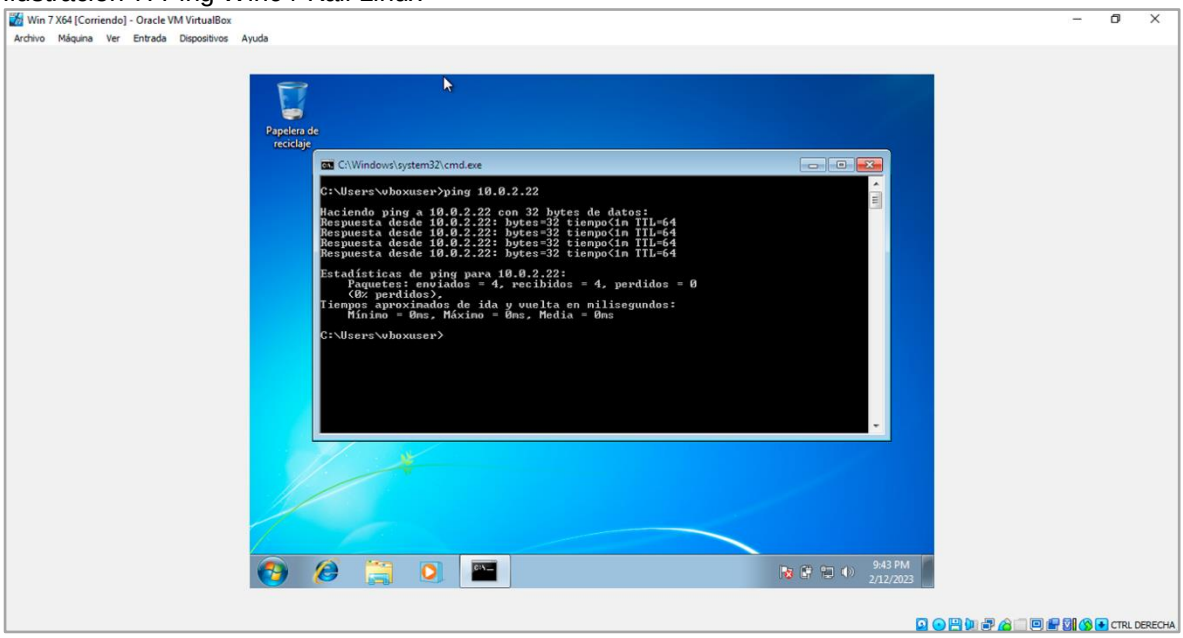
Ilustración 6. Ping Win32-Kali Linux



Fuente: Propia (2023)

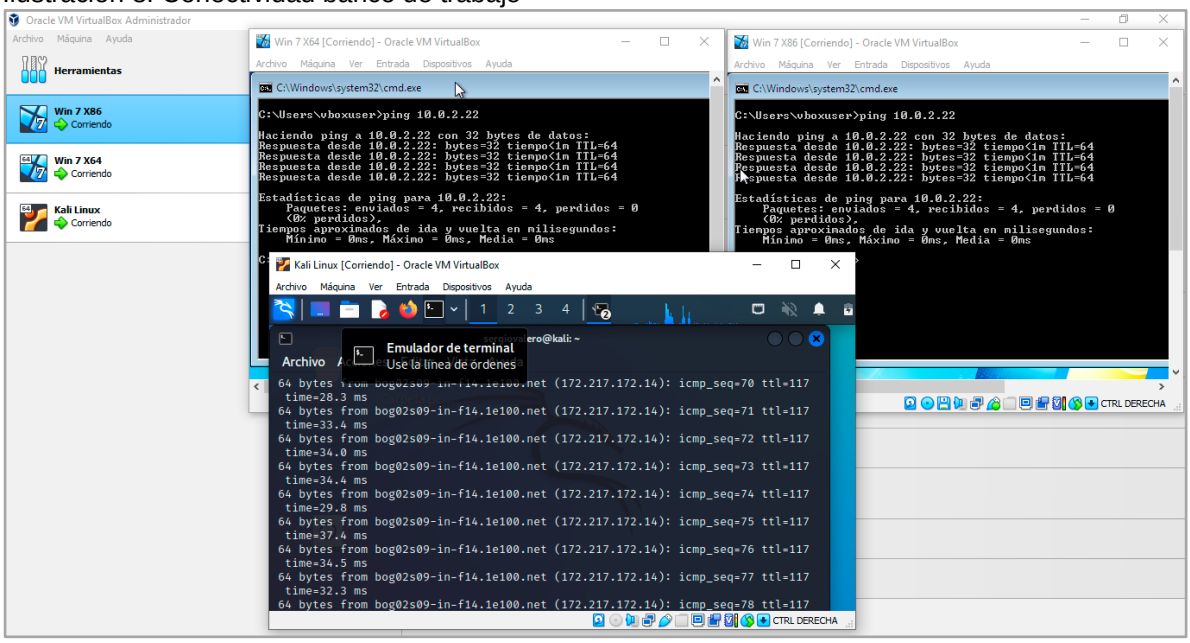
Se hace ping de la máquina Windows 7-64 Bits a Kali Linux.

Ilustración 7. Ping Win64-Kali Linux



Fuente: Propia (2023)

Ilustración 8. Conectividad banco de trabajo



Fuente: Propia (2023)

2.4 ACTUACIÓN ÉTICA Y LEGAL

A continuación, se desarrollará la Etapa 2 – Actuación ética y legal, el cual será la segunda fase del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

2.4.1 Análisis legal

Anexo 2 – Situación Problema – Análisis Legal.

A continuación, se transcribe la situación planteada del problema para su posterior análisis en el desarrollo de la actividad:

La organización WhiteHouse Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.

Para dar inicio, la organización WhiteHouse Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión “característica” de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

Al Analizar la situación problema en la organización WhiteHouse Security según la redacción anterior del anexo 2 – situación problema – análisis legal, en cuanto al reclutamiento de los miembros de los equipos Red team y Blue team, se procede a emitir un concepto técnico-legal en primera instancia acerca del mismo:

Siendo la organización WhiteHouse Security líder a nivel mundial en asesoría gubernamental en el mundo en procesos de ciberseguridad y ciberdefensa, y analizada la situación planteada del problema, esta presenta un error que no es permitido en una empresa de este tamaño corporativo a nivel mundial y es la evidencia que, primero la alta gerencia no es el área o grupo de profesionales designados para el análisis, revisión, modificación y/o aprobación de documentos legales en la empresa como se informa en anexo 2 – situación problema – análisis legal **"La alta gerencia no revisó los contratos"** ya que existe en la estructura jerárquica de la organización un área jurídica, quien es la encargada de las minutas de los contratos que se suscriben. Dicho lo anterior es un error de la alta gerencia hacer entrega de un documento sin el análisis, revisión, modificación y/o aceptación por parte del área jurídica de la empresa.

Segunda situación de análisis, en el anexo 2 – situación problema – análisis legal se transcribe **"el contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos"**, en el texto anterior se evidencia que el abogado fue retirado de su cargo por denunciar procesos irregulares en la organización mas no que el profesional fuera quien lo estuviera realizando, lo que se deduce es que fue despedido por descubrir un acto ilícito el cual significó el despido al parecer sin justa casusa por parte de su superior o la alta gerencia (supuesta teoría de despido de la organización del abogado).

Anexo 3 – Acuerdo de Confidencialidad

A continuación, se transcribe el acuerdo de confidencialidad como se encuentra formateado en el documento con extensión .pdf para un análisis legal y ético.

ACUERDO DE CONFIDENCIALIDAD ENTRE
NOMBRE DEL ESTUDIANTE Y WHITEHOUSE SECURITY

Por la parte reveladora
Nombre: The WhiteHouse Security Dirección: EE.UU
Teléfono: 1100011100
E-mail: Info@Thewhitehousesecurity.com
Por la **parte receptora de la información**
Nombre:
Dirección:
Teléfono:
E-mail:

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a Whitehouse Security, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del proceso de selección de personal.

2. Que la información de propiedad de Whitehouse Security Whitehouse Security ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal, nombre estudiante que para el presente caso actual como revelador, guarda y administrados de la información de propiedad de Whitehouse Security.

En consecuencia, las partes se suscriben a las siguientes cláusulas:

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

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

1. La información que no sea pública y sea conocida por la parte receptora con ocasión del proceso de selección de personal.

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”.

parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

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

Cuarta. Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:
De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:
1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.
2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Whitehouse Security, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.
3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
4. Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
5. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
6. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.
7. Responder por el mal uso que le den sus representantes a la **información confidencial.**
8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.
9. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security.
Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.
Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:
1. Mantener la reserva de la **información confidencial** hasta tanto
Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.
Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos

alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.
Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.
Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente Acuerdo y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los (xxx) días del mes de (xxx) de 201_

Una vez analizado el anterior documento de confidencialidad para el reclutamiento de los equipos Red team y Blue team, se procede a emitir un concepto ético y legal acerca del mismo discriminado este por clausulas:

Cláusula primera. Objeto: En el documento de confidencialidad se transcribe: "en virtud del presente **acuerdo de confidencialidad**, la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, **la información confidencial** o sobre ***procesos ilegales*** dentro de Whitehouse Security no podrán ser divulgados."
Observaciones a la cláusula: La empresa no podrá coaccionar a la parte receptora a través de un documento acuerdo de confidencialidad a encubrir a la empresa en procesos ilegales que este evidencie o que la autoridad competente lo requiera en parte de un proceso legal. De igual forma restringe mediante este documento cualquier tipo de denuncia ante las autoridades locales, nacionales e internacionales.

Cláusula segunda. Punto 2. En el acuerdo de confidencialidad se transcribe que es información confidencial o secreto: "Cualquier dato secreto como **"*datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos*.** Por la parte receptora que tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados."

Observaciones a la cláusula: La empresa no podrá coaccionar a la parte receptora a través de un documento acuerdo de confidencialidad a encubrir a la empresa en procesos ilícitos, los cuales están tipificados en las siguientes leyes, Ley 1273 de

2009 o ley de delitos informáticos, Ley 1273 de 2009[11], Decreto 1377 de 2013[12] y la Ley 1581 de 2012[13].

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

Observaciones a la cláusula: La empresa no podrá reconocer información confidencial como suya si la misma es obtenida a través de forma ilegal ya que se estaría incurriendo en un delito informático el cual se encuentra tipificado en la Ley 1273 de 2009, el Decreto 1377 de 2013 y la Ley 1581 de 2012, y demás leyes y tratado internacionales que se apliquen como consecuencia del ilícito para su obtención.

Cláusula cuarta. Punto 3: En el documento de confidencialidad se transcribe: **"*No denunciar ante las autoridades actividades sospechosas de espionaje*** o cualquier otro proceso en el cual intervenga la apropiación de información de terceros. **Punto 4:** Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas."

Observaciones a la cláusula: La empresa no podrá coaccionar a la parte receptora a través de un documento acuerdo de confidencialidad a encubrir a la empresa en procesos ilícitos, los cuales están tipificados en las siguientes leyes, Ley 1273 de 2009 o ley de delitos informáticos, Ley 1273 de 2009, Decreto 1377 de 2013 y la Ley 1581 de 2012 y demás leyes y tratados internacionales que se apliquen como consecuencia del ilícito para su obtención. A demás de encubrir a la empresa en prácticas delictivas, la parte receptora de la información conociendo del hecho, este

[11] Secretaría del Senado. (2022) *Ley 1273 de 2009.* Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/arbol/1000.html

[12] Función Pública. (n.d.) *Decreto 1377 de 2013.* Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646#:~:text=Se%C3%B1ala%20lo%20relacionado%20con%20el,al%20tratamiento%20de%20datos%20personales

[13] Función Pública. (n.d.) *Ley 1581 de 2012.* Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

no lo denuncia lo cual lo hace cómplice del mismo bien sea por omisión y/o acción si esta información la parte receptora la publica conociendo los medios por el cual se apropiaron de la información.

Cláusula cuarta. Punto 7: En el documento de confidencialidad se transcribe: **"*Responder por el mal uso que le den sus representantes a la información confidencial*."**

Observaciones a la cláusula: La parte receptora no es solidaria en responsabilidades por el mal uso que la empresa haga de la información confidencial que ella posea, siempre y cuando se no demuestre lo contrario en un juicio.

Cláusula Cuarta. Punto 8: En el acuerdo de confidencialidad se transcribe: **"*Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento*."**

Observaciones a la cláusula: La parte receptora sí posee información confidencial, esta deberá responder ante la autoridad. Si esta no fue obtenida de forma licita, deberá demostrar 1. Que ella no la obtuvo, sino que le fue entregada por la empresa, lo cual deberá demostrarlo en un juicio de responsabilidades ante un juez y 2. Que aun sabiendo que era poseedor de la información ¿por qué no denunció el ilícito si este era de su conocimiento? Lo cual lo hace responsable de la información que se encuentra en su poder.

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

Observaciones a la cláusula: La parte receptora está obligada en la cláusula de confidencialidad a no revelar parcial o total información confidencial de la organización, sin embargo, no es ético y menos aún legal encubrir a la empresa en actos ilícitos como es la obtención de información confidencial obtenida de forma ilegal sabiendo que es un delito y esta mediante una cláusula pretenda que la receptora la encubra lo cual si lo hace, la hace cómplice de un delito informático.

Cláusula quinta. Punto 1: En el documento de confidencialidad se transcribe: **"*Mantener la reserva de la información confidencial hasta tanto*".**

Observaciones a la cláusula: En esta cláusula la información al parecer se encuentra incompleta o eliminada intencionalmente ya que no es coherente la finalización de la misma o que se quiere transmitir en el párrafo. De igual forma, se evidencias espacios entre líneas lo que se puede interpretar como espacios en blanco para transcribir información a conveniencia en caso de ser necesaria.

Cláusula sexta. Responsabilidad: En el acuerdo de confidencialidad se transcribe: **"*la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo***, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas."

Observaciones a la cláusula: De acuerdo a la cláusula anterior, con la firma del documento de confidencialidad, la parte receptora se somete a las condiciones laborales tanto licitas como ilícitas por parte de la parte reveladora en este caso la organización Whitehouse Security.

Cláusula séptima. No existe esta cláusula en el documento de confidencialidad entregado por la organización, sin embargo, hay un espacio interlineado el cual se podría prestar para redactarla en caso de ser conveniente para la organización.

Cláusula octava. Responsabilidad: En el acuerdo de confidencialidad se transcribe: **"*En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security*."**

Observaciones a la cláusula: De acuerdo a la cláusula anterior, con la firma del documento de confidencialidad, la empresa no se hace responsable de los ilícitos en los que ella incurra y deja por escrito, quien responde es la parte receptora eximiendo de responsabilidades civiles y penales a la organización lo cual no es ético ni legal aun sabiendo que es culpable de delitos que cometerá dejándolo implícitamente claro en el acuerdo de confidencialidad.

Validando el documento de confidencialidad, como un todo, son claros los procesos ilegales y no éticos en la redacción del documento descritos en los párrafos anteriores y a eso hay que agregar que se evidencian gran cantidad de espacios entre líneas lo que se puede interpretar como espacios en blanco para anexar información a conveniencia en caso de ser necesaria.

De igual forma hay una redacción que no es acorde en un documento legal de una empresa como WhiteHouse Security, organización con reconocimiento a nivel mundial el cual cuenta con un departamento jurídico que tiene en su equipo jurídico profesionales de la más alta calidad.

La recomendación es no firmar el acuerdo de confidencialidad redactado por organización Whitehouse Security, para el reclutamiento de sus equipos Red team y Blue team ya que este se encuentra explícitamente elaborado con el único fin que los miembros de los equipos en caso de una investigación judicial estos sean los responsables de cualquier hallazgo que encuentren las autoridades.

Anexo 3 – Vulneración Ley 1273 de 2009 - Acuerdo de Confidencialidad

Cláusula primera. En el documento de confidencialidad, cláusula primera no se vulneran artículos de la ley 1273 de 2009 o ley de delitos informáticos ya que él documento cita "**la información confidencial** o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados". La frase procesos ilegales es amplia y no hace referencia específica sobre delitos informáticos.

Cláusula segunda. En el documento de confidencialidad redactado por organización Whitehouse Security, cláusula segunda se vulneran los siguientes artículos de la ley 1273 de 2009 o ley de delitos informáticos ya que él documento cita "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

Artículo 269A. ***ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.*** Se vulnera este artículo ya que se accesa al sistema sin autorización a un sistema informático en contra de la voluntad del poseedor de la información.

Artículo 269C. ***INTERCEPTACIÓN DE DATOS INFORMÁTICOS***. Vulnera el presente artículo ya que se intercepta un sistema sin orden judicial a un sistema informático.

Artículo 269F. ***VIOLACIÓN DE DATOS PERSONALES****.* Vulnera el presente artículo ya que se obtiene o sustrae información de datos personales y/o confidenciales para el beneficio de la organización.

Artículo 269H. ***CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA:*** Se puede inferir que hay agravante ya que se revelará o entregará el contenido de la información en perjuicio de otro, provecho para la organización o un tercero.

Cláusula tercera. En el acuerdo de confidencialidad redactado por organización Whitehouse Security, cláusula tercera no se vulneran artículos de la ley 1273 de 2009 o ley de delitos informáticos.

Cláusula cuarta. En el acuerdo de confidencialidad redactado por organización Whitehouse Security, punto 3 y punto 4 se vulneran todos los artículos de la ley 1273 de 2009 o ley de delitos informáticos ya que él documento cita “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.” Se entiende que al aceptar firmando el acuerdo de confidencialidad, es cómplice al no denunciar ya que, al hablar de espionaje, la forma de obtener información de terceros de forma ilícita es mediante técnicas conocidas y no conocidas utilizadas por delincuentes informáticos lo cual harán que se vulneren los artículos de la ley 1273 de 2009 y demás leyes nacionales e internacionales según el origen u origen de la información obtenida ilegalmente.

Cláusula décima. En el documento de confidencialidad, al aceptar firmarlo se vulneran todos los artículos de la ley 1273 de 2009 o ley de delitos informáticos ya que él documento se encuentra redactado para que, la parte receptora de la información e caso de una investigación sea la única responsable de la conducta ilícita de la organización.

Aceptación o No del Acuerdo de Confidencialidad.

Existiendo procesos poco confiables en el anexo 3 – Acuerdo, usted como experto en ciberseguridad ¿Aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

Es claro que la Organización The WhiteHouse, no tiene definido en sus procesos contractuales como marco legal, la legislación sobre delitos informáticos ni la ética de los profesionales que contratará ya que ellos al firmar aceptarán de forma explícita que vulnerarán entre otras leyes nacionales e internacionales, la Ley 1273 de 2009 sobre delitos informáticos, Decreto 1377 de 2013 sobre protección de datos personales, la Ley 1581 de 2012 sobre protección de datos personales y el código de ética del ingeniero (Consejo Profesional Nacional de Ingeniería - COPNIA[14]).

Cabe resaltar que los siguientes capítulos, CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES. ARTÍCULO 32. PROHIBICIONES GENERALES A LOS PROFESIONALES, del código de ética del ingeniero no serán tenidos en cuenta a la hora de firmar el acuerdo de confidencialidad entre el profesional y Whitehouse Security.

Sí bien es cierto que existe un marco legal del comportamiento del profesional, para este caso, el código de ética del Consejo Profesional Nacional de Ingeniería - COPNIA (para ingenieros y sus profesiones afines o auxiliares), el cual regula la profesión, de igual forma existe la ética propia de cada individuo como persona que por más estudios que tenga, legislación que regule la profesión o leyes civiles y/o penales, esta se tiene o no!

Expuesto lo anterior no aceptaría la propuesta de trabajo ofrecida por la Empresa Whitehouse Security ya que eso sería aceptar una condena judicial, económica y profesional anticipada y la segura perdida de la tarjeta profesional.

2.4.2 Caso Operación Andrómeda Buggly

A continuación, se analizará el caso “Operación Andromeda Buggly” desde el punto de vista del autor del presente informe, con relación a las implicaciones legales y éticas.

Antes de analizar el caso “Operación Andromeda Buggly”, definiremos que es “Buggly”; Una construcción de dos plantas ubicado en el barrio Galerías, zona residencial y comercial de la ciudad de Bogotá, en el cual en su primera planta funcionaba un restaurante y en la segunda planta funcionaba una empresa cuyo nombre o razón social era BUGGLY, un hackerspaces con equipos tecnológicos de

[14] COPNIA (2023). *Código de ética.* Recuperado de https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

última tecnología en donde se reunía una comunidad de hacking ético y seguridad informática, para realizar capacitaciones, conferencias y entrenamiento sobre hacking ético; como resultado de la Operación Andromeda Buggly, se evidenció que realmente era una fachada para interceptación ilegal del Ejército Colombiano financiado con los gastos reservados del ejército y el cual tenía como propósito reclutar civiles expertos en hacker y/o proyección del mismo.

Ilustración 9. Hackerspace Buggly

Fuente: https://www.noticiasrcn.com/nacional-justicia/juez-declara-legal-captura-militares-caso-andromeda

Los cibercriminales contaban con un software que interceptaba comunicaciones de propiedad y utilización limitada solo al gobierno y software malicioso obtenido a través del llamado “mercado negro”. Estos softwares permitían a los cibercriminales acceder a datos personales y financieros de usuarios para vender información y bases de datos en el mercado negro, utilizarlas en transacciones fraudulentas, como método de espionaje para obtener información de las Farc y ELN en el territorio nacional, información de las FARC en la Habana (Cuba), información de las bases de datos de desmovilizados y acaldes de la zona del Catatumbo para utilizarlas en contrainteligencia del ejército nacional.

Desde un punto de vista operacional e investigativo, la Operación Andrómeda Buggly fue un éxito en la lucha contra el cibercrimen, ya que permitió la detención de civiles y militares, así como la desarticulación de una red nacional e internacional de cibercriminales financiado por las fuerzas militares de Colombia (Ejército de

Colombia). Sin embargo, es importante tener en cuenta las implicaciones legales y éticas a futuro de las acciones realizadas por parte de la red de hackers, ya que la privacidad y seguridad de usuarios, instituciones nacionales y gobiernos extranjeros fueron vulneradas; aquí en Colombia se vulneraron además de leyes penales y civiles, la Ley 1273 de 2009 sobre delitos informáticos, Decreto 1377 de 2013 sobre protección de datos personales, la Ley 1581 de 2012 sobre protección de datos personales entre otras leyes y tratados internacionales.

La Operación Andrómeda Buggly dejó en evidencia la necesidad de una cooperación de todas las fuerzas del estado colombiano, así como internacional en la lucha contra el cibercrimen, siendo esta un ejemplo de la importancia de la lucha contra la ciberseguridad en el mundo actual y de la urgente necesidad de capacitación, colaboración e intercambio de recursos humanos y de tecnología para hacer frente a las amenazas cibernéticas que crecen de forma exponencial en un mundo cada vez más digital.

2.5 EJECUCIÓN DE PRUEBAS DE INTRUSIÓN

A continuación, se desarrollará la Etapa 3 – Ejecución pruebas de intrusión, tercera fase del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

Análisis de anexos

Anexo 2 – Situación Problema – Analisis Red Team.

A continuación, se transcribe el texto entregado por el curso de la situación planteada del problema para su posterior análisis en el desarrollo de la actividad:

“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 llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta

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

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos."

Para desarrollar el presente informe, se presentan las máquinas activas en el banco de trabajo con las OVA de Windows 7 X86 y Windows 7 X64 suministradas por el curso, con sus Ip configuradas.

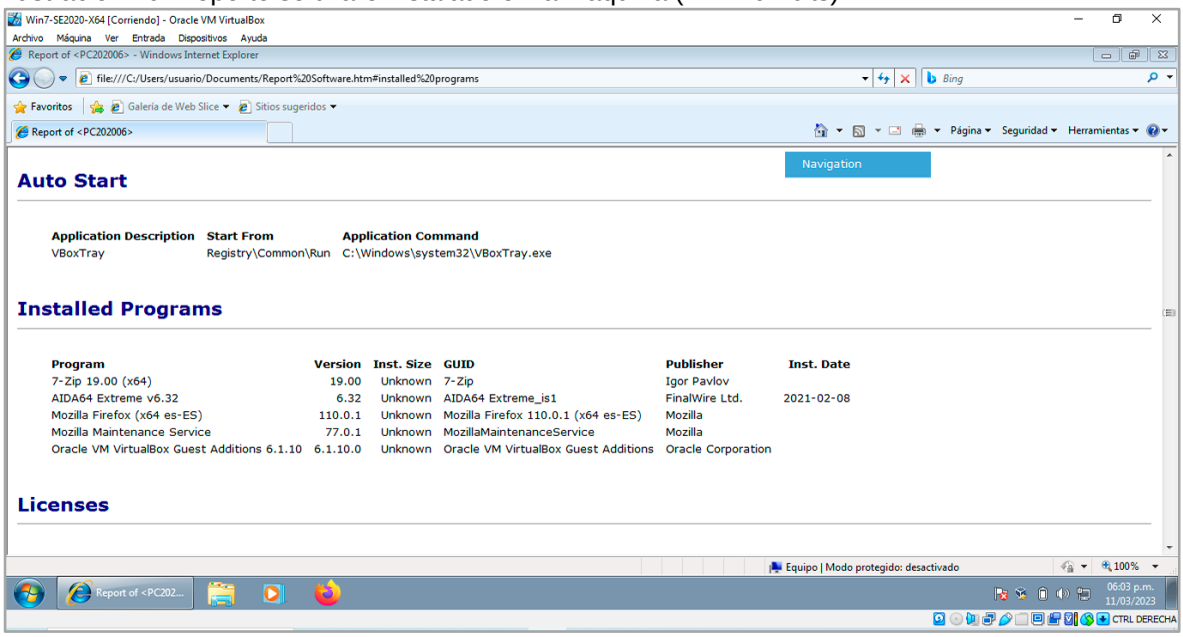
Win7-SE2020 (Win 7 32 bits) IP: 10.0.2.20 en la máquina Windows 7 32 bits
Win7-SE2020-X64 (Win 7 64 bits) IP: 10.0.2.21 en la máquina Windows 7 64 bits
KALI LINUX IP: 10.0.2.22 en la máquina Kali Linux

Situación problema – rejetto V 2.3

Al analizar la situación del problema, este plantea Anexo 2 – Situación Problema – Analisis Red Team, lo siguiente "La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter".

Lo primero es analizar la máquina Win7-SE2020-X64 (Win 7 64 bits), validando que la aplicación rejetto v. 2.3 se encuentre instalada en ella, para esto se utiliza el software AIDA64_Extreme_6.32.5600 con el cual generamos un reporte de las aplicaciones instaladas en el equipo.

Ilustración 10. Reporte software instalado en la máquina (Win7 64 bits)



Fuente: Propia (2023)

Informe de aplicaciones instalados en la máquina Win7-SE2020-X64 (Win 7 64 bits):

- 7-Zip 19.00 (x64)
- A10A64 Extreme v6.32
- Morilla Firefox (x64 os* ES)
- Mordía Mawitenance Service
- Oracle VM VirtualBox Guest Addibons 6.1.10

Se evidencia la no instalación de la aplicación rejetto v. 2.3 en la maquina Win7-SE2020-X64 (Win 7 64 bits), OVA enviada por el Ing. John F. Quintero T. - Director de curso a través del correo del seminario, motivo por el cual no se puede realizar el análisis al requerimiento del Anexo 2 – Situación Problema – Analisis Red Team.

2.5.1 Recopilación, planificación y preparación

Para dar inicio al proceso, se realiza un escaneo de red para establecer maquinas activas, sistemas operativos, direcciones IP y puertos abiertos. Para realizar el proceso utilizaremos la herramienta nmap[15] con el cual conoceremos la información (Hardware y Software) en cada máquina de la red.

[15] Escribir nota https://nmap.online/es/nmap-commands

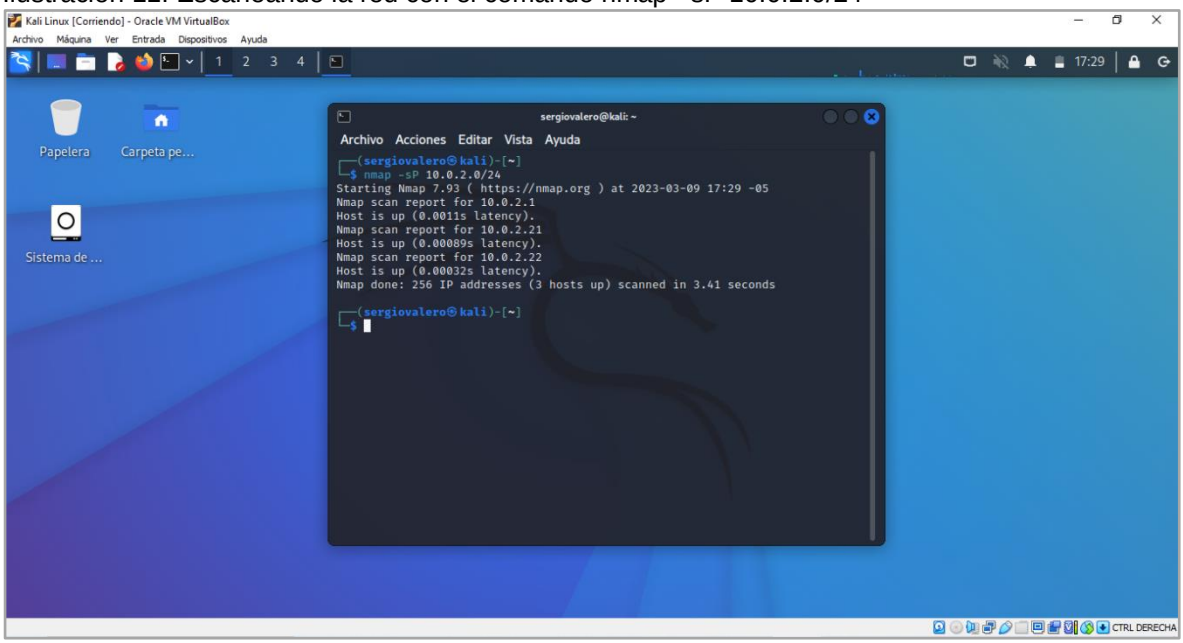
Comandos de consola utilizados en el desarrollo de exploración y penetración de vulnerabilidades.

nmap –sP 10.0.2.0/24

Evidencia

Se identifican las siguientes tres Ip activas: 10.0.2.1 - 10.0.2.21 - 10.0.2.22

Ilustración 11. Escaneando la red con el comando nmap –sP 10.0.2.0/24



Fuente: Propia (2023)

2.5.2 Investigación y análisis vulnerabilidades

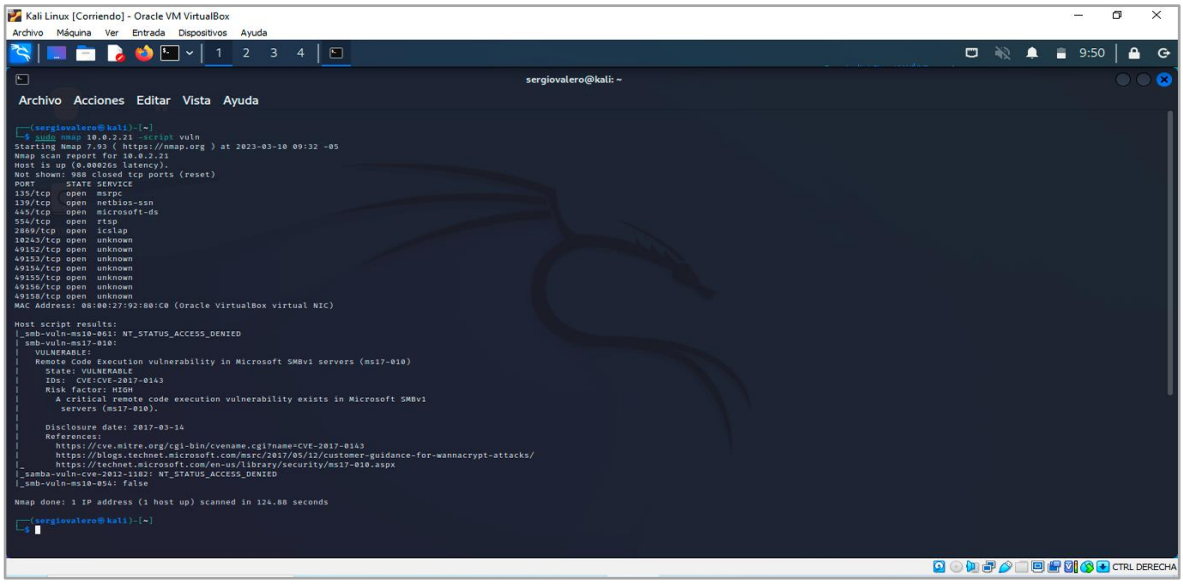
En el siguiente bloque se ejecutarán los siguientes comandos de consola para la exploración y penetración de vulnerabilidades.

sudo nmap 10.0.2.21 -script vuln

Evidencia

PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
smb-vuln-ms17-010:
VULNERABLE:
Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
State: VULNERABLE
IDs: CVE:CVE-2017-0143
Risk factor: HIGH
A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).

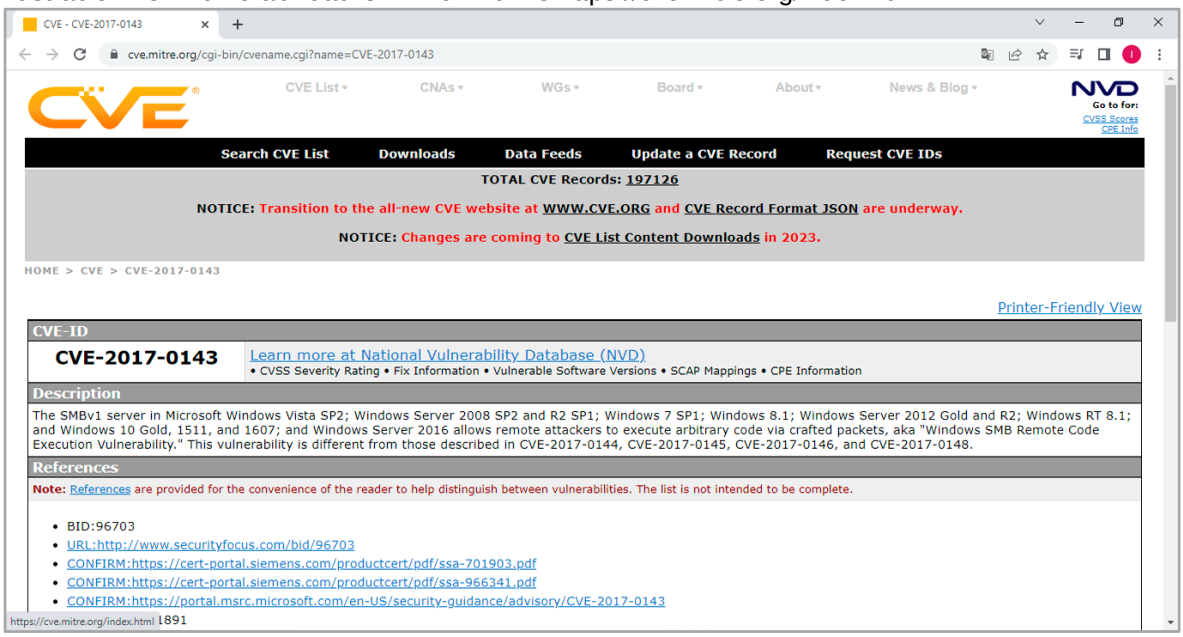
Ilustración 12. Análisis de vulnerabilidades



Fuente: Propia (2023)

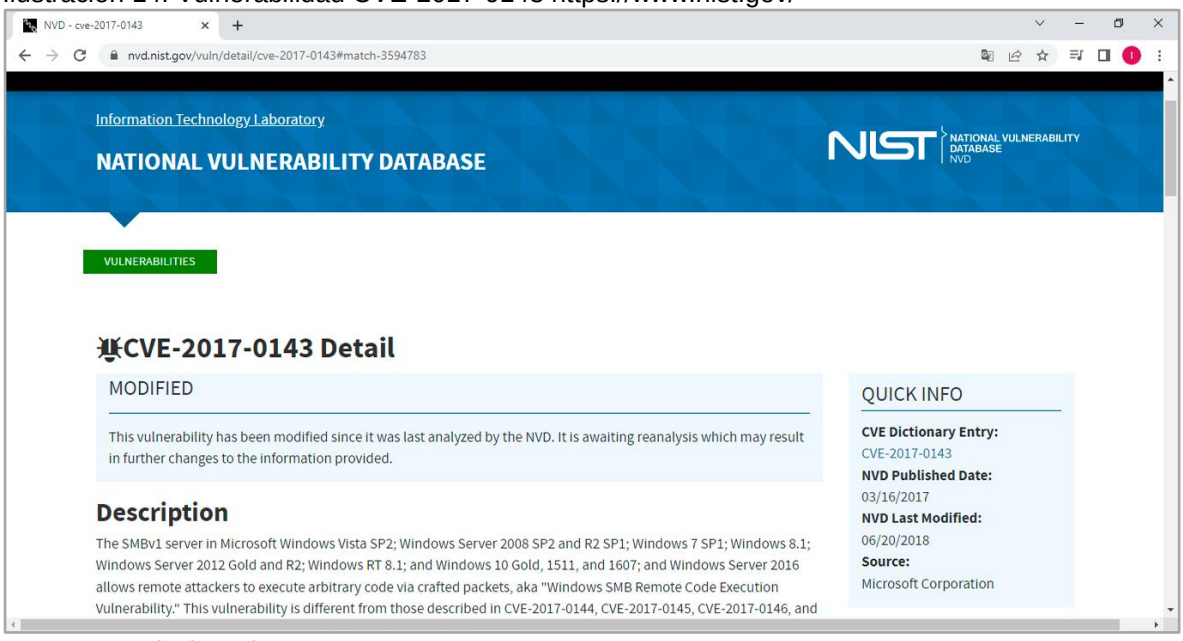
A continuación, se hace una recopilación de información acerca de las vulnerabilidades evidenciadas con la herramienta nmap.

Ilustración 13. Vulnerabilidad CVE-2017-0143 https://cve.mitre.org/index.html



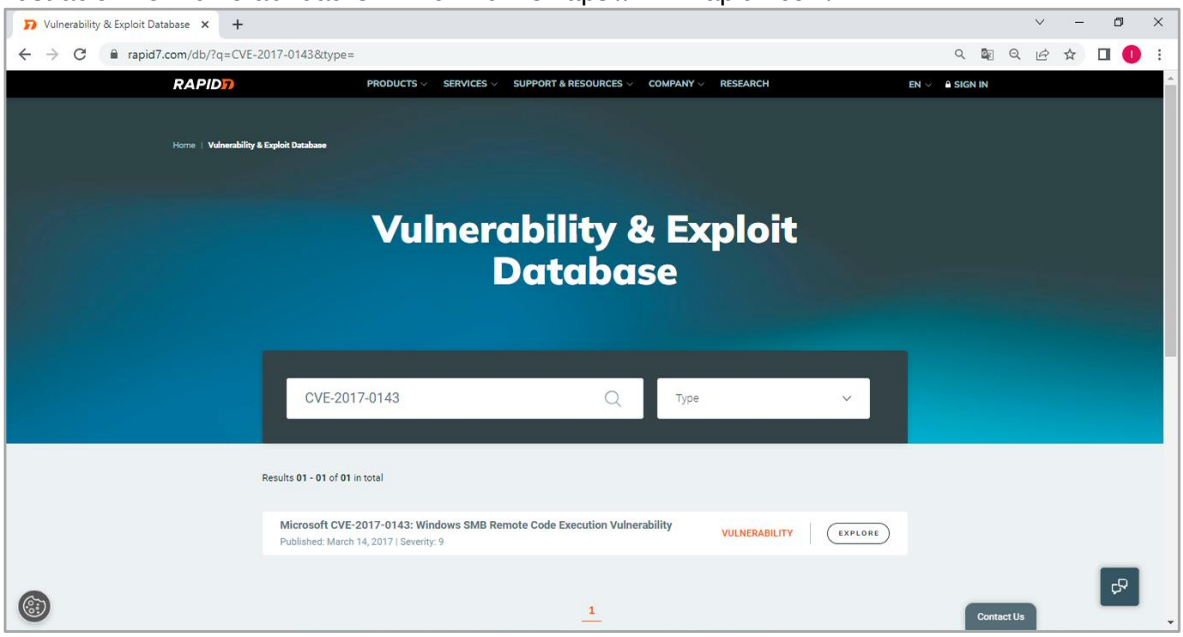
Fuente: Propia (2023)

Ilustración 14. Vulnerabilidad CVE-2017-0143 https://www.nist.gov/



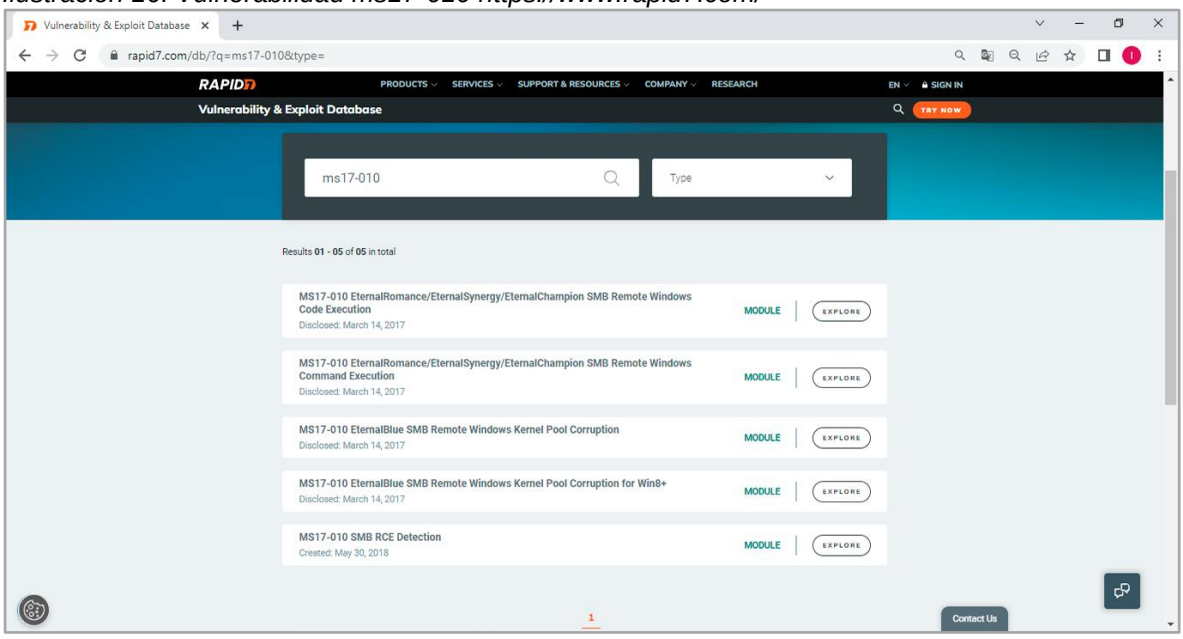
Fuente: Propia (2023)

Ilustración 15. Vulnerabilidad CVE-2017-0143 https://www.rapid7.com/



Fuente: Propia (2023)

Ilustración 16. Vulnerabilidad ms17-010 https://www.rapid7.com/



Fuente: Propia (2023)

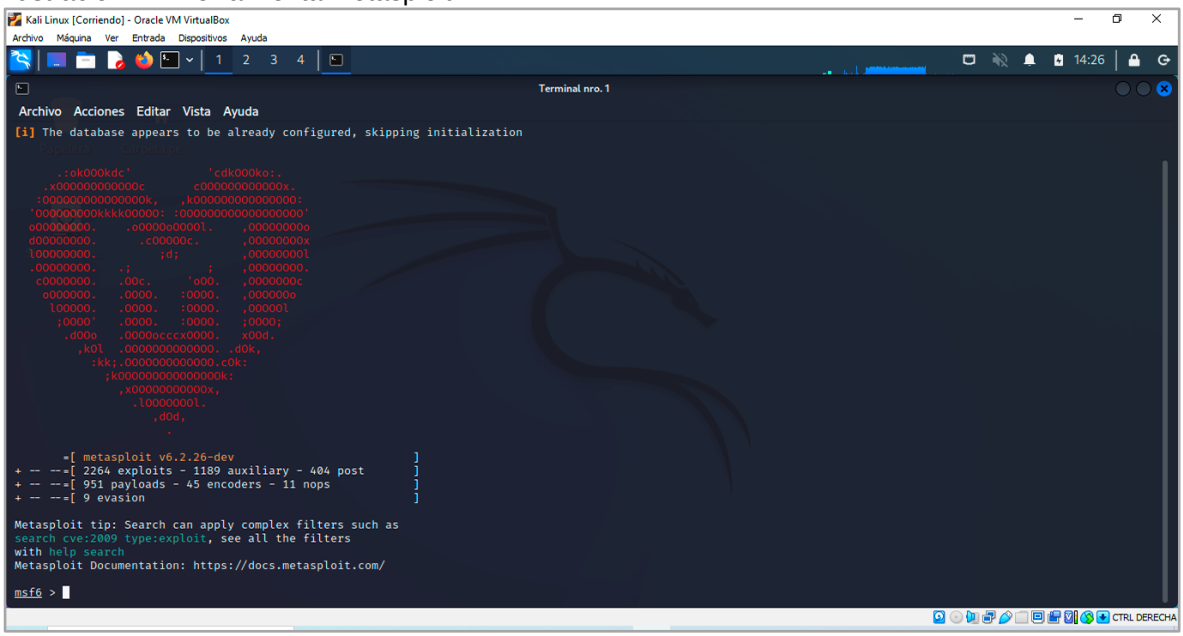
2.5.3 Penetración y explotación de vulnerabilidades

En el siguiente bloque se utilizará una herramienta para ejecutar exploits en la maquina remota con vulnerabilidades **IDs: CVE:CVE-2017-0143** servers (ms17-010) como es Metasploit, Meterpreter ejecutará un payload para realizar acciones en el equipo remoto y en el último paso el Shell obteniendo información.

Comandos de consola utilizados en el siguiente bloque.

metasploit framework

Ilustración 17. Herramienta Metasploit



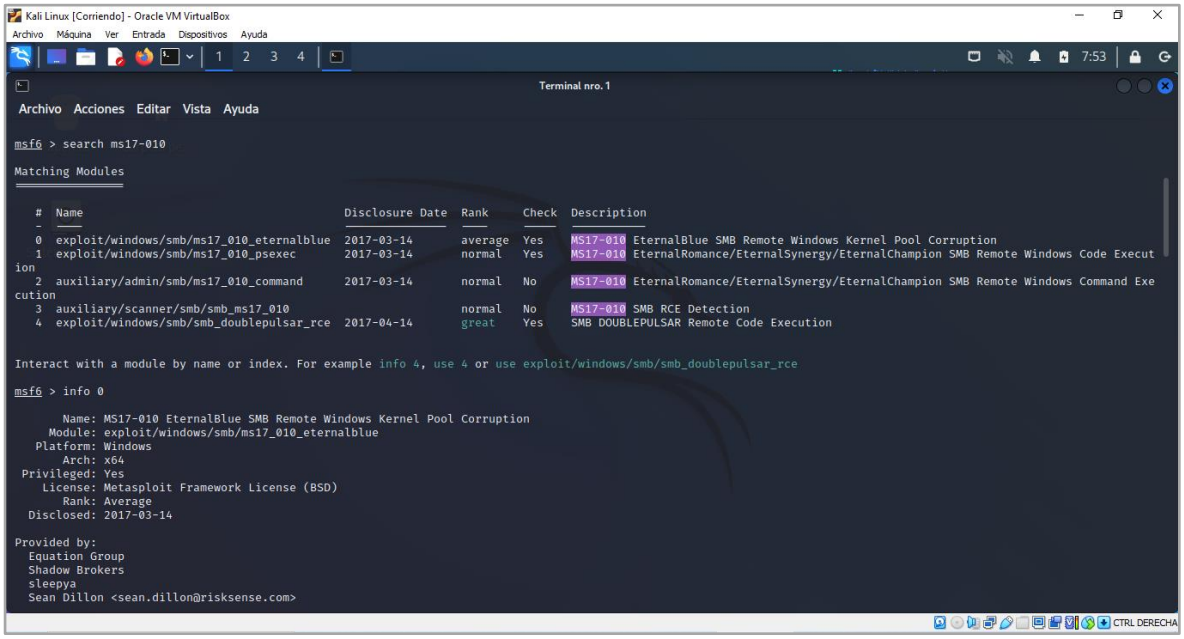
Fuente: Propia (2023)

search ms17-010

Evidencia

Id 0
Nombre exploit/windows/smb/msl7_010_eternalblue
Descripción MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

Ilustración 18. Comando search ms17-010



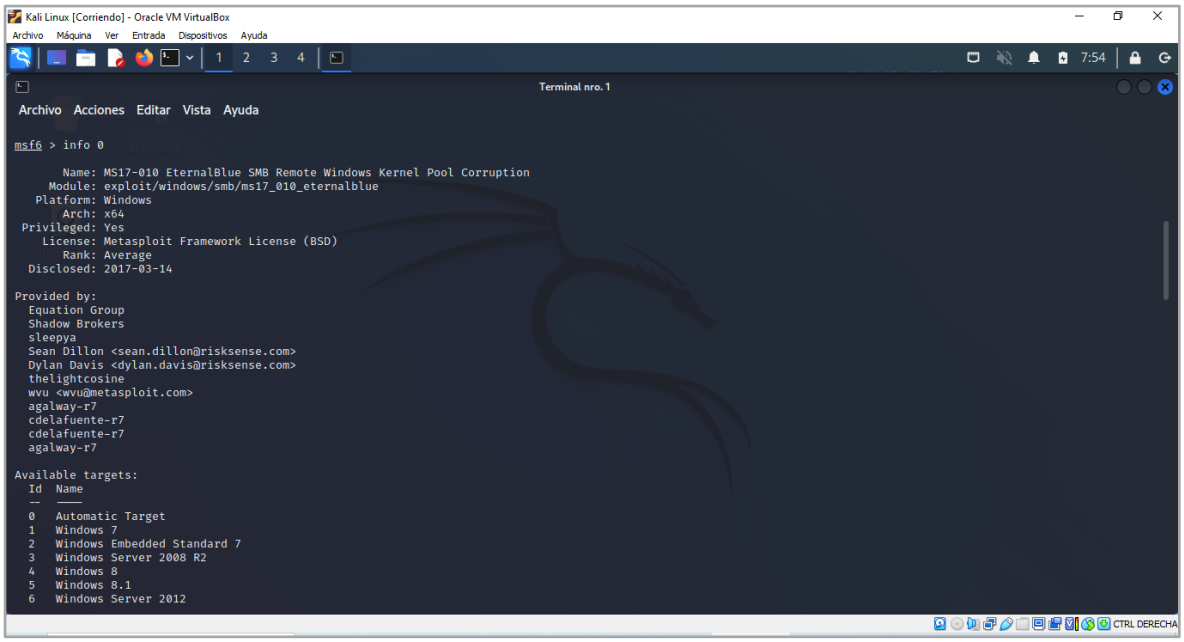
Fuente: Propia (2023)

Info 0

Evidencia

Información del Id 0

Ilustración 19. Comando info 0



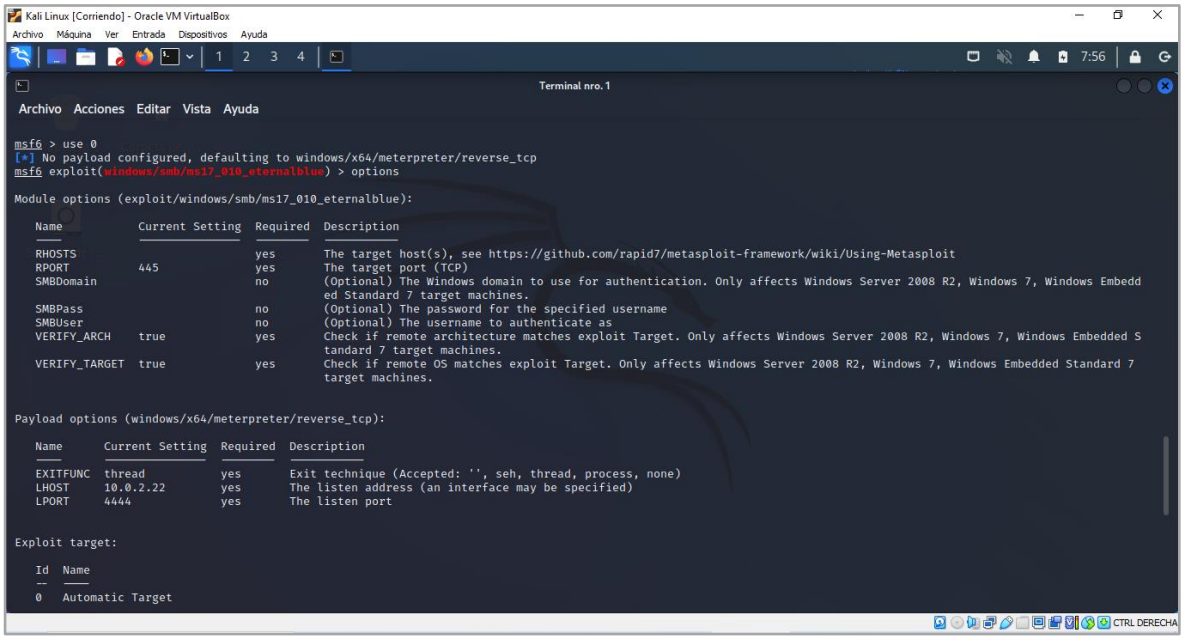
Fuente: Propia (2023)

Use 0

Evidencia

Se selecciona el Id 0. No se configura el Payload, se toma el que viene configurado por defecto.

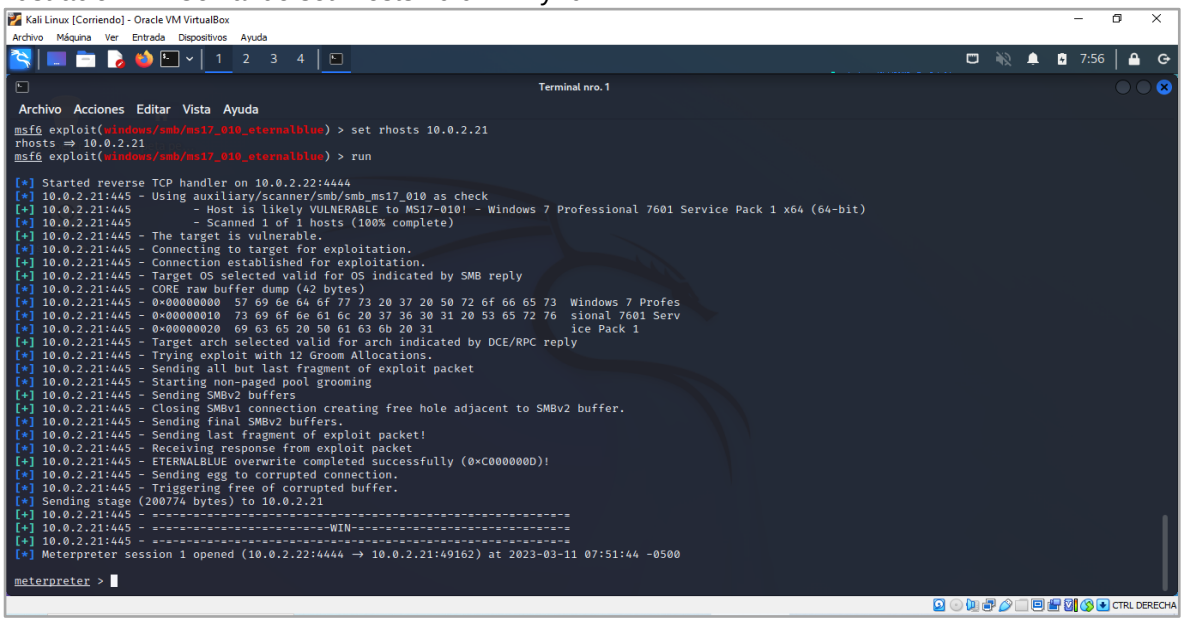
Ilustración 20. Comando use 0



Fuente: Propia (2023)

set rhosts 10.0.2.21 y luego run (ejejcutar)

Ilustración 21. Comando set rhosts 10.0.2.21 y run



Fuente: Propia (2023)

En el siguiente paso se explotan las vulnerabilidades a través de la sesión abierta de meterpreter lo cual da acceso la máquina remota Win7-SE2020-X64 (Win 7 64 bits) y se crea un usuario administrador llamado sergiovalero y se ejecuta el archivo winse20w0.exe

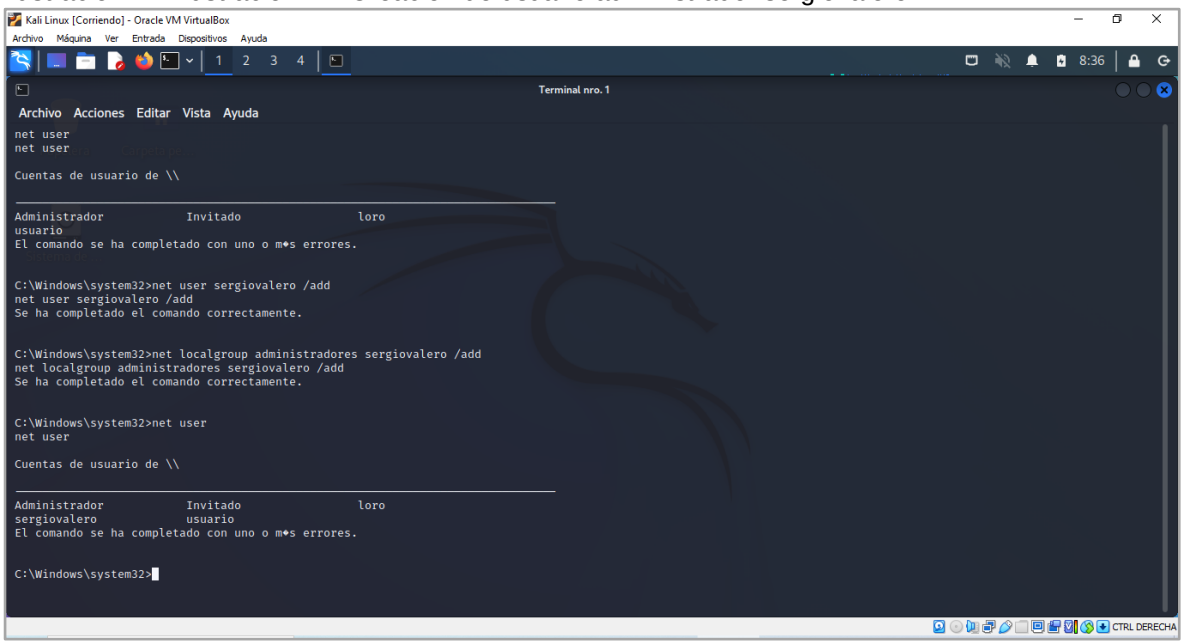
Comandos de consola utilizados en el siguiente bloque.

Meterpreter>Shell
net user net user sergiovalero/add
net localgroup administradores sergiovalero /add

Evidencia

Se crea el usuario sergiovalero y se le dan privilegios de administrador

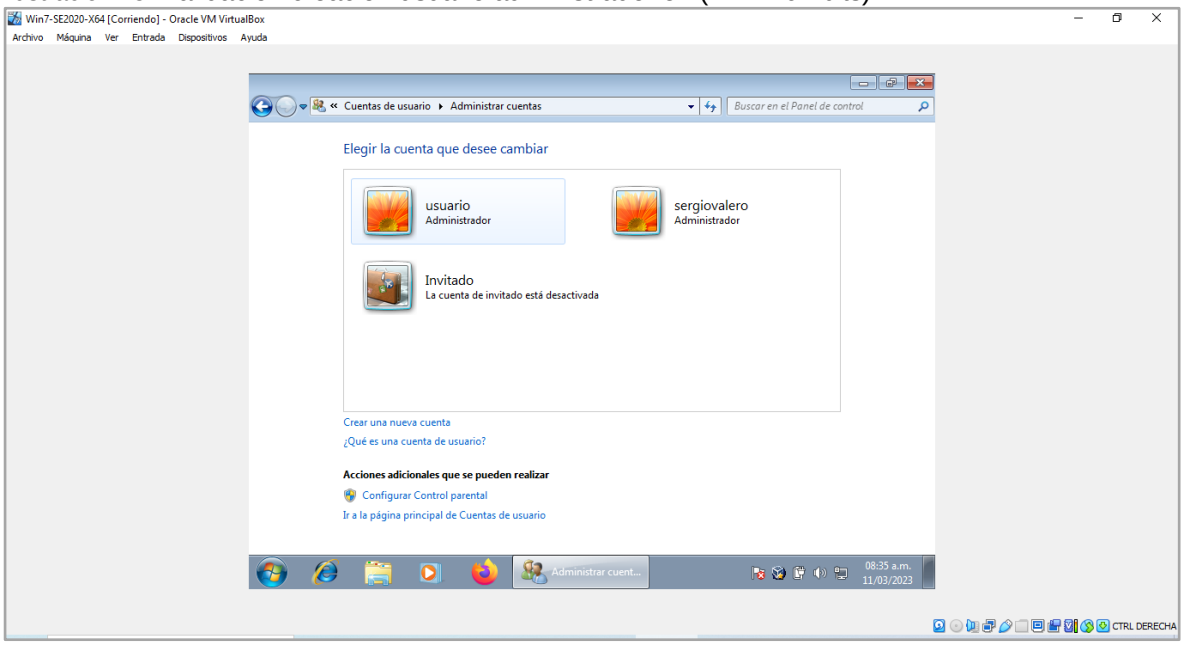
Ilustración 22. Ilustración 14. Creación de usuario administrador sergiovalero



Fuente: Propia (2023)

A continuación, se valida la creación del usuario sergiovalero como administrador en la máquina remota Win7-SE2020-X64 (Win 7 64 bits).

Ilustración 23. Validación creación usuario administrador en (Win 7 64 bits)



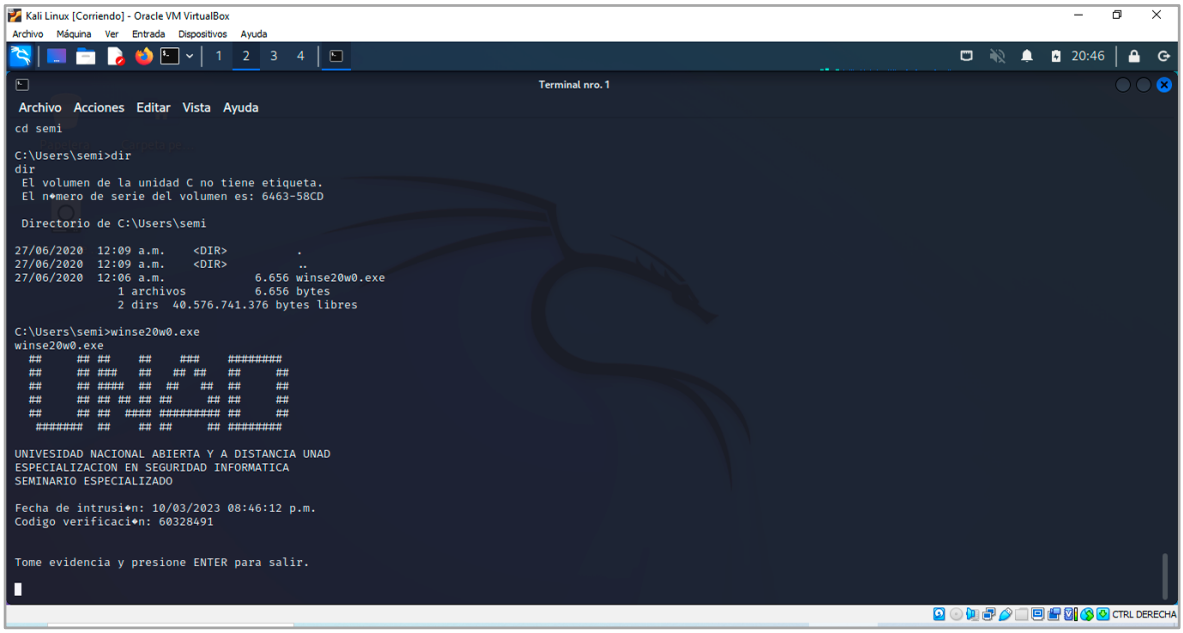
Fuente: Propia (2023)

Se accede en la máquina remota Win7-SE2020-X64 (Win 7 64 bits), directorio C:\Users\semi>

Se ejecuta el archivo winse20w0.exe

Evidencia

Ilustración 24. Corriendo el archivo C:\Users\semi>winse20w0.exe



Fuente: Propia (2023)

2.5.4 Análisis y reporte

En la siguiente etapa se describe la información que evidencia la vulnerabilidad de la Máquina remota Win7-SE2020-X64 (Win 7 64 bits).

- Análisis de la fuga de información 11 de marzo de 2023
- Máquina remota Win7-SE2020-X64 (Win 7 64 bits).
- Sistema Operativo Windows 7 Professional 7601 Service Pack 1 x64 (64-bit).
- Última actualización se realizó el 26/06/2020 y fue Revisión para Microsoft Windows (KB2534111).
- Sistema Operativo Win7-SE2020-X64 (Win 7 64 bits), con SMBv1 Vulnerabilidad de ejecución remota de código en servidores Microsoft SMBv1 (ms17-010) CVE-2017-0143

2.5.5 Herramientas utilizadas en el análisis de vulnerabilidades

A continuación, se expone las herramientas utilizadas en el análisis de vulnerabilidad de la Máquina remota Win7-SE2020-X64 (Win 7 64 bits).

Se utilizó una herramienta llamada nmap, esta realiza un escaneo de la red y devuelve una lista de máquinas activas, puertos abiertos, y sistemas operativos. El puerto abierto es el 445/tcp el servicio microsoft-ds.

2.5.6 Explicación paso a paso del ataque

En los siguientes párrafos se explicará la forma en que se realizó el ataque y como este afectó la máquina remota Win7-SE2020-X64 (Win 7 64 bits).

Validamos que maquinas se están activas en la red y cuales se comunican entre sí. Para eso hacemos ping desde Kali Linux (IP 10.0.2.22) a Win7-SE2020-X64 (Win 7 64 bits) (IP 10.0.2.21) y de Win7-SE2020-X64 (Win 7 64 bits) (IP 10.0.2.21) a Kali Linux (IP 10.0.2.22). una vez establecido que, si hay comunicación, se procede a ejecutar la herramienta nmap, una vez se accede a la herramienta se digita a través del comando de consola nmap –sP 10.0.2.0/24 para determinar las ip activas en la red. Una vez se determina que la maquina Win7-SE2020-X64 (Win 7 64 bits) (IP 10.0.2.21) se encuentra activa en la red con la herramienta nmap, se procede a escanear las vulnerabilidades de esta máquina por lo cual utilizaremos el comando de consola sudo nmap 10.0.2.21 -script vuln. Se evidencia la vulnerabilidad en la Win7-SE2020-X64 (Win 7 64 bits) la cuales es SMBv1 uan vulnerabilidad de ejecución remota de código en servidores Microsoft SMBv1 (ms17-010) CVE-2017-0143 con un factor de riesgo alto. Una vez se establecen las vulnerabilidades de la máquina que se desea atacar, se procede a ejecutar la herramienta metasploit con la cual se pretende acceder a la maquina Win7-SE2020-X64 (Win 7 64 bits) explotando las vulnerabilidades que presenta la máquina. Una vez se ingresó a la herramienta metasploit, se digita el comando de consola search ms17-010 para identificar el exploit, una vez identificado el exploit se selecciona con el comando de consola use 0 para iniciar la configuración del script. No se configura el payload, se toma el que viene configurado por defecto. Una vez seleccionado se digita el comando de consola show options para determinar las opciones que son requeridas para la explotación de la vulnerabilidad. Se digita el comando de consola set rhosts 10.0.2.21 como parámetro requerido y se procede a digital luego run para ejecutar el exploit. Ejecutado el exploit se abre una sesión de meterpreter en la maquina remota Win7-SE2020-X64 (Win 7 64 bits). Abierta la sesión meterpreter, se digita el comando de consola shell y se accede a la consola de Windows del equipo Win7-

SE2020-X64 (Win 7 64 bits), C:\Windows\system32> una vez allí se digital el comando net user net user sergiovalero/add, el cual creará el nuevo usuario sergiovalero, una vez creado se asignan privilegios de administrador digitando el comando net localgroup administradores sergiovalero /add. Por último, se accede a la maquina atacada Win7-SE2020-X64 (Win 7 64 bits) y se valida la creación del nuevo usuario con privilegios de administrador. En este punto ya se completó el objetivo el cual era acceder a la maquina atacada Win7-SE2020-X64 (Win 7 64 bits) desde la maquina Kali Linux del atacante, conocer las vulnerabilidades y posterior explotación de la misma para acceder a ella y crear un usuario administrador sergivalero.

A continuación, se genera una infografía para evidenciar los pasos en el ataque.

Ilustración 25. Flujo de ataque Red Team

Fuente: Propia (2023)

2.6 CONTENCIÓN DE ATAQUES

A continuación, se desarrollará la Etapa 4 – Contención de ataques informáticos, cuarta fase del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

Análisis de anexos

Anexo 5 – situación problema – análisis Blue Team.

A continuación, se transcribe el texto entregado por el curso de la situación planteada del problema para su posterior análisis en el desarrollo de la actividad:

"WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL."

Para desarrollar el presente informe, se presentan las máquinas activas en el banco de trabajo con las OVA de Windows7 X64 suministradas por el curso, con sus IP.

Win7-SE2020-X64 (Win 7 64 bits) IP: 10.0.2.21 en la máquina Windows 7 64 bits
KALI LINUX IP: 10.0.2.22 en la máquina Kali Linux

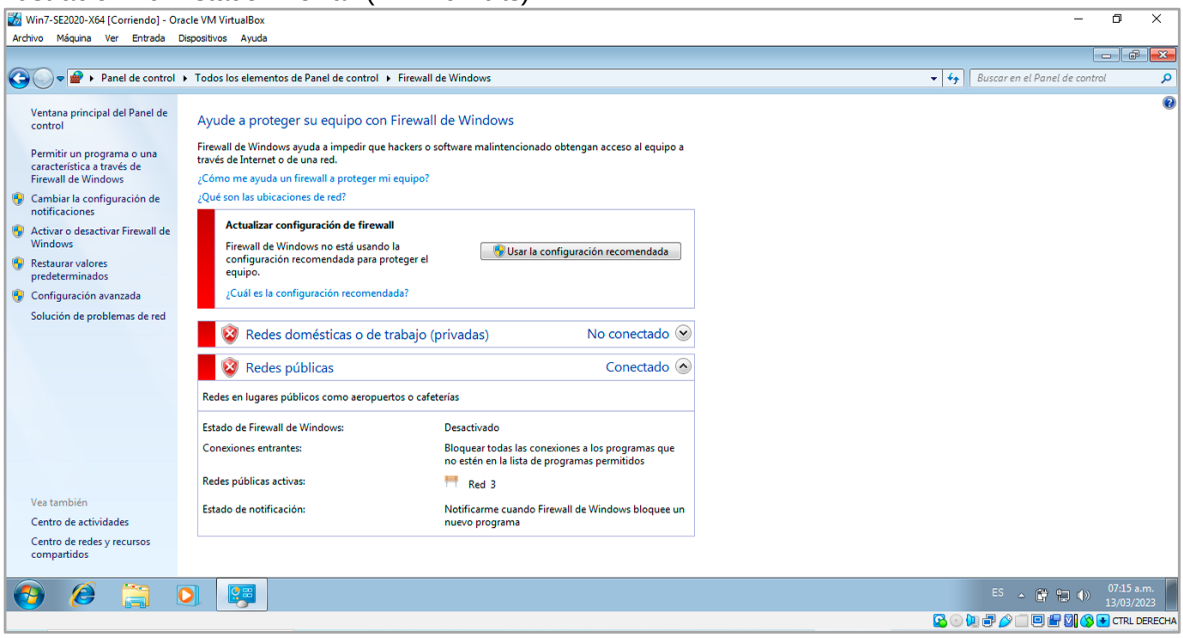
2.6.1 Acciones para contener un ataque en tiempo real.

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

Se procede a realizar un análisis en tiempo real del equipo, los equipos y/o la red atacada, lo cual sería el primero de una serie de pasos para validar el estado del ataque.

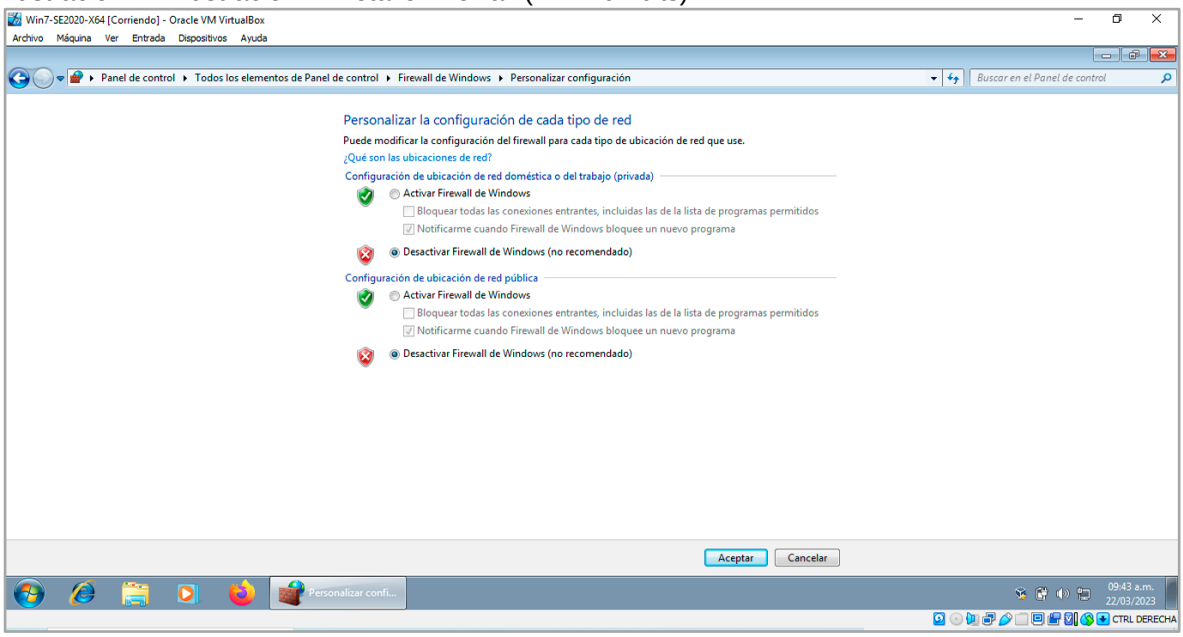
Se inicia con la validación del estado del firewall del equipo que está siendo atacado para evaluar su configuración y determinar si el sistema se encuentra protegido de conexiones remotas no deseadas.

Ilustración 26. Estado Firewall (Win7 64 bits)



Fuente: Propia (2023)

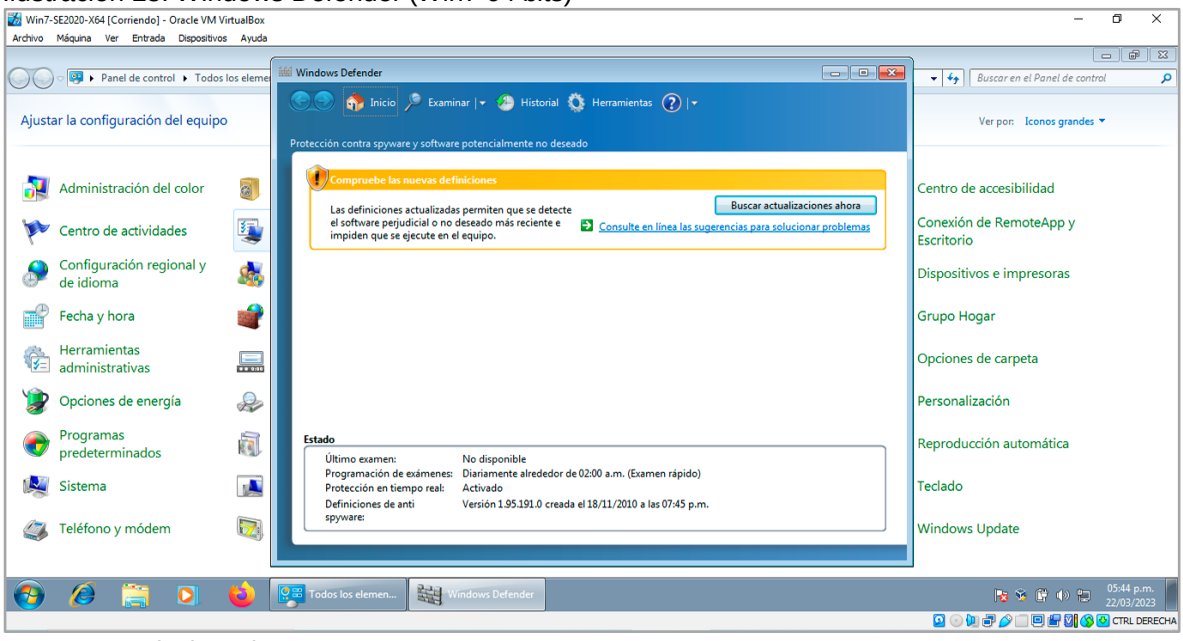
Ilustración 27. Ilustración 2. Detalle Firewall (Win7 64 bits)



Fuente: Propia (2023)

Se continua con la validación del estado del Windows Defender en el equipo que está siendo atacado.

Ilustración 28. Windows Defender (Win7 64 bits)



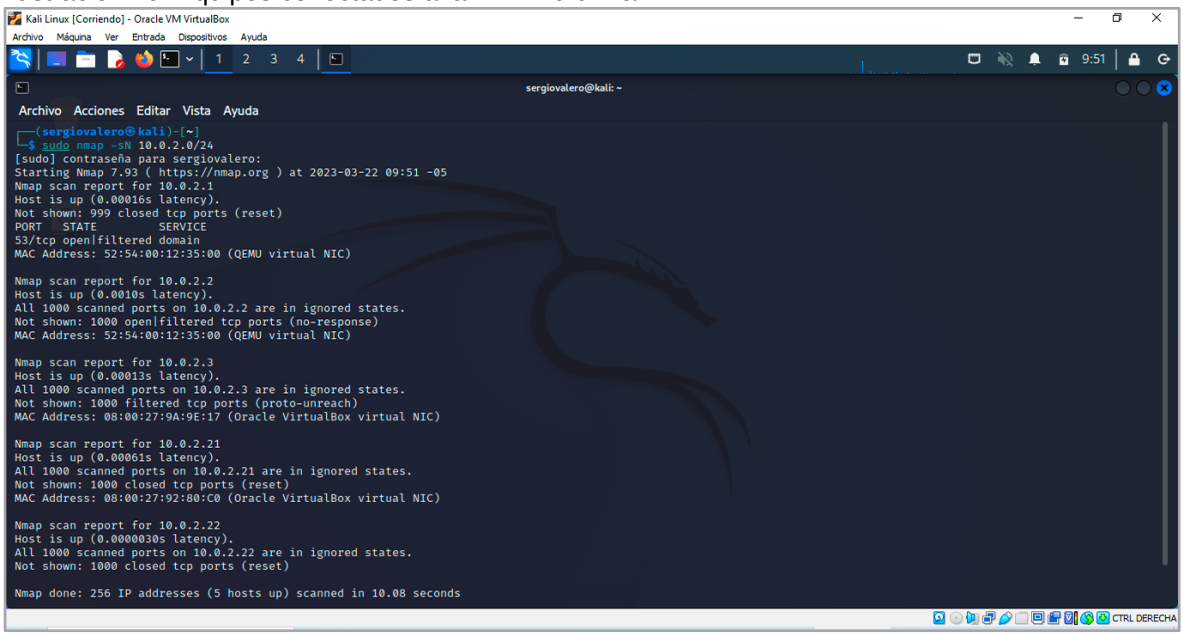
Fuente: Propia (2023)

Se continúan evaluando los dispositivos que se encuentran conectados a la red.

Comandos de consola utilizados en el siguiente bloque en Kali Linux.

sudo nmap -sN 10.0.2.0/24

Ilustración 29. Equipos conectados a la RED 10.0.2.0/24



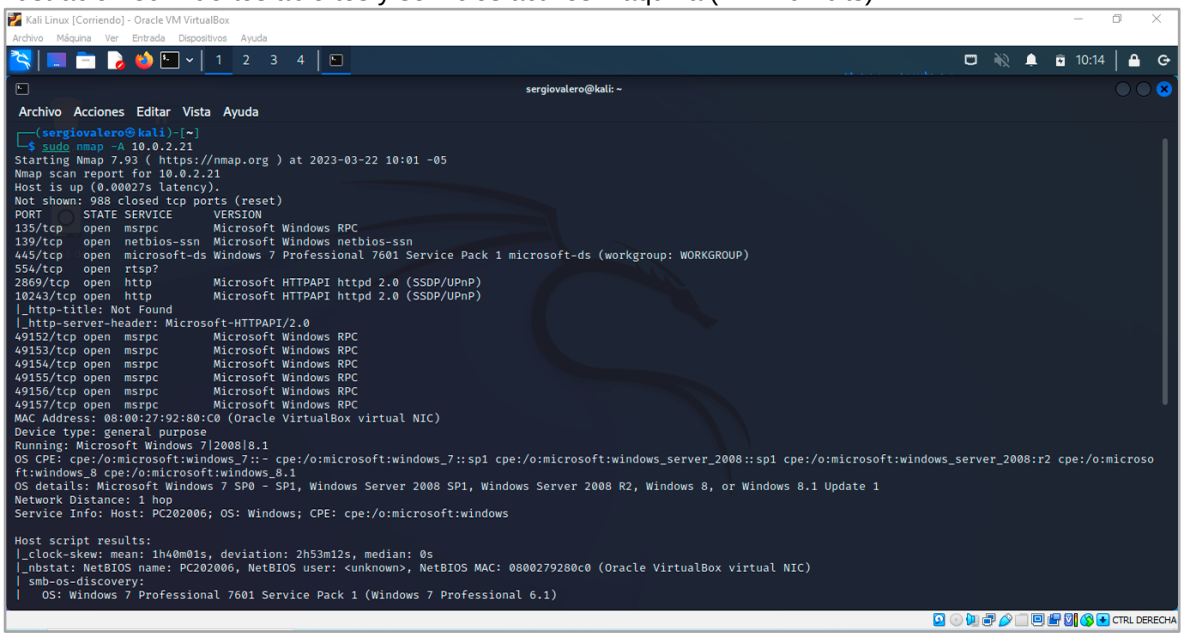
Fuente: Propia (2023)

A continuación, se relacionan los puertos abiertos y servicios activos en la maquina Win7-SE2020-X64 (Win 7 64 bits) IP: 10.0.2.21

Comandos de consola utilizados en el siguiente bloque en Kali Linux

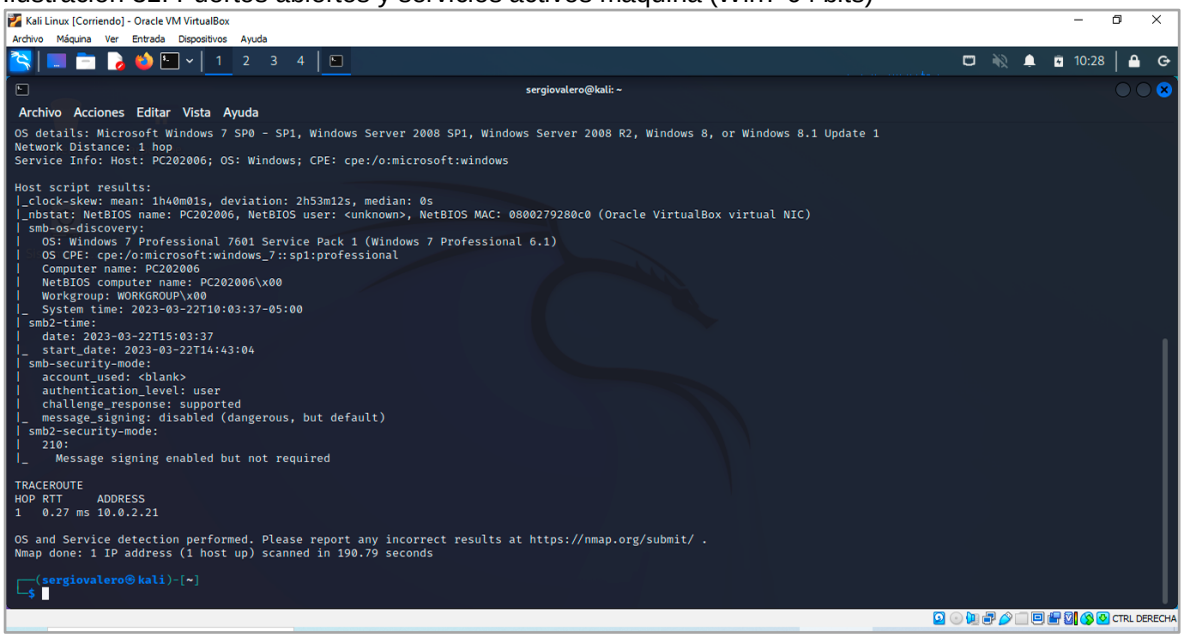
sudo nmap -A 10.0.2.21

Ilustración 30. Puertos abiertos y servicios activos maquina (Win7 64 bits)



Fuente: Propia (2023)

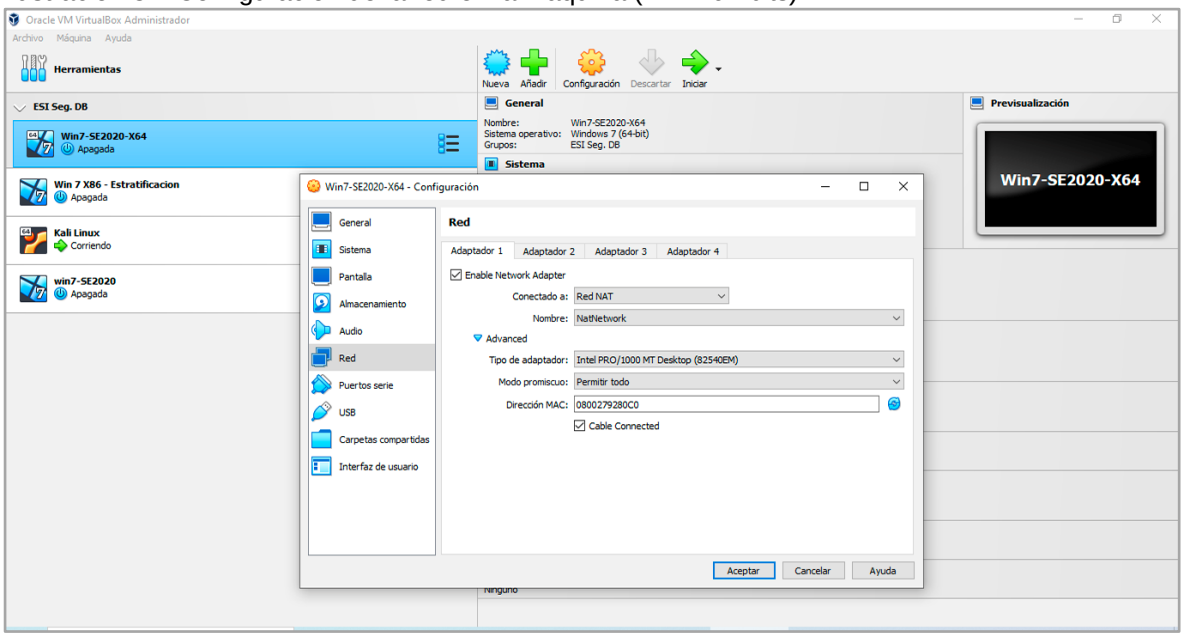
Ilustración 31. Puertos abiertos y servicios activos maquina (Win7 64 bits)



Fuente: Propia (2023)

El próximo paso es identificar la configuración de la red en la maquina Win7-SE2020-X64 (Win7 64 bits)

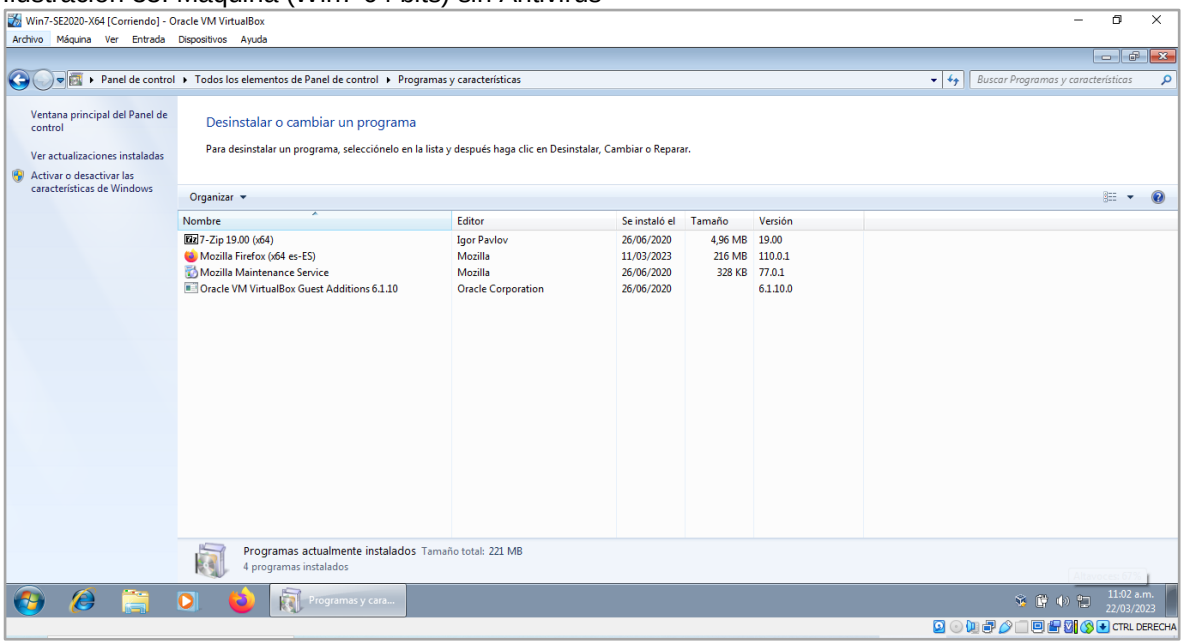
Ilustración 32. Configuración de la red en la maquina (Win7 64 bits)



Fuente: Propia (2023)

El siguiente paso es validar si se encuentra instalado un antivirus en la maquina Win7-SE2020-X64 (Win7 64 bits). Lo cual es evidente que no se evidencia sistema antivirus instalado.

Ilustración 33. Máquina (Win7 64 bits) sin Antivirus

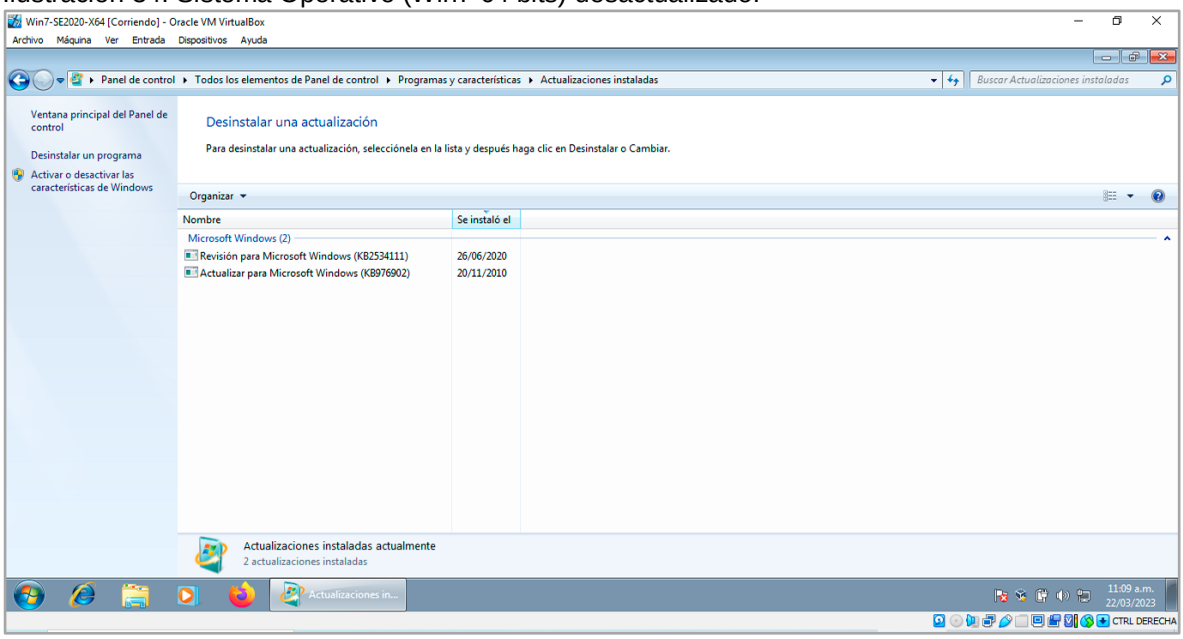


Fuente: Propia (2023)

Un paso importante es validar la actualización del sistema operativo en la máquina Win7-SE2020-X64 (Win7 64 bits), el cual nos informará si se encuentra eexpuesto a vulnerabilidades y fallos de seguridad recientes. Se evidencia que no se encuentra actualizado y su vulnerabilidad es evidente.

Se aclara que Windows 7 no tiene soporte desde el 14 de enero de 2020, fecha en la que finalizó por lo tanto este sistema operativo queda expuesto y vulnerable a virus y malware.

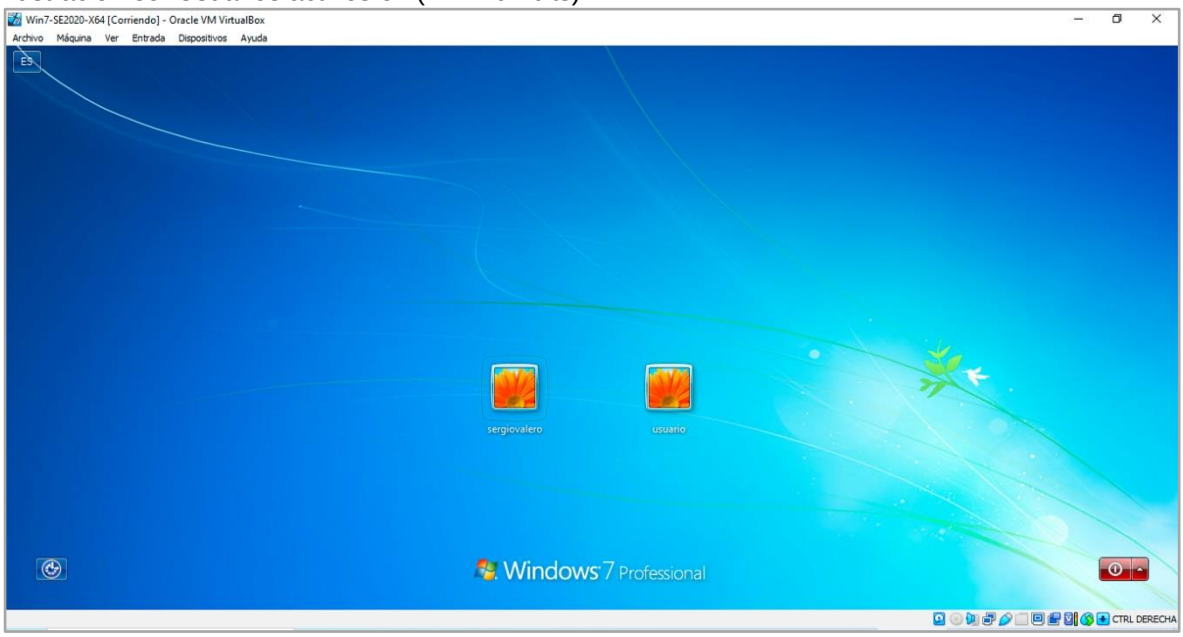
Ilustración 34. Sistema Operativo (Win7 64 bits) desactualizado.



Fuente: Propia (2023)

A continuación, se validan que usuarios activos que se encuentran en la máquina Win7-SE2020-X64 (Win7 64 bits)

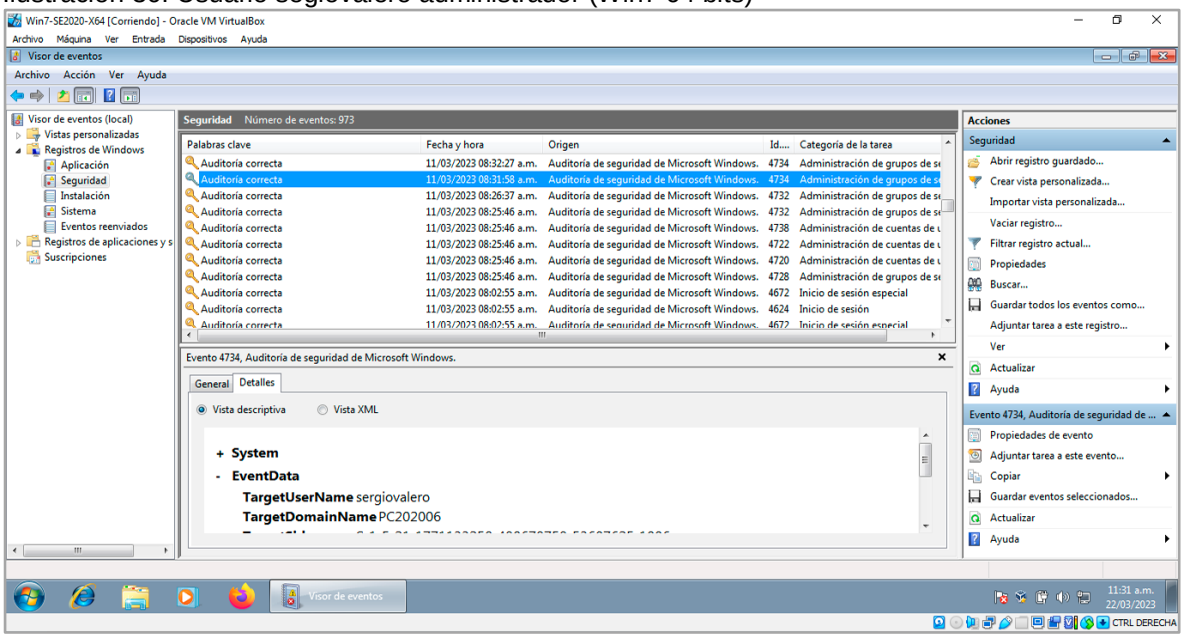
Ilustración 35. Usuarios activos en (Win7 64 bits)



Fuente: Propia (2023)

A continuación, se analiza el Visor de eventos en la máquina Win7-SE2020-X64 (Win7 64 bits), el cual muestra la creación de un usuario segiovalero con privilegios de administrador, el cual no está autorizado su creación.

Ilustración 36. Usuario segiovalero administrador (Win7 64 bits)



Fuente: Propia (2023)

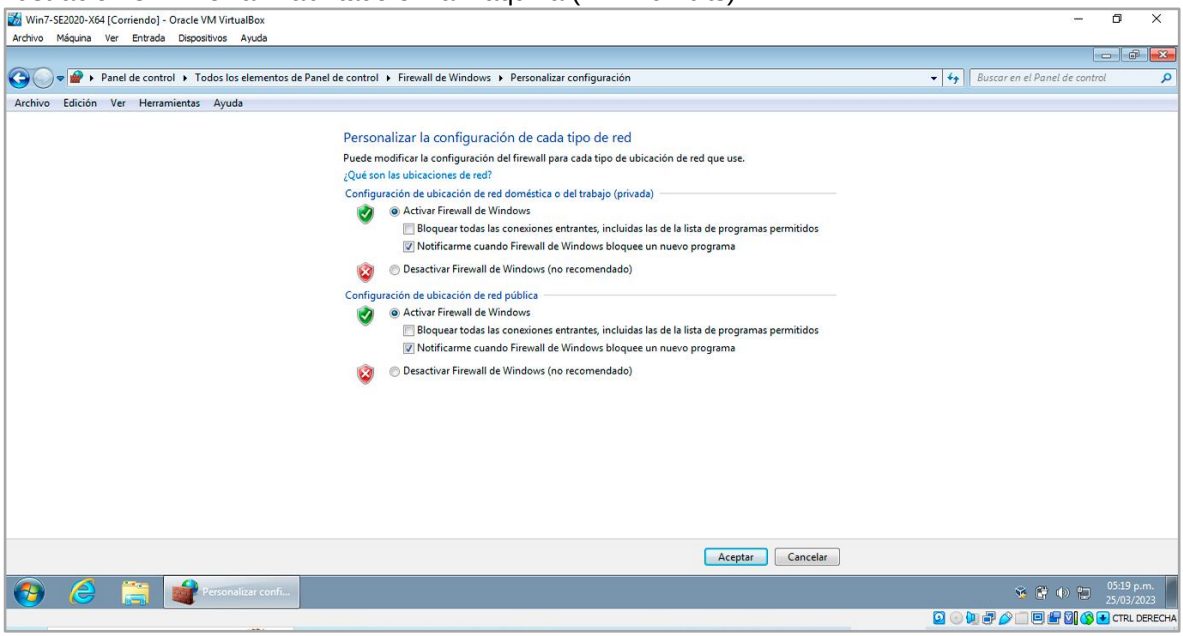
¿Teniendo en cuenta el ataque ejecutado en el ejercicio de Red team qué medidas de hardening[16] propondría para que el ataque no se repita?

A continuación, se proponen los siguientes métodos para endurecer (proteger) el sistema y de esta forma minimizar las amenazas y/o contenerlas al máximo.

Cerrar puertos que no sean prioridad o no se encuentren en uso.

Se habilita el firewall en la máquina Win7-SE2020-X64 (Win7 64 bits) e instalar y configurar uno de terceros para mejorar la protección en la primera línea de defensa entre el flujo de información entrante y saliente de la red de la organización.

Ilustración 37. Firewall habilitado en la máquina (Win7 64 bits)



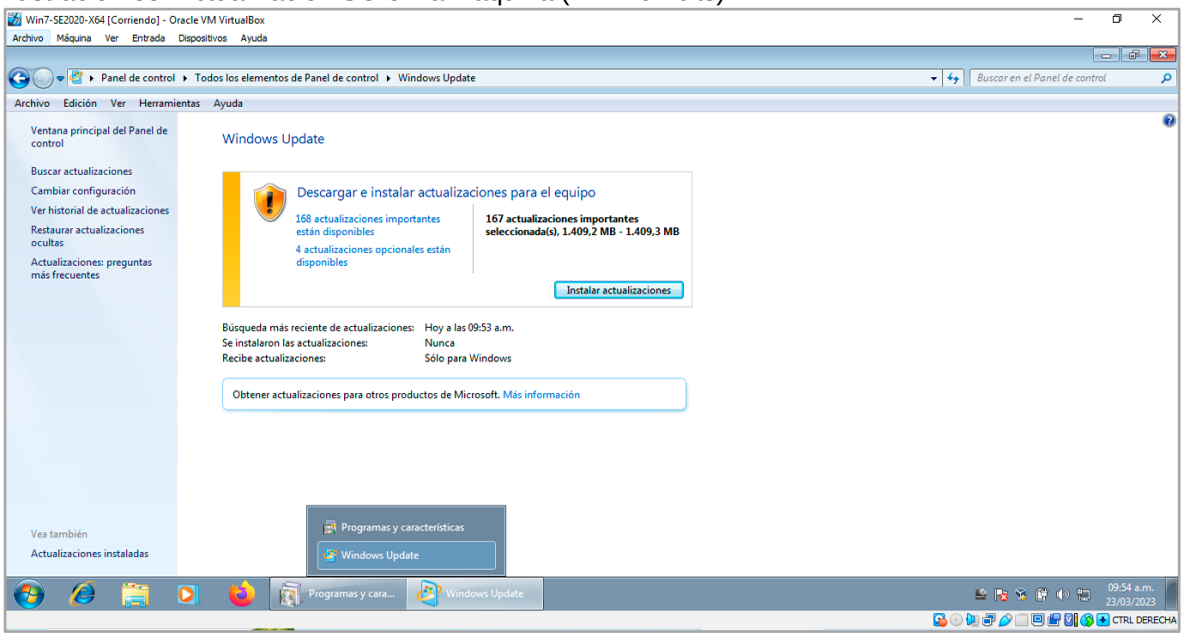
Fuente: Propia (2023)

Deshabilitar servicios que no se encuentren en uso o eliminarlos según la validación del administrador de seguridad de la red.

Actualizar el sistema operativo en la máquina Win7-SE2020-X64 (Win7 64 bits), el cual no ayudará a blindar las vulnerabilidades y fallos de seguridad a los que se encuentre expuesto el sistema.

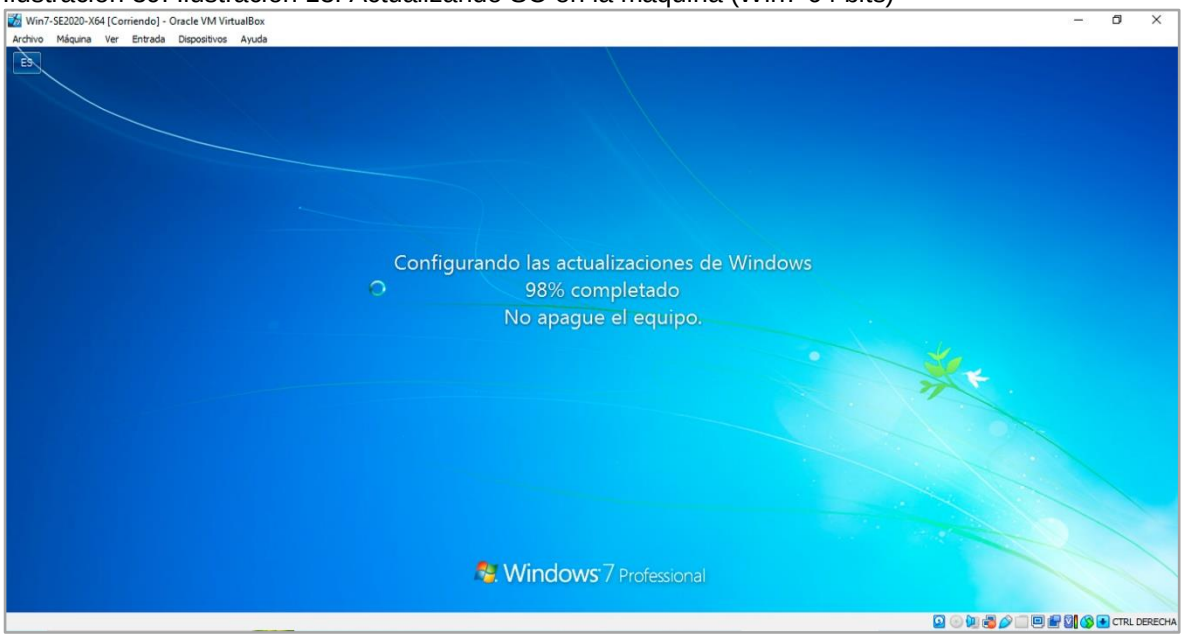
[16] SICET (2022) Hardening Recuperado de **https://www.ciset.es/publicaciones/blog/746-hardening**

Ilustración 38. Actualización SO en la máquina (Win7 64 bits)



Fuente: Propia (2023)

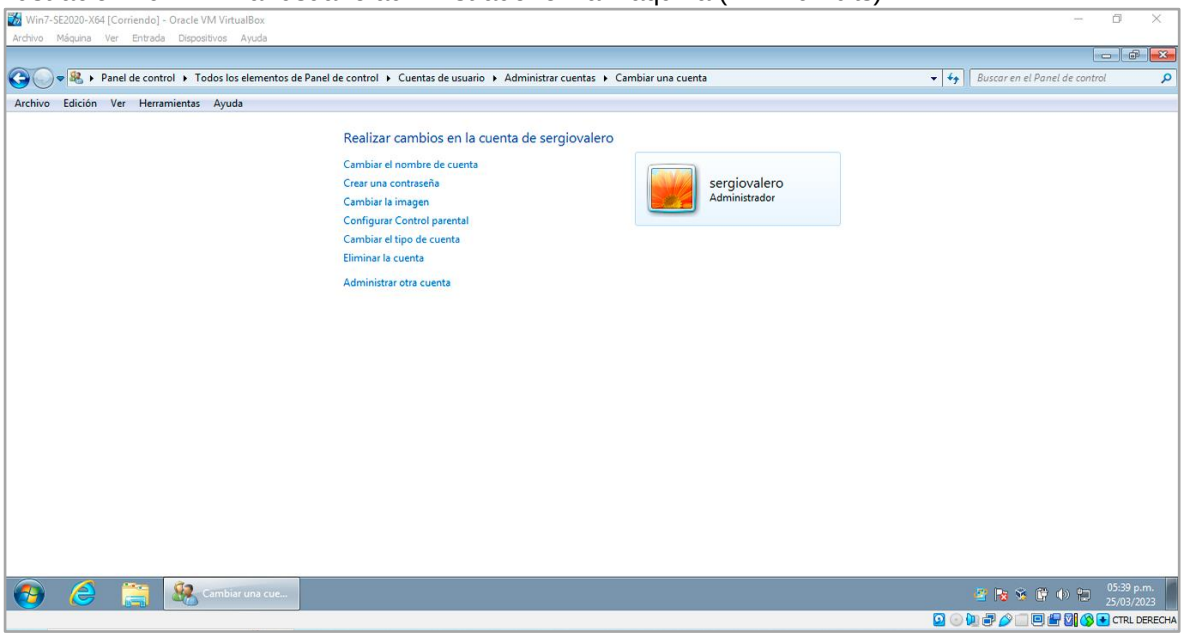
Ilustración 39. Ilustración 13. Actualizando SO en la máquina (Win7 64 bits)



Fuente: Propia (2023)

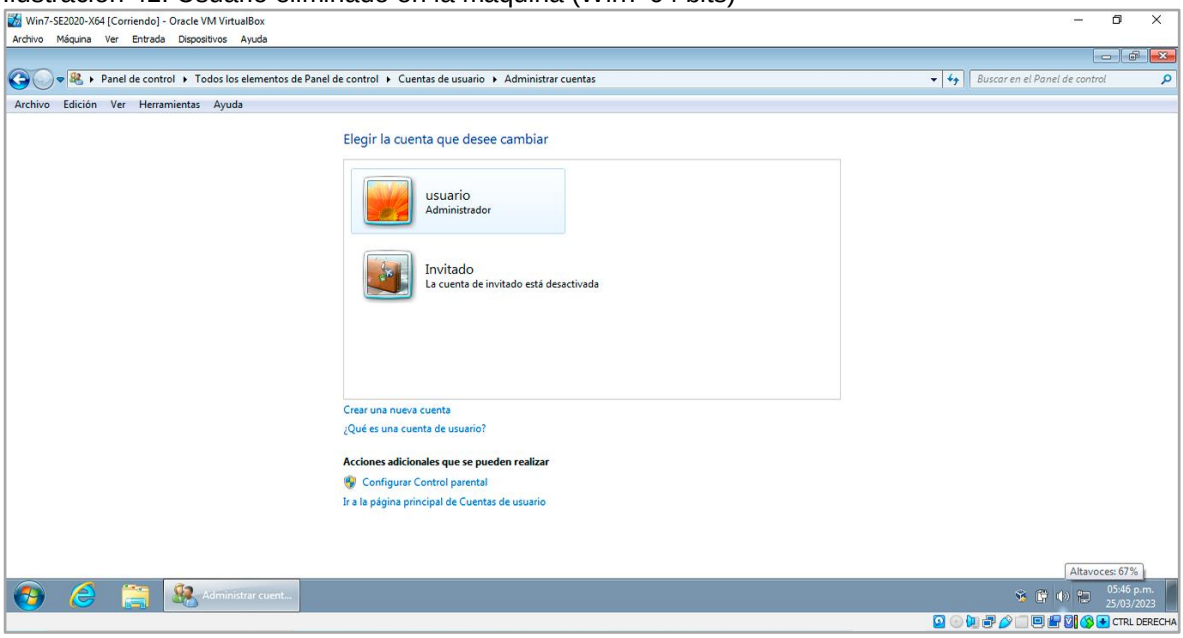
Eliminar usuario administrador creado en el ataque a la máquina Win7-SE2020-X64 (Win7 64 bits).

Ilustración 40. Eliminar usuario administrador en la máquina (Win7 64 bits).



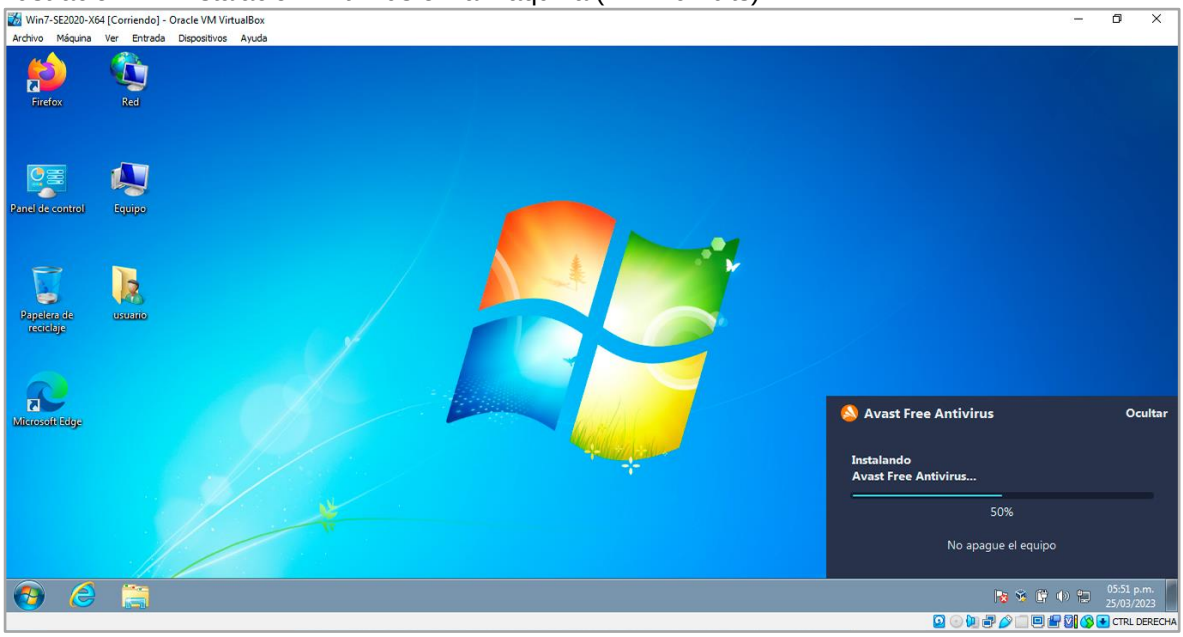
Fuente: Propia (2023)

Ilustración 41. Usuario eliminado en la máquina (Win7 64 bits)



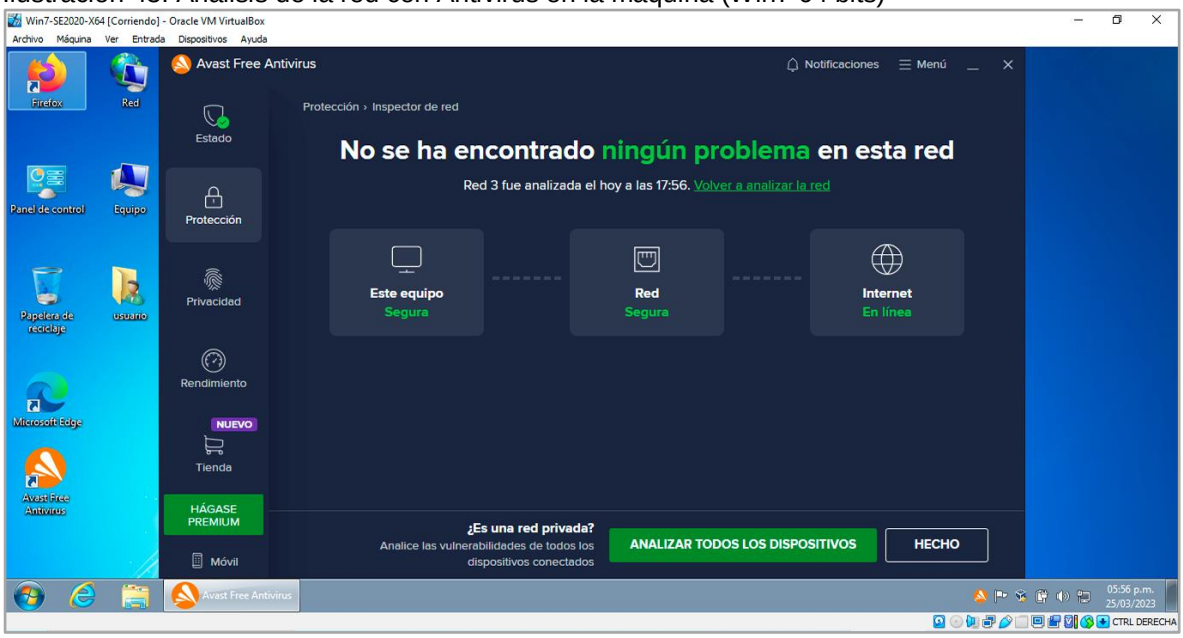
Fuente: Propia (2023)

Ilustración 42. Instalación Antivirus en la máquina (Win7 64 bits)



Fuente: Propia (2023)

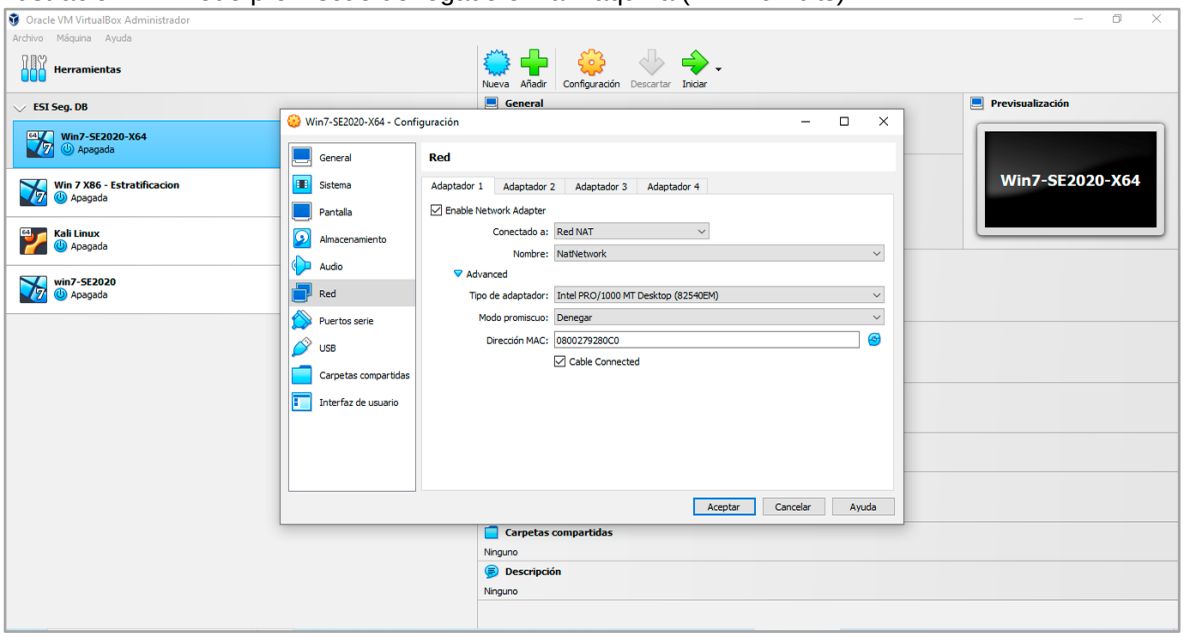
Ilustración 43. Análisis de la red con Antivirus en la máquina (Win7 64 bits)



Fuente: Propia (2023)

Se procede a realizar modificaciones a los permisos del modo promiscuo a la máquina Win7-SE2020-X64 (Win7 64 bits)

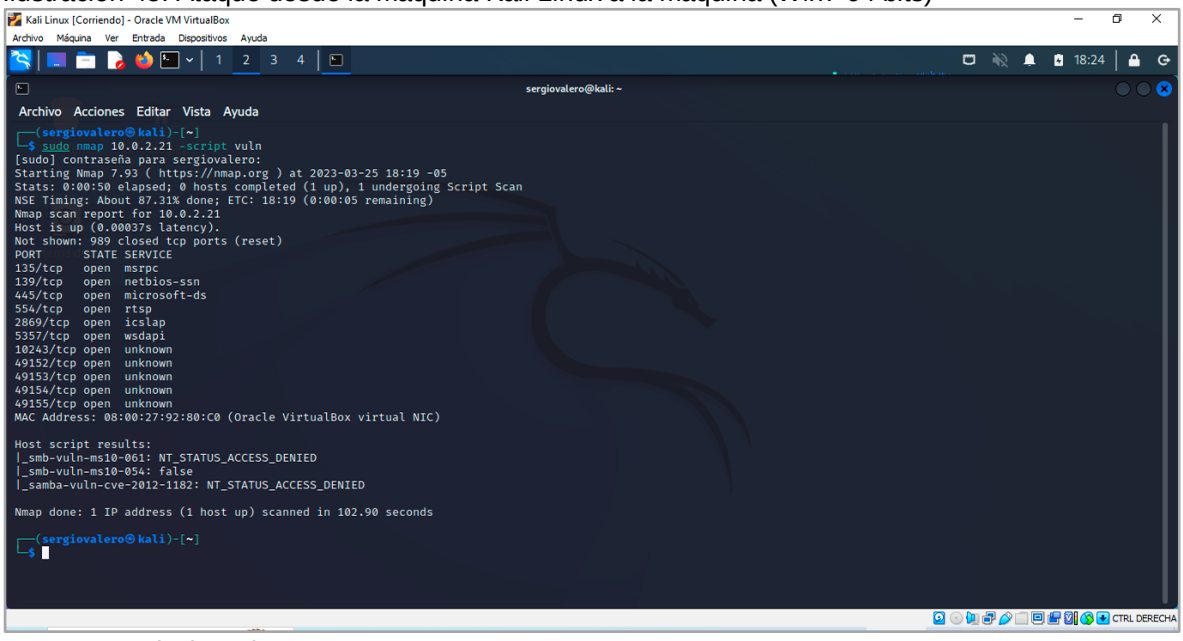
Ilustración 44. Modo promiscuo denegado en la máquina (Win7 64 bits)



Fuente: Propia (2023)

Por ultimo realizamos nuevamente el ataque desde la maquina Kali Linux a la maquina Win7-SE2020-X64 (Win7 64 bits) para validar las medidas de hardenización propuestas para bloquear los ataques.

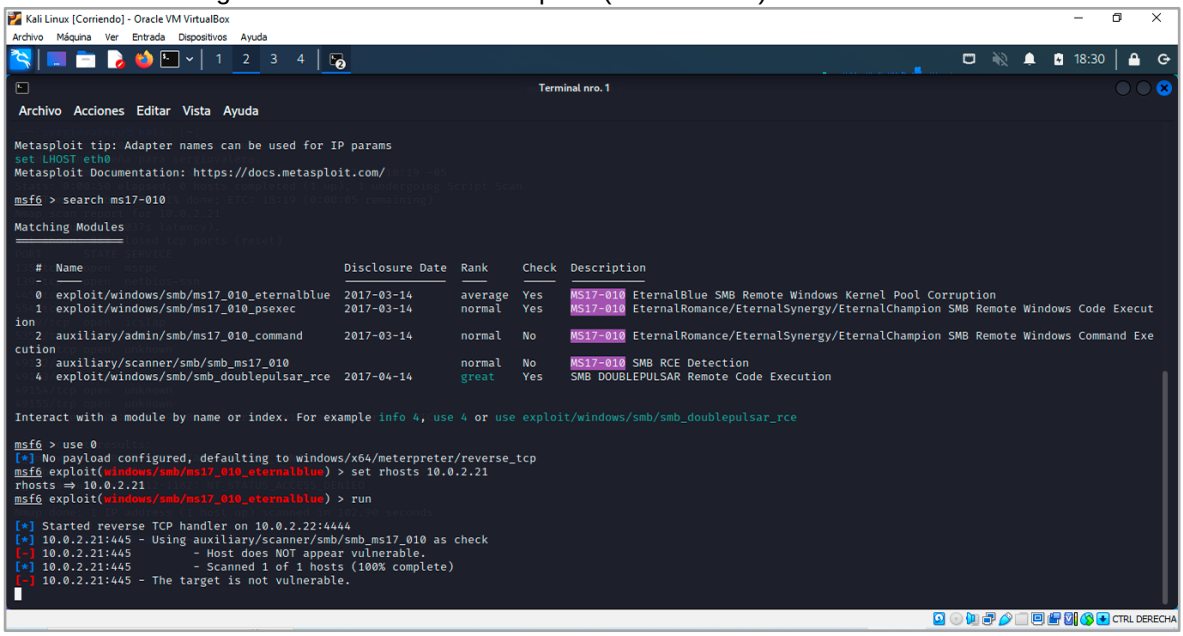
Ilustración 45. Ataque desde la maquina Kali Linux a la maquina (Win7 64 bits)



Fuente: Propia (2023)

Se evidencia que la maquina Win7-SE2020-X64 (Win7 64 bits), no es vulnerable a los ataques desde la maquina Kali Linux, validando que las medidas de hardenización propuestas para la protección del ataque fueron las correctas.

Ilustración 46. Target no vulnerable en la maquina (Win7 64 bits)



Fuente: Propia (2023)

2.6.2 Describa las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos

EQUIPO BLUETEAM	EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS (CSIRT)
¿Qué son?	
Un equipo Blueteam son un equipo de profesionales especialistas en seguridad informática en diferentes áreas con capacidades de reacción ante ataques informáticos en tiempo real convirtiéndolos en una seguridad ofensiva ante incidentes digitales.	Un equipo de respuesta a incidentes informáticos (CSIRT), es un grupo de profesionales expertos en ataques preventivos y reactivos a los cuales se hace entrega de un informe acerca de ataques a la seguridad informática en una empresa pública o privada, gobierno, etc.
Funciones principales	
Analizar en tiempo real el funcionamiento y comportamiento de sistemas informáticos a través de métodos o herramientas para detectar patrones anormales. Hardenización o endurecimiento de software y hardware para mitigación o	SU función es la seguridad defensiva y la documentación de amenazas y vulnerabilidades constantes. Rastrear incidentes informáticos y de Ciberseguridad.

eliminación de incidentes informáticos al interior de la organización. Validación permanente de los controles y métodos aplicados en la seguridad informática en organizaciones para una mejora continua. Constante seguimiento a los sistemas de información e informáticos para detectar posibles amenazas en tiempo real	Gestionar respuestas ante incidentes informáticos para la eliminación del riesgo, ataque o prevención de los mismos. Ayudar a la comunidad en la protección ante incidentes informáticos a través de la difusión de contenido digital acerca de las constantes amenazas a la seguridad.

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

Si hay la posibilidad en el equipo Blueteam de trabajar con CIS[17] "Center For Internet Security", claro que se trabajaría, ya que esto permitirá trabajar con controles y procedimientos estandarizados preestablecidos contra incidentes informáticos y de seguridad cibernética en la prevención siendo esto de apoyo fundamental en las políticas de seguridad informática de cualquier empresa que desee blinda sus infraestructura tecnológica.

2.6.4 Funciones y características de lo que es un SIEM.

Para explicar y redactar las funciones de un sistema SIEM, primero hay que definir qué es y para qué sirve.

Un sistema SIEM es una información sobre seguridad y gestión de eventos o SIEM (Security Information and Event Management) el cual permite a los responsables de la seguridad informática y de la información de la empresa detectar patrones anormales del comportamiento en los sistemas informáticos para su análisis y actuar en tiempo real ante las amenazas.

Sus funciones principales son:

- Monitoreo en tiempo real los sistemas informáticos (hardware y software) en la organización en busca de patrones anormales.
- Asignar personal experto para la solucionar el incidente informático.

17 ManageEngine (No) ¿Qué son y cómo implementar los Controles de CIS (CIS Controls)? Recuperado de https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

- Documentar el proceso desde su detección, como se actuó ante el hallazgo y finalmente la solución del incidente informático, creando una base de datos de incidentes en la organización.
- Hacer cumplir la normatividad y legislación vigente acerca de la protección de la información y seguridad informática en la organización.

Sus características principales son:

- Diferencia amenazas reales de incidentes falsos.
- Las potenciales amenazas son monitoreadas de forma centralizada.
- Funciones específicas del personal especialista calificado para soluciones eficientes.
- Su cumplimiento de la normatividad vigentes y legislación para el cumplimiento de la protección de la información y la seguridad de los datos.

2.6.5 Herramientas de contención de ataques informáticos.

NEXT GENERATION FIREWALL (NGFW). Es un tipo de firewall avanzado que utiliza tecnologías de seguridad adicionales a las utilizadas en los firewalls tradicionales, tales como filtrado de paquetes y control de acceso basado en políticas.

Entre las características que hacen que un NGFW sea considerado de "próxima generación" se encuentran el análisis de contenido en profundidad, la identificación de aplicaciones y usuarios, la prevención de intrusiones, el filtrado de URL, el control de acceso granular y la integración con sistemas de inteligencia de amenazas.

El NGFW se centra en proporcionar una seguridad más completa y eficaz en comparación con los firewalls tradicionales, y puede detectar y bloquear amenazas avanzadas y ataques sofisticados, lo que lo hace ideal para empresas que buscan una seguridad de red avanzada y adaptada a las amenazas actuales.

En resumen, un NGFW ofrece una capa adicional de seguridad a la red empresarial, y ayuda a proteger la red y los datos críticos de la empresa de las amenazas cibernéticas.

Cisco FireSight. Cisco FireSight es una solución de seguridad integral desarrollada por Cisco que ayuda a las organizaciones a detectar, prevenir y responder a amenazas de seguridad en tiempo real. Esta solución integra las funciones de un

sistema de prevención de intrusiones (IPS) y un sistema de detección de intrusiones (IDS) para proporcionar una protección avanzada contra amenazas de seguridad.

FireSight utiliza una tecnología de análisis avanzada para detectar y prevenir amenazas de seguridad, lo que incluye la identificación de patrones de tráfico maliciosos, la identificación de malware y la prevención de intrusiones. La solución también incluye herramientas de análisis y gestión de seguridad centralizadas, permitiendo a las empresas la identificación y respuesta a los incidentes informáticos en línea.

Además, FireSight utiliza una arquitectura escalable y flexible permitiendo a las organizaciones adaptarse y evolucionar con la continua transformación de las amenazas en la seguridad. La solución también se integra con otras soluciones de seguridad de Cisco, permitiendo a las empresas desarrollar una barrera de seguridad robusta.

En resumen, Cisco FireSight es una solución de seguridad avanzada que ayuda a las organizaciones a protegerse contra amenazas de seguridad en tiempo real, ofreciendo una variedad de características y herramientas para garantizar una protección completa y efectiva.

ESET Endpoint Antivirus. ESET Endpoint Antivirus es una solución de seguridad desarrollada por ESET que protege los dispositivos de una organización contra amenazas de seguridad en tiempo real. Esta solución utiliza una combinación de detección basada en firmas y tecnología de detección heurística para proteger los sistemas contra virus, spyware, ransomware y otros tipos de malware.

Endpoint Antivirus también incluye herramientas de análisis y gestión centralizadas, lo que permite a los administradores de TI monitorear y administrar la seguridad de todos los dispositivos dentro de la organización. Estas herramientas también permiten la configuración de políticas de seguridad para garantizar una protección consistente y efectiva en todos los dispositivos. Esta solución también utiliza tecnología de prevención de intrusiones (HIPS) y un firewall personal para proteger los sistemas contra amenazas de seguridad conocidas y desconocidas.

En resumen, ESET Endpoint Antivirus es una solución de seguridad avanzada que protege los sistemas de una organización contra una amplia variedad de amenazas de seguridad en tiempo real, ofreciendo herramientas de análisis y gestión centralizadas para una protección completa y efectiva.

3. CONCLUSIONES

La seguridad informática es un activo crítico en la era digital actual, debido a que los datos y sistemas informáticos son valiosos y sus vulnerabilidades pueden ser explotadas por individuos malintencionados para cometer delitos digitales.

Es importante tomar medidas para proteger los sistemas y datos, implementando políticas y prácticas de seguridad, usando herramientas y tecnologías de ciberseguridad y estar al tanto de las amenazas y tendencias en el ámbito de la seguridad informática. Además, es necesario conocer las leyes y regulaciones existentes sobre delitos informáticos y protección de datos personales para evitar ser víctima o ser acusado de cometer un delito informático.

En general, los delitos informáticos en Colombia requieren una mayor atención y recursos para combatirlos. Esto incluye una mejor capacitación de a los legisladores encargados de judicializar a los ciberdelincuentes, así como una mayor educación a la población sobre cómo protegerse contra este tipo de delitos.

La creciente amenaza contra la privacidad de la información a nivel mundial, demuestra la necesidad de cooperación internacional en la lucha contra el cibercrimen, siendo ejemplo de la importancia de la ciberseguridad en el mundo actual y la necesidad de capacitación, colaboración e intercambio recursos humanos y de tecnología para hacer frente a las amenazas cibernéticas.

Como conclusión el equipo Red Team es responsable de simular ataques informáticos para detectar posibles vulnerabilidades y debilidades en los sistemas de seguridad de la organización y el equipo Blue Team es responsable de defender los sistemas y prevenir posibles ataques, razón por la cual ambos equipos deben trabajar juntos para identificar las debilidades y mejorar la seguridad de los sistemas, siendo la comunicación y la colaboración fundamentales para lograr una contención efectiva de los ataques informáticos.

Hoy en día es de vital importancia que, dentro de las organizaciones, existan profesionales expertos en seguridad informática, el cual constantemente monitoreen la red en busca de vulnerabilidades para blindar a la empresa ante ataques informáticos y contar con profesionales expertos red team y blue team en las organizaciones.

En conclusión, la prevención es clave en la contención de ataques informáticos. Las organizaciones deben contar con medidas de seguridad proactivas, como la actualización regular de software y la capacitación de los empleados en ciberseguridad, para reducir el riesgo de ataques.

En conclusión, la seguridad informática es esencial para garantizar la privacidad, integridad y disponibilidad de los datos y sistemas informáticos.

En resumen, la contención de ataques informáticos requiere la colaboración y comunicación efectiva entre los equipos de Red Team y Blue Team, así como la implementación de medidas de seguridad proactivas para prevenir posibles ataques.

4. RECOMENDACIONES

Se recomienda que las organizaciones cuenten con un equipo blue team y red team para detectar posibles vulnerabilidades y debilidades en los sistemas y defenderlo de posibles ataques.

Se recomienda desarrollar estrategias de educación en seguridad informática y de la información dentro de las organizaciones junto con la implementación de medidas correctivas en caso de un incidente informático.

Se recomienda la actualización permanente del software y hardware en los equipos informáticos y en las redes digitales en las organizaciones, para prevenir y corregir vulnerabilidades.

Se recomienda no utilizar software “pirata” o no licenciado ya que deja en riesgo y vulnerable los sistemas informáticos de la organización.

Se recomienda la contratación de personal profesional especializado en seguridad informática y de la información para un constante monitoreo de los sistemas de la organización.

BIBLIOGRAFÍA

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

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

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. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24). https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf
.

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

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

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

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

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27). https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

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

Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35). https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19). https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Mintic. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57). https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

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

ANEXOS

ANEXO A. PRESENTACIÓN

Se anexa al documento la presentación del Informe capacidades técnicas, legales y de gestión para equipos blue team y red team en el siguiente enlace:

Drive:
https://docs.google.com/presentation/d/1NPUe3DmiDF20-bxCrTggB3UF5VLLQB73/edit?usp=sharing&ouid=100106421197659878372&rtpof=true&sd=true

ANEXO B. VÍDEO DE SUSTENTACIÓN

Se anexa al documento el video de la sustentación del informe capacidades técnicas, legales y de gestión para equipos blue team y red team en el siguiente enlace:

Drive:
https://drive.google.com/file/d/1hgLHcTrmJPJ5YzIOokS_Vo6-ijATFV7S/view?usp=sharing