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

LILIANA CAROLINA ROJAS ALVARADO

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

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

LILIANA CAROLINA ROJAS ALVARADO

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

Luis Fernando Zambrano Hernández
Director

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

CONTENIDO

Pág.

INTRODUCCIÓN 13
1. DEFINICIÓN DEL PROBLEMA 14
1.1 ANTECEDENTES DEL PROBLEMA 15
1.1.1 Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. 15
1.1.2 Metodología para la Detección de Vulnerabilidades en Redes de Datos 15
1.2 FORMULACIÓN DEL PROBLEMA 16
2. JUSTIFICACIÓN 17
3. OBJETIVOS 18
3.1 OBJETIVO GENERAL 18
3.2 OBJETIVOS ESPECÍFICOS 18
4. MARCO REFERENCIAL 19
4.1 MARCO TEÓRICO 19
4.1.1 Seguridad Informática 19
4.1.2 Las Amenazas 19
4.1.3 Redes de Computadoras 20
4.1.4 *Firewall* 20
4.1.5 *Red Team* o Seguridad Ofensiva 21
4.1.6 *Blue Team* o Seguridad Defensiva 22
4.2 MARCO LEGAL 22
4.2.1 Normatividad Internacional 22
4.2.2 Normatividad Nacional 24
5. DESARROLLO DE LOS OBJETIVOS 26
5.1 DESARROLLO OBJETIVO 1 – ANALIZAR LA NORMATIVIDAD VIGENTE EN TEMAS RELACIONADOS CON LA PROTECCIÓN DE DATOS PERSONALES Y DELITOS INFORMÁTICOS APLICABLE A LA IMPLEMENTACIÓN DE EQUIPOS *RED TEAM* Y *BLUE TEAM* CON EL PROPÓSITO DE DETERMINAR SU MARCO LEGAL. 26
5.1.1 Margen Legal en Colombia para Delitos Informáticos y Protección de Datos Personales 26
5.1.2 Análisis de la normatividad Vigente 28
5.1.3 Análisis de Acuerdo de Confidencialidad descrito en el caso de estudio desde la perspectiva legal y no ética 30
5.1.4 Estudio desde la perspectiva legal y ética del caso “Operación Andromeda Buggly” 33

5.2 DESARROLLO OBJETIVO 2 – ELABORAR PRUEBAS DE *PENTESTING* CON EL FIN DE IDENTIFICAR POSIBLES FALLOS Y VULNERABILIDADES. ...34
5.2.1 Descripción del ataque 34
5.2.2 Montaje del Banco de Trabajo....35
5.2.3 Fases del Test de Penetración....44
5.2.3.1 Recolección de Información....46
5.2.3.2 Búsqueda de Vulnerabilidades 48
5.2.3.3 Explotación de Vulnerabilidades 57
5.2.3.4 Post explotación....69
5.2.3.5 Informe....71
5.2.4 Herramientas para ejecución del Test de Penetración....71
5.2.4.1 Pre – Ataque o Recolección de Información....71
5.2.4.2 Búsqueda de vulnerabilidades 74
5.2.4.3 Explotación de vulnerabilidades....75
5.2.4.4 Post explotación....75
6.3 DESARROLLO DEL OBJETIVO 3 – DESARROLLAR EL ANÁLISIS E IDENTIFICACIÓN DE VULNERABILIDADES CON EL FIN DE DETERMINAR LAS ACTIVIDADES DE CONTENCIÓN NECESARIAS PARA MITIGARLAS....77
6.3.1 Análisis de Vulnerabilidades y Acciones de Contención 77
6.3.1.1 Análisis de Vulnerabilidades 77
6.3.1.2 Acciones de Contención 78
6.3.2 Medidas de Hardenización. 80
6.3.3 Diferencias entre equipos de Blue Team y el de Respuesta a Incidentes Informáticos 82
6.3.4 Análisis CIS "*Center for Internet Security*" 82
6.3.5 Características y Funciones de un SIEM....84
6.3.5.1 Características....84
6.3.5.2 Funciones....85
6.3.5.3 Ventajas 85
6.3.6 Herramientas de contención *Hardware* y *Software* 86
6.3.6.1 Hardware....86
6.3.6.2 Software 87
7 LINK VIDEO DE SUSTENTACION....88
8 CONCLUSIONES 89
9 RECOMENDACIONES....90
10 BIBLIOGRAFÍA 91
11 ANEXOS 97

LISTA DE TABLAS

Pág.

Tabla 1. Fases del Test de Penetración 45
Tabla 2. Comparativo *Blue Team Vs*. Equipo de Respuesta a Incidentes.....82

LISTA DE FIGURAS

Pág.

Figura 1. Diagrama de ataque 35
Figura 2. Descarga de Virtual Box versión 6.1.36....35
Figura 3. Virtual Box instalado en su versión 6.1.36....36
Figura 4. Instalación maquina Kali en Virtual Box....36
Figura 5. Maquina Kali en Virtual Box instalada 37
Figura 6. Maquina *Windows* 7 64 bits en *Virtual Box* instalada 37
Figura 7. Instalación maquina *Windows 7 32 Bits* en *Virtual Box* 38
Figura 8. Configuración del segmento de red del Banco de Trabajo 38
Figura 9. IP Kali Linux....39
Figura 10. IP Windows 7 64 bits 39
Figura 11. Ejecución comando *PING* en la maquina *Windows 7 64 bits* 40
Figura 12. Ejecución comando *PING* en la maquina *Windows 7 32 bits* 40
Figura 13. Características técnicas maquina *Kali Linux*....41
Figura 14. Características técnicas maquina *Windows* 7 64 *bits* 42
Figura 15. Configuración sistema *Windows 7 64 bits* 42
Figura 16. Características técnicas maquina *Windows 7 32 bits* 43
Figura 17. Configuración sistema *Windows 7 32 bits* 44
Figura 18. Versión nmap instalada en la maquina *Kali Linux* 46
Figura 19. Salida del comando NMAP para el escaneo de la red....47
Figura 20. Salida del comando NMAP para la IP 10.0.2.4....47
Figura 21. Salida del comando *NMAP* para la IP 10.0.2.5....48
Figura 22. Herramienta *Nessus* instalada en la maquina *Kali Linux*....49
Figura 23. Ingreso de la IP a analizar en la herramienta *Nessus* 49
Figura 24. Envío de análisis a la maquina indicada....50
Figura 25. Resumen de análisis de vulnerabilidades maquina 10.0.2.5 51
Figura 26. Reporte detallado de las vulnerabilidades halladas....51
Figura 27. Vulnerabilidad MS11-030....52
Figura 28. Vulnerabilidad sistema operativo sin soporte....53
Figura 29. Vulnerabilidad *SMB Remote Windows* 54
Figura 30. Vulnerabilidad *SMB signing not required*....55
Figura 31. Vulnerabilidad MS16-047 *Security Update for SAM and LSAD Remote Protocols*....56
Figura 32. Reporte vulnerabilidades maquina *Windows* de 64 *bits* con IP 10.0.2.4 57
Figura 33. Herramienta *Metasploit* desplegada en la maquina *Kali Linux* 58
Figura 34. Listado de *exploits* asociados a la vulnerabilidad MS17-010 SMB *Remote Windows*....59
Figura 35. Opciones de configuración del *exploit* 60
Figura 36. Parámetro RHOTS asignado....61
Figura 37. Cargue y ejecución del *exploit* 61
Figura 38. Pantalla azul generada por la ejecución del *payload*....62

Figura 39. *Payload* ejecutado sin establecer sesión con maquina objetivo 63
Figura 40. Arquitectura del *payload* ejecutado.....64
Figura 41. Instalación herramienta *wine32* 64
Figura 42. Descarga desde *Git* el script a ejecutar 65
Figura 43. *Script* en la ruta del *framework Metasploit* 65
Figura 44. *Exploit* descargado *eternalblue_doublepulsar* 66
Figura 45. Parámetros *exploit eternalblue_doublepulsar*.....66
Figura 46. Asignación de parámetros *eternalblue_doublepulsar* 67
Figura 47. Maquina objetivo vulnerada 67
Figura 48. Ejecución de instrucciones con información de la maquina objetivo 68
Figura 49. Búsqueda del archivo "*winse2020.exe"* 68
Figura 50. Pantalla del contenido del archivo "winse2020.exe" 69
Figura 51. Consola *Shell* en la maquina atacada.....69
Figura 52. Verificación directorio usuario 70
Figura 53. Archivo creado en directorio de usuario.....70
Figura 54. Informe generado por la herramienta *Nessus*.....71
Figura 55. *Virtual Box* versión 6.1.36 72
Figura 56. Maquina *Kali Linux* versión 2020 73
Figura 57. Comando *NMAP* ejecutado 74
Figura 58. Herramienta *Nessus* instalada y ejecutada.....74
Figura 59. Ejecución de comandos en *Metasploit*.....75
Figura 60. Ejecución de comandos con la herramienta CMD 76
Figura 61. Informe herramienta *Nessus*.....76
Figura 62. Controles *CIS* 83

LISTA DE ANEXOS

ANEXO A. Caso de estudio 97
ANEXO B. Acuerdo de Confidencialidad 99
ANEXO C. Reporte Herramienta *Nessus* 103

GLOSARIO

AMENAZA: “es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información”[1]

ATAQUE FUERZA BRUTA: es una técnica a través de la cual por medio de reiterados intentos a manera de prueba y error quien ataca pretende establecer datos de acceso de la víctima tales como contraseña, nombre de usuario o códigos de acceso con el propósito de ingresar a un sistema.

BLUE TEAM: son equipos de expertos en temas ciberseguridad multidisciplinarios capaces de analizar los comportamientos de los sistemas y el de sus usuarios con el propósito de establecer lineamientos que permitan a una organización prepararse ante un ataque a la seguridad.

COPNIA (CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA): es una entidad pública encargada controlar, inspeccionar y vigilar el ejercicio de la profesión de ingeniera y afines, en Colombia.

CSIRT: Equipo de Respuesta ante Emergencias Informáticas, son centros que dan respuesta a incidentes de ciber seguridad.

CVE: “los puntos vulnerables y las exposiciones comunes (CVE) conforman una lista de fallas de seguridad informática que se encuentra disponible al público. Cuando alguien habla de un CVE, se refiere a una falla a la cual se le asignó un número de identificación.”[2]

DELITO INFORMATICO: corresponde a actividades por fuera de la ley con el propósito de irrumpir en los sistemas informáticos sin autorización para lucrarse de ello o generando acciones de sabotaje en los sistemas.

EXPLOIT: es un *software* o una parte de este o una secuencia de comandos que se aprovecha de un error o vulnerabilidad con el objetivo de generar un comportamiento no contemplado del *software*, *hardware* o dispositivo electrónico.

---

[1] INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [En línea]. 20 de Marzo 2017. Consultado el 25 de Noviembre del 2021. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[2] REDHAT. El concepto de CVE. [En línea]. 20 de Noviembre 2020. Consultado el 25 de Noviembre del 2021. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

HARDENING: es proceso de endurecimiento de la infraestructura de TI con el propósito de mitigar las vulnerabilidades y así prevenir los ataques.

INCIDENTES DE SEGURIDAD: actividades a través de las cuales se accede o se intenta acceder a una infraestructura de TI para quebrantar los pilares de la seguridad informática.

FIREWALL: “son programas de *software* o dispositivos de *hardware* que filtran y examinan la información que viene a través de su conexión a Internet. Representan una primera línea de defensa porque pueden evitar que un programa malicioso o un atacante obtengan acceso a su red y a su información antes de que se produzca cualquier posible daño”[3].

PENTESTING: o Prueba de Penetración es un proceso por medio del cual se busca ingresar a un sistema informático con el fin de identificar las debilidades en seguridad y a aquello a lo que se puede acceder a través de estas.

RED TEAM: corresponde a un grupo de expertos en Seguridad con capacidades técnicas para realizar ataques a objetivos específicos establecidos con anterioridad por el cliente dentro de lo acordado en un contrato de confidencialidad para explotar vulnerabilidades y fallas en sistemas y equipos.

RIESGOS DE SEGURIDAD: es la probabilidad de ocurra la materialización de una amenaza en Seguridad.

VULNERABILIDAD: es una falla o debilidad de una infraestructura de TI que puede representar un riesgo para los activos de información de las empresas donde se puede ver afectada su integridad, confidencialidad o disponibilidad.

[3] MCAFEE. ¿Qué es un firewall? [Sitio Web]. Consultado el 25 de Noviembre del 2021. Disponible en: https://www.mcafee.com/es-co/antivirus/firewall.html

RESUMEN

El presente documento contiene el informe técnico correspondiente a las actividades desarrolladas en el Seminario Especializado Equipos Estratégicos en Ciber seguridad *Red Team* y *Blue Team* estructurado en fases que representan el desarrollo de los objetivos propuestos y que permiten definir las funciones, responsabilidades y roles de los equipos *Red Team* y *Blue Team*.

Las fases desarrollan lo siguiente:

1. Análisis Ético – Legal: se realiza un estudio repasando la legislaion vigente en el país relacionada con la seguridad informática que sirve de marco para las actuaciones de los equipos *Red Team* y *Blue Team* asi como lo relacionado con la actuación ética de los profesionales.

2. Ejecución de Pruebas de *Pentesting*: desde el punto de vista de un equipo *Red Team* se lleva a cabo un ejercicio de *Pentesting* de acuerdo con el caso de estudio propuesto identificando el alcance de la explotación de las vulnerabilidades identificadas.

3. Análisis de Vulnerabilidades: al identificar las vulnerabilidades presentes en el escenario del caso de estudio se realiza un análisis de las mismas con el fin de establecer su impacto en caso de explotación y las actividades que se deben llevar a cabo para mitigarlo.

4. Determinar medidas de Contención: se elaboran lineamientos para la contención del ataque ilustrado y se establecen medidas de hardenizacion de la infraestructura de TI desde un punto de vista de un equipo Blue team con el fin de prevenir ataques futuros.

5. Conclusiones y Recomendaciones: en este capítulo se generan las conclusiones del ejercicio realizado y las recomendaciones que puedan servir de mejora a la infraestructura de TI del caso de estudio propuesto.

A través de estas actividades es posible identificar las actividades que se llevan a cabo para la implementación de equipos de Ciberseguridad *Red Team* y *Blue Team* y su importancia a la hora de poner a salvo los diferentes activos de información de una Infraestructura de TI.

PALABRAS CLAVE: *Blue Team*, Ciberseguridad, Hardenizacion, *Pentesting*, *Red Team,*

ABSTRACT

This document contains the technical report corresponding to the activities developed in the Specialized Seminar Strategic Teams in Cyber Security Red Team and Blue Team structured in phases that represent the development of the proposed objectives and that allow defining the functions, responsibilities and roles of the teams. RedTeam and BlueTeam.

The phases develop the following:

1. Ethical - Legal Analysis: a study is carried out reviewing the current legislation in the country related to computer security that serves as a framework for the actions of the Red Team and Blue Team teams as well as that related to the ethical performance of professionals.

2. Execution of Pentesting Tests: from the point of view of a Red Team, a Pentesting exercise is carried out in accordance with the proposed case study, identifying the scope of the exploitation of the identified vulnerabilities.

3. Analysis of Vulnerabilities: when identifying the vulnerabilities present in the scenario of the case study, an analysis of them is carried out in order to establish their impact in case of exploitation and the activities that must be carried out to mitigate it.

4. Determine Containment measures: guidelines are drawn up for the containment of the illustrated attack and hardenization measures of the IT infrastructure are established from a Blue team point of view in order to prevent future attacks.

5. Conclusions and Recommendations: in this chapter the conclusions of the exercise carried out and the recommendations that can serve to improve the IT infrastructure of the proposed case study are generated.

Through these activities it is possible to identify the activities that are carried out for the implementation of Red Team and Blue Team Cybersecurity teams and their importance when it comes to safeguarding the different information assets of an IT Infrastructure.

KEY WORDS: Blue Team, Cybersecurity, Hardening, Pentesting, Red Team.

INTRODUCCIÓN

Sin duda alguna las organizaciones hoy en día están más inmersas en el mundo digital, esto sin duda ha representado muchas ventajas competitivas y de presencia en el mercado, pero viene de la mano de una nueva amenaza, la Ciber Delincuencia. Esto implica que las organizaciones deben ahora realizar acciones para protegerse de esta amenaza latente y cada día cambiante.

Para ello se han implementado equipos de seguridad tales como *Red Team* y *Blue Team* que tienen como principal propósito salvaguardar el activo más importante de cualquier organización como lo es su información la cual en buena parte reposa en una Infraestructura de TI. Estos equipos de seguridad realizan sus actividades bajo una serie de normatividad legal que establece el cumplimiento normativo en materia de seguridad que debe realizar una organización. Las actividades de un equipo *Red Team* se enmarcan en identificar las maneras de explotar las vulnerabilidades identificadas mientras que las de un equipo *Blue Team* tienen un enfoque más de análisis y prevención, juntos estos equipos logran establecer las estrategias que en materia de seguridad debe tomar la organización para prevenir la acción de los ciber delincuentes.

En el desarrollo de este informe se abarcará a través de un caso de estudio, todas las capacidades de los equipos *Red Team* y *Blue Team* partiendo de la base normativa hasta la generación de recomendaciones que ayudan a la mejora de la seguridad en el caso propuesto.

1. DEFINICIÓN DEL PROBLEMA

Claramente la pandemia del *Covid* 19 volcó a las organizaciones, clientes y/o usuarios migrar sus actividades cotidianas hacia la *Web*, de la misma manera es claro que también lo hicieron los Cibercriminales, situación que obliga a las organizaciones a establecer medidas para salvaguardar sus activos de información, infraestructura de TI y la seguridad de sus usuarios o clientes.

A lo largo el año 2020 se presentó un aumento sustancial en el tráfico de internet donde según el informe de la Comisión de Regulación de Comunicaciones CRC "Para el caso de Colombia, al analizar el tráfico mensual de Internet, para el año 2020, se evidencia un crecimiento significativo en el mes de marzo con 38,5% comparado con el mes inmediatamente anterior, lo que en términos absolutos representa un aumento de 583 millones de GB, ocasionado principalmente por el inicio del aislamiento social"[20] lo que demuestra el aumento en la realización de actividades que utilzian medios digitales y que conlleva a las organizaciones a establecer acciones que permitan mantener seguros sus sistemas e Infraestructuras de TI a través de la implementación de equipos *Red Team* y *Blue Team*.

Estos equipos de *Red Team* y *Blue Team* elaboran lineamientos a través de las cuales es posible para las organizaciones identificar aquellas falencias en sus sistemas y redes de datos, así como establecer las actividades necesarias e inversiones a realizar asociadas a ciber seguridad para salvaguardar su información cada día se ve más expuesta a intrusiones o sabotajes dada su incursión en el mundo digital. Hoy todo el *core* de las empresas se han ido migrando al mundo digital haciendo que las organizaciones se vean expuestas a nuevas amenazas que constantemente cambian en materia de técnicas y herramientas, la incursión de los equipos *Red Team* y *Blue Team* en las organizaciones contribuye a tomar oportunamente, por lo que es importante conocer la relevancia de sus actividades en la seguridad informática y su aporte a la salvaguarda del activo más preciado en una organización como lo es su información.

[20] Comisión de Regulación de Comunicaciones. CRC presenta informe sobre comportamiento del servicio de Internet desde el inicio del estado de Emergencia por COVID-19. [En Línea]. [2021]. [Consultado el 4 de octubre del 2021] Disponible en: https://www.crcom.gov.co/es/noticia/crc-presenta-informe-sobre-comportamiento-del-servicio-de-internet-desde-el-inicio-del-estado-de-emergencia-por-covid-19

1.1 ANTECEDENTES DEL PROBLEMA

A continuación, se presentan una serie de trabajos relacionados con la situación problemática.

1.1.1 Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios.

"Titulo: *Vulnerability Detection Tool using Banner Grabbing.*

Autor: Franco, David A; Perea, Jorge L; Tovar, Luis C.

Temas: Vulnerabilidad de Redes; Servicios de Red; Seguridad; Pruebas de Penetración; Identificación de Servicios; *Network Vulnerabilities*; *Network Services*; *Security*; *Penetration Test*; *Banner Grabbing.*

En: Información tecnológica, 2013, Vol. 24(5), pp.13-22 [Revistas arbitradas].

Descripción: El objetivo principal de este trabajo fue diseñar un nuevo enfoque para la detección y evaluación de vulnerabilidades en equipos de red mediante la técnica de identificación de servicios. Este enfoque consiste en determinar los nombres y versiones de los servicios activos en un equipo de red para luego buscar las vulnerabilidades de seguridad de los mismos en la Base de Datos Nacional de Vulnerabilidades".[21]

1.1.2 Metodología para la Detección de Vulnerabilidades en Redes de Datos

"Titulo: *Methodology for Detecting Vulnerabilities in Data Networks.*

Autor: Franco, David A; Perea, Jorge L; Puello, Plinio.

Temas: Detección De Vulnerabilidades; Enumeración de Servicios; Escaneo de Puertos; Seguridad Informática; *Vulnerability Detection*; *Service Enumeration*; *Port Scanning*; Information Security

En: Información tecnológica, 2012, Vol.23 (3), pp.113-120 [Revistas arbitradas].

---

[21] FRANCO, David A; PEREA, Jorge L y TOVAR, Luis C. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Información. Tecnológica. [En línea]. 2013, vol.24, n.5, pp.13-22. Consultado el 27 de Noviembre del 2021. Disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003&lng=es&nrm=iso

.

Descripción: este trabajo tuvo como objetivo principal diseñar una metodología que permita la detección de vulnerabilidades en las redes de datos"[22]

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo a través de la implementación de los equipos *Red Team* y *Blue Team* en un caso de estudio, se pueden establecer las capacidades técnicas y legales de estos equipos que permiten mitigar el riesgo de Ciber seguridad en una organización?

[22] FRANCO, David A; PEREA, Jorge L y PUELLO, Plinio. Metodología para la Detección de Vulnerabilidades en Redes de Datos. Información. Tecnológica. [En línea]. 2012, vol.23, n.3, pp.113-120. Consultado el 27 de Noviembre del 2021. Disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014&lng=es&nrm=iso

2. JUSTIFICACIÓN

La realización de este informe tiene su razón de ser en la necesidad de documentar las actividades asociadas a la implementación de equipos *Red Team* y *Blue Team* donde se realizan acciones para la identificación y análisis de vulnerabilidades en una Infraestructura de TI así como las actividades que se deben llevar a cabo para el endurecimiento de la Infraestructura en pro del manejo y mitigación de estas, todo bajo el marco de una legislación vigente en el país que determina el procedimiento a realizar mediante la virtualización de escenarios a través de los cuales es posible identificar las acciones para proteger a las organizaciones de estos incidentes.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer las capacidades Técnicas, Legales y de Gestión de Equipos *Red Team* y *Blue Team* mediante la elaboración de un informe técnico basado en el análisis de un caso de estudio.

3.2 OBJETIVOS ESPECÍFICOS

Analizar la normatividad vigente en temas relacionados con la Protección de Datos Personales y Delitos informáticos aplicable a la implementación de equipos *Red Team* y *Blue Team* con el propósito de determinar su marco legal.

Elaborar pruebas de *Pentesting* con el fin de identificar posibles fallos y vulnerabilidades.

Desarrollar el análisis e identificación de vulnerabilidades con el fin de determinar las actividades de contención y hardenizacion necesarias para mitigarlas.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Seguridad Informática. El propósito principal de la Seguridad Informática consiste en ofrecer la garantía que los recursos dispuestos por una organización en relación a infraestructura de TI y sus sistemas e infraestructura tengan un uso según lo determinado y que su acceso y modificación se encuentre habilitado únicamente al personal autorizado.

La seguridad de la información se debe encontrar bajo el marco de sus pilares fundamentales:

- Confidencialidad: se relaciona con la reserva de información y la capacidad de limitar el acceso a únicamente personas o programas autorizados.
- Integridad: propiedad que garantiza que un activo de información no se ha modificado y a la capacidad de establecer que el documento original no ha sufrido modificaciones.
- Disponibilidad: se relaciona con la capacidad de un sistema en garantizar que la información que allí de encuentre sea posible recuperarla tan pronto esto sea requerido.

4.1.2 Las Amenazas. Las amenazas son aquellas situaciones o características que le pueden llegar a permitir que un atacante acceda a cualquier tipo de dispositivo electrónico para así tomar de forma ilegal información a la cual no esta autorizado.

4.1.2.1 Amenazas Lógicas. Las amenazas lógicas hacen referencia a cualquier tipo de *software* que puede llegar generar daños en un sistema de manera intencionada o por error, aquí se tiene entre otros:

Software Incorrecto: Hace referencia programas con errores de codificación programas o *bugs.*

Puertas Trasera: Son partes de código que permanecen sin ejecutar hasta tanto son activados por un atacante que accede sin ser detectado.

Virus: es un tipo de *malware* que altera el funcionamiento de una máquina y que se puede propagar entre los equipos de una red usando otro programa o archivo.

Caballos de Troya: estos programas que ejecutan instrucciones de manera oculta simulando realizar operaciones normales.

4.1.2.2 Amenazas Físicas. Hacen referencia a los daños daños en el hardware que pueden darse en cualquier momento como por ejemplo daños en disco duros, errores en funcionamiento de la memoria entre otros, así como también los desastres naturales.

Acceso Físico: Hace referencia al acceso a un recurso que genera riesgo con un impacto alto ya que cuando es accedido no existe seguridad sobre él.

Radiaciones Electromagnéticas: son las señales que emiten los dispositivos digitales y son susceptibles de ser atacadas, como por ejemplo, la interceptación de las señales enviadas a través de una red *WiFi*.

Desastres Naturales: se encuentra asociado a los diferentes fenómenos naturales que pueden impactar a una infraestructura de TI.

Criminalidad: se dan por acciones hostiles sobre la infraestructura de TI como robo, fraude o sabotaje.

4.1.3 Redes de Computadoras. "Una red de computadoras es una interconexión de computadoras para compartir Información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico"[23].

Las redes se comunican entre sus elementos a través de protocolos de red.

Equipos en una Red de Computadoras

Los dispositivos que conforman una red de computadoras generan, envian o reciben datos, estos pueden incluir, computadoras personales, *switch*, servidores, *firewall* entre otros.

4.1.4 *Firewall.* "Es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permitir o bloquear tráfico específico según un conjunto definido de reglas de seguridad. Los cortafuegos han sido una primera línea de defensa en seguridad de redes durante más de 25 años. Un *firewall* puede ser *hardware*, *software* o ambos"[24]

Tipos de *Firewall:* Los *Firewall* poseen la siguiente clasificación donde principalmente se tienen:

---

[23] ALEGSA. Definición de Red de computadoras. [2018]. [Sitio Web]. Consultado el 27 de Noviembre del 2021. Disponible en: https://www.alegsa.com.ar/Dic/red_de_computadoras.php

[24] CISCO. What Is a Firewall? [En Línea]. [2021] [Consultado el 6 de octubre del 2021]. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

- Firewall *Software*: Son programas instalados en un ordenador incluidos en el sistema operativo y que ofrece protección al equipo en el que se encuentra instalado y no a los demás dispositivos de la red.

- Firewall de *hardware*: Estos equipos se ubican antes del en el *router* utilizado para acceder a Internet y, por ende, por lo que pueden ofrecer protección a todos los ordenadores de una red.

- Firewall en Cloud: funciona de igual manera que los Firewall tradicionales pero bajo un entorno de servicios *Cloud* que se puede desplegar directamente desde la tienda de la plataforma de acuerdeo con las necesidades de la organización.

Ventajas del *Firewall*:

- Monitoreo y registro de los servicios asociados al *Internet*, *FTP* y entre otros protocolos.

- Construyen una "barrera" excluyendo las conexiones no autorizadas.

- Previenen de ataques generados desde otras redes externas.

- Controlan de actividades inusuales la red y a cada uno de los dispositivos conectados.

- Controlan el uso apropiado del acceso a internet realizando bloqueos de material no permitido según las políticas de la organización.

Desventajas del *Firewall*:

- Disminución en el rendimiento del equipo

- Imposibilidad de acceso a algunos sitios *web* sin justificación

4.1.5 *Red Team* o Seguridad Ofensiva. Son equipos conformados por *hackers* éticos cuyo personal posee habilidades técnicas en seguridad que con autorización de la organización simula una amenaza con el fin de vulnerar los controles de seguridad evaluando la eficacia de los controles existentes o no en la organización.

Actividades realizadas por un *Red Team*

Generar un plan de las actividades a realizar en el sistema objetivo.

Recopilar la mayor cantidad posible de información del sistema objetivo.

Elaborar plan de acción para ataque de vulnerabilidades identificadas.

Emplear diversas técnicas para proceder a la explotación de vulnerabilidades

Realizar la documentación del proceso.

4.1.6 *Blue Team* o Seguridad Defensiva. Estos equipos conocen los objetivos del negocio y establecen la estrategia en materia de ciber seguridad que debe adoptar la organización para protegerse de futuros ataques.

Actividades realizadas por un *Blue Team*

Identificar los activos críticos de la organización y sus vulnerabilidades.

Realizar un análisis de riesgos.

Establecer las acciones necesarias para mitigar el impacto de los ataques en el negocio.

4.2 MARCO LEGAL

4.2.1 Normatividad Internacional

4.2.1.1 Estándar ISO/IEC 17799. "Debido a la necesidad de hacer segura la información que poseen las organizaciones era necesaria la existencia de alguna normativa o estándar que acogiera todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente frente a todos los probables incidentes que pudieran afectarla por esta necesidad apareció el BS 7799 o estándar para la gestión de la seguridad de la información, el cual es un estándar desarrollado por el *British Standard Institute* en 1999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad de la información dentro de la organización. Esta normativa británica acabó desembocando en la actual ISO/IEC 17799:2000 – *Code of Practice Information Security Management*."[25]

[25] MEJÍA LONDOÑO Cesar Augusto, RAMÍREZ GALVIS Nini Johana y RIVERA CARDONA Juan Sebastián. Vulnerabilidad, Tipos de Ataques y Formas de Mitigarlos en las Capas del Modelo OSI

ISO/IEC 17799 (también ISO 27002) es un estándar para la seguridad de la información el cual por primera vez fue publicado en el año 2000 bajo la denominación de ISO/IEC 17799:2000 por la International *Organization for Standardization* y por la Comisión *International Electrotechnical Commission* y con el título de *Information Technology - Security Techniques - Code of Practice For Information Security management*. La versión más reciente de los aspectos del estándar se publicó en el año 2013, el documento con la actualización es denominado ISO/IEC 27002:2013.

4.2.1.2 Estándar ISO/IEC 27001. "Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido Ciclo de *Deming*: PDCA - acrónimo de *Plan*, *Do, Check, Act* (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la *British Standards Institution (BSI)."*[26]

La norma Internacional ISO/IEC 27001 que es la única auditable y establece los requisitos que se requieren para llevar a cabo la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). La norma emergió con el objetivo de garantizar aquellos de controles de seguridad adecuados. Lo que permite mantener protegidos los activos de información de las organizaciones y generando confianza a todas las partes interesadas.

4.2.1.3 Estándar ISO/IEC 27000:2013. Es parte de un grupo de normas relacionadas con los Sistemas de Gestión de Seguridad de la Información (ISMS), las "series ISO/IEC 27000".

ISO/IEC 27000, es un estándar internacional llamado "Tecnología de la Información – Técnicas de Seguridad – Sistemas de Administración de la Seguridad de la Información – Visión general y Vocabulario". Fue llevado a elaborado por el subcomité 27 (SC27) del primer Comité Técnico Conjunto (JTC1), de la ISO (*International Organization for Standardization*) y el IEC (*International Electrotechnical Commission*). La norma ISO/IEC 27000 otorga una vista a nivel general en la introducción de los estándares de la familia ISO/IEC 27000 y un vocabulario de términos de vital importancia, usados en toda la familia ISO/IEC

---

en las Redes de Datos de las Organizaciones. [En línea]. [2012]. Trabajo de Grado. Universidad Tecnológica de Pereira, Facultad de Ingenierías Eléctrica, Electrónica, Física y Ciencias de la Computación. Pp 30 – 32. Consultado el 27 de Noviembre del 2021. Disponible en: http://recursosbiblioteca.utp.edu.co/tesisd/textoyanexos/0058R173.pdf

[26] ISO. ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements. [Sitio Web]. Consultado el 27 de Noviembre del 2021. Disponible en https://www.iso.org/standard/42103.html

27000 lo que evidencia la utilización utilizan de los estándares ISO/IEC 27000 de manera conjunta para planear, implementar, certificar y operar un Sistema de Gestión de Seguridad de la información, bajo un entorno de sistemas de gestión y administración de riesgos.

4.2.2 Normatividad Nacional

4.2.2.1 Ley 1273 del 2009 Delitos Informáticos. Fue promulgada el 5 de Enero del 2019 realiza la definición de los siguientes delitos informáticos en Colombia y sus agravantes:

1. Acceso abusivo a un sistema informático.
2. Obstaculización ilegítima de sistema informático o red de telecomunicación.
3. Interceptación de datos informáticos.
4. Daño Informático.
5. Uso de *software* malicioso.
6. Violación de datos personales.
7. Suplantación de sitios *web* para capturar datos personales.
8. Hurto por medios informáticos y semejantes.
9. Transferencia no consentida de activos.

4.2.2.2 Ley 1032 del 2006. Tiene relación con la definición de delitos asociado a los derechos de autor y servicios de telecomunicaciones:

- De la prestación, acceso o uso ilegales de los servicios de telecomunicaciones.
- Violación a los derechos patrimoniales de autor y derechos conexos.
- Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones.

4.2.2.3 Ley Estatutaria 1581 de 2012. Dicta disposición en materia de protección de Datos Personales en el sentido de dar herramientas a los ciudadanos para desarrollar el derecho constitucional de conocer, actualizar y rectificar las informaciones recogidas en bases de datos o archivos y los demás derechos, libertades y garantías referidas en el artículo 15 de la Constitución Política, así como el derecho a la información referido en el artículo 20.

4.2.2.4 Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital. Es un documento establece la hoja de ruta que define los lineamientos que fortalecen las capacidades de las partes interesadas para la identificación, gestión, tratamiento y mitigación de los riesgos de seguridad digital de las actividades de distintito índole realizadas en un entorno digital, enmarcadas en la cooperación, colaboración y asistencia.

4.2.2.5 Documento CONPES 3701 de 2011 – Lineamientos de Política para la Ciberseguridad y Ciberdefensa. Es un documento que define la hoja de ruta en materia de política en ciber seguridad y ciber defensa en Colombia orientados a desarrollar una estrategia de aplicación nacional que permita neutralizar el incremento de las amenazas informáticas que pueden afectar a cualquier sector del país.

4.2.2.6 Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009. Es un marco normativo que tiene relación con la seguridad de los proveedores de redes y/o servicios de telecomunicaciones y sus servicios ofrecidos. A través de esta legislación se modifican en los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta normativa establce para los para los proveedores de redes y/o servicios de telecomunicaciones la obligatoriedad que ofrecer dentro de su catálogo de productos o servicios llevar a cabo modelos de seguridad, de acuerdo con las características y necesidades propias de la red, que ayuden a mejorar de la seguridad de las redes de acceso según los marcos de seguridad establecidos por la UIT. Así mismo, establece obligaciones para los proveedores de redes y/o servicios de telecomunicaciones en materia de la inviolabilidad de las comunicaciones y la seguridad de la información.

5. DESARROLLO DE LOS OBJETIVOS

5.1 DESARROLLO OBJETIVO 1 – ANALIZAR LA NORMATIVIDAD VIGENTE EN TEMAS RELACIONADOS CON LA PROTECCIÓN DE DATOS PERSONALES Y DELITOS INFORMÁTICOS APLICABLE A LA IMPLEMENTACIÓN DE EQUIPOS *RED TEAM* Y *BLUE TEAM* CON EL PROPÓSITO DE DETERMINAR SU MARCO LEGAL.

5.1.1 Margen Legal en Colombia para Delitos Informáticos y Protección de Datos Personales. En relación a la Protección de Datos Personales y Delitos Informáticos existen la siguiente normatividad entre otras:

- **"Ley 527 de 1999:** define y realiza la reglamentación respecto al acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales, y se determinan las entidades certificadoras entre otras"[27].

- **"Ley 603 de 2000"[28]:** hace referencia a la protección de los derechos de autor en Colombia. El *software* es definido como un activo protegido por derechos de autor el cual las empresas según esta norma deben indicar si los problemas en el *software* son de tipo legal o no.

- **"Ley 1150 de 2007"[29]:** determina aspectos relacionados con la Seguridad de la información en relación con la contratación en línea.

- **"Ley 1266 de 2008"[30]:** se establecen disposiciones generales respecto al habeas data y se reglamenta el manejo de la información de datos personales en bases de datos financieras, crediticias, comerciales, de servicios y la provenientes de terceros países, entre otros.

---

[27] SENADO DE LA REPÚBLICA DE COLOMBIA. Ley 527 de 1999. [En Línea]. [2022]. [Consultado el 31 de agosto del 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

[28] SENADO DE LA REPÚBLICA DE COLOMBIA. Ley 603 de 2000. [En Línea]. [2022]. [Consultado el 31 de agosto del 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0603_2000.html

[29] SENADO DE LA REPÚBLICA DE COLOMBIA. Ley 1150 de 2007. [En Línea]. [2022]. [Consultado el 31 de agosto del 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1150_2007.html

[30] SENADO DE LA REPÚBLICA DE COLOMBIA. Ley 1266 de 2008. [En Línea]. [2022]. [Consultado el 31 de agosto del 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

- **“Ley 1273 de 2009”[31]:** se realiza la modificación del Código Penal donde se crea un nuevo bien jurídico denominado "de la protección de la información y de los datos" y se realiza la preservación de los sistemas que hacen uso de las *TIC* entre otras disposiciones.

- **“Decreto 2952 de 2010”[32]:** defina la reglamentación asociada a los artículos 12 y 13 de la Ley 1266 de 2008.

- **“Ley Estatutaria 1581 de 2012”[33]:** se desarrolla el propósito del derecho constitucional de *Habeas Data* a través del conocimiento, actualización y rectificación de los datos almacenados en bases de datos o archivos, y las garantías del cumplimiento de los artículos 15 y 20 de la Constitución Política.

- **“Decreto 1377 de 2013”[34]:** reglamenta de manera parcial la Ley 1581 de 2012 respecto a la Protección de Datos.

- **“Ley 1712 de 2014”[35]**: esta norma crea la “Ley de Transparencia y Derecho de acceso a la Información Pública” y define los procedimientos que dan garantía del derecho.

- **“Decreto 2573 de 2014”[36]:** define como lineamiento la Seguridad y Privacidad de la Información y define acciones a nivel transversal que permiten proteger la información de acceso, divulgación o destrucción no autorizado.

---

[31] MINTIC. Ley 1273 2009. (2009). [En línea]. [Consultado el 30 de agosto del 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/ley_1273_2009.htm

[32] ALCALDIA DE BOGOTA. Decreto 2952 del 2010. (2010). [En línea]. [Consultado el 31 de agosto del 2022]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=40120&dt=S

[33] FUNCIÓN PÚBLICA. Ley 1581 de 2012. [En Línea]. [2012]. [Consultado el 30 de agosto del 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[34] FUNCIÓN PÚBLICA. Decreto 1377 de 2013. [En Línea]. [2013]. [Consultado el 29 de agosto del 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[35] FUNCIÓN PÚBLICA. Ley 1712 de 2014. [En Línea]. [2014]. [Consultado el 29 de agosto del 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

[36] FUNCIÓN PÚBLICA Decreto 2573 de 2014. [En Línea]. [2014]. [Consultado el 29 de agosto del 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60596

- **"Circular 37 de 2018"[37]:** tiene como objetivo aumentar los niveles de Ciberseguridad y establecer la respuesta ante Incidentes de ciberseguridad y define el modelo de seguridad y privacidad de la información *MPSI* del *MINTIC*.

- **"Resolución 500 de 10 de marzo de 2021"[38]:** determina los lineamientos y la estandarización de la estrategia de seguridad digital y se acoge el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

5.1.2 Análisis de la normatividad Vigente. Actualmente Colombia cuenta con reglamentación en la cual se definen los delitos informáticos y se establecen lineamientos respecto a la Protección de Datos Personales, como lo describen las normas revisadas en el punto anterior que son la Ley 1273 del 2009, la Ley Estatutaria 1581 del 2012 y el Decreto 1377 del 2013.

Allí se puede encontrar artículos que hacen referencia a las sanciones estipuladas contra los delitos que atentan a los pilares de la seguridad informática que son la confidencialidad, integridad y disponibilidad de los datos y sistemas de información.

Específicamente se dictan sanciones respecto a temas como los accesos no autorizados, la obstaculización de sistemas informáticos, interceptación y daño de sistemas informáticos, uso de *software* malicioso, suplantación de sitios *web* y hurtos a través de medios electrónicos y en la cual se definen castigos que van desde 48 a 120 meses de prisión según la gravedad del delito y que para los equipos de *Red Team* y *Blue Team* representan herramientas a través de las cuales se pueden buscar castigos legales a los que pueden verse enfrentados los ciber delicuentes que atenten contra las organizaciones en general.

Adicionalmente estas conductas son sancionadas, en el caso de cometerse por profesionales de la ingeniería, por *COPNIA*, organización que desempeña el rol en el país de entidad rectora en el ejercicio de la profesión de Ingeniería incluyendo las actividades realizadas por profesionales en Ingeniería de Sistemas y cuyos lineamientos establecen a través del Código de Ética como deberes de los profesionales "Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones"[39].

---

[37] SECRETARIA GENERAL ALCALDIA DE BOGOTA. Circular 37 de 2018. (2018). [En línea]. [Consultado el 31 de agosto del 2022]. Disponible en: https://secretariageneral.gov.co/sites/default/files/marco-legal/circular_37.pdf

[38] GOBIERNO DIGITAL. Resolución 500 de 2021. (2021). [En línea]. [Consultado el 31 de agosto del 2022]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

[39] COPNIA. Código de Ética. [2015]. [En línea]. Consultado el día 8 de Diciembre del 2021. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Respecto a la normatividad aplicable a la Protección de Datos personales se puede establecer que representa una herramienta fundamental toda vez que define los principios a cumplir por las personas u organizaciones responsables del tratamiento, manipulación, custodia y divulgación de datos personales.

Como se indicó anteriormente, el decreto 1377 del 2013 establece una definición de términos fundamentales en la protección de datos personales entre los cuales se puede ver:

Aviso de Privacidad: "Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales"[40]

Dato público: "Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva"[41]

Datos sensibles: "Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos"[42]

A través de estas herramientas legales es posible analizar el caso de estudio en materia del cumplimento de deberes éticos y normativos que pueden ser utilizados por los equipos *Red* y *Blue Team* con el objeto de brindar asesoría que va más allá de la parte técnica, sino que le permite indicar a la organización las normas violadas

---

[40] FUNCIÓN PÚBLICA. Decreto 1377 de 2013. [En Línea]. [2013]. [Consultado el 8 de Diciembre del 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[41] FUNCIÓN PÚBLICA. Decreto 1377 de 2013. [En Línea]. [2013]. [Consultado el 8 de Diciembre del 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[42] FUNCIÓN PÚBLICA. Decreto 1377 de 2013. [En Línea]. [2013]. [Consultado el 8 de Diciembre del 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

en procesos de ataques informáticos y las respectivas sanciones que se pueden dar a los implicados en estos delitos.

A su vez esta normatividad es un marco que deben tomar los equipos *Red* y *Blue Team* como principios rectores antes de establecer contractualmente sus actividades ya que independiente de las obligaciones que establezca la empresa contratante primero se debe validar que están condiciones no superen lo establecido en la norma.

Los equipos *Red* y *Blue Team* amparados en esta normatividad deben tener claro el alcance de sus funciones y establecer los límites de sus actividades dentro de este marco legal para no incurrir por falta de conocimiento en Delitos que puedan conllevar desde sanciones económicas, pasando por cancelación de su tarjeta profesional.

5.1.3 Análisis de Acuerdo de Confidencialidad descrito en el caso de estudio desde la perspectiva legal y no ética. En el análisis que se realizó al acuerdo de confidencialidad propuesto en la situación descrita del caso de estudio, suscrito entre el personal a contratar y la empresa Hackers Security donde se observan las siguientes irregularidades:

- Clausula 1 – Objeto. "... *se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Hackers Security...*"[43] aquí existe una irregularidad partiendo de que la cláusula indica que no se debe entregar información a "autoridades legales" lo que implica un incumplimiento tanto legal como ético respecto a lo contenido en la **Ley 842 del 2003 articulo 31 Deberes Generales de los Profesionales inciso E**, que reza "*Permitir el acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades de policía, a los lugares donde deban adelantar sus investigaciones y el examen de los libros, documentos y diligencias correspondientes, así como prestarles la necesaria colaboración para el cumplido desempeño de sus funciones*"[44] que corresponde al **Código de Ética para el ejercicio de profesión de ingeniería** por lo que a través de esta cláusula se está incurriendo a la comisión de una falta en el ejercicio de la profesión, seguido del apartado que hace referencia a la información relacionada con "procesos ilegales" lo que nos da a entender que la empresa realiza actividades que faltan a la normatividad existente y que al aceptar este acuerdo también se estaría faltando a

[43] Anexo C. Acuerdo de Confidencialidad. UNAD.
[44] COPNIA. Ley 842 del 2003. (9, octubre, 2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. En: Diario Oficial. Octubre, 2003. No. 45.340.

la **Ley 842 del 2003 articulo 31 Prohibiciones Generales de los Profesionales** que en su **inciso B** reza "*Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley*"[45] por parte de los firmantes ya que de esta manera al tener conocimiento de las actividades ilegales que realiza la organización se estaría tolerando la comisión del delito.

- Clausula 2 - Definición de información confidencial. "*Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos*"[33] si bien en este caso el acuerdo cumple con lo requerido en el sentido de indicar lo que define como información confidencial aquí se denota que la organización realiza la recolección de información de manera ilegal, incumpliendo lo establecido en la **Ley 1273 de 2009** en lo que respecta a los artículos **Artículo 269A Acceso abusivo a un sistema informático** y **Artículo 269C: Interceptación de datos informáticos** lo que implica en caso de firmar dicho acuerdo, ser conocedor y cómplice de los delitos indicados así como del código de ética estipulado en la **Ley 842 del 2003.** Es importante indicar que en este punto seria valido que la empresa también indicara de manera explícita las distintas exclusiones de lo que se define como información confidencial o que no es información confidencial.

- Clausula 3 - Origen de la información confidencial. "*provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial* "[33]. en esta cláusula es importante decir que si bien se cumple en el sentido de indicar el Origen de la información catalogada como Confidencial, esta no precisa que elementos "intangibles" serán considerados como confidenciales, información que es indispensable que sea indicada de manera explícita en el acuerdo ya que de la manera que se encuentra redactado es muy abierto y puede hacer incurrir a los firmantes en incumpliendo del mismo acuerdo, de igual manera se indica en la cláusula que la fuente de esta información puede ser indeterminada por lo que como firmante del acuerdo puedo incurrir en un delito ya que de acuerdo con lo indicado en las cláusulas anteriores la empresa obtiene

esta información de manera presuntamente ilegal y al aceptarlo se puede exponer a sanciones inclusive penales, también si bien no es ilegal advertir o no el carácter de confidencialidad de la información, sería una mejor practica incluir dicha advertencia con el propósito de dar garantías en la confidencialidad de la información que allí se maneja.

- Clausula 4 - Obligaciones de la parte receptora. "*Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella...numerales 3,4, 7, 8 y 9...*"[33] es una cláusula abusiva en las que se incurre al firmante a la posible complicidad de delitos que presuntamente puede cometer la compañía ya que se insta a la no denuncia lo que puede conllevar a consecuencias que pueden ser de tipo penal en caso de que las autoridades identifiquen que se tuvo conocimiento de un delito y que este se mantuvo en silencio (**Código Penal Colombiano Artículo 25. Acción y omisión**). Adicionalmente en los numerales 7 y 8 se insta a la autoincriminación cuando se puede observar que la responsabilidad en este caso sería compartida y cuando según la normatividad vigente solo se es penalmente responsable de los delitos de los cuales se le haya declarado culpable coartando el derecho de la Presunción de Inocencia. En el numeral 9 se puede observar que la empresa declara que es posible que haya adquirido de manera ilegal información lo que puede poner en alerta al firmante del acuerdo.

- Clausula 5 - Obligaciones de la parte reveladora. Esta cláusula se encuentra aparentemente incompleta, motivo por el cual el firmante del acuerdo debería abstenerse de firmarlo.

- Clausula 8 - Solución de controversias." ...*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...*"[33] Si bien la cláusula inicialmente insta a la resolución de conflictos de una manera sana, el apartado indicado en comillas insta al firmante a asumir toda la responsabilidad penal de los posibles delitos cometidos en la empresa lo cual carece de legalidad ya que como se indicó anteriormente las personas solo son responsables de aquellos delitos de los cuales se les halle culpable.

Es importante indicar que el acuerdo no contiene la cláusula 7 situación que impediría la firma del acuerdo hasta tanto no se aclare su motivo.

5.1.4 Estudio desde la perspectiva legal y ética del caso "Operación Andromeda Buggly". Para conocer respecto de la "Operación Andrómeda *Buggy*" se revisó el artículo que al respecto realizo la revista *Enter.Co* reconocida por tratar temas relacionados con la tecnología, allí se describe el modus operandi de la organización a través de la cual, mediante la captación de personas curiosas y expertas en temas de seguridad informática, así como en realizar explotación de vulnerabilidades, personal de las fuerzas militares se instruyeron de cierta manera para lograr acceder a información de manera ilegal, del proceso de paz que es ese momento se estaba llevando a cabo para venderla a terceros interesados. Todo ocurrió a través de una fachada donde funcionó un *hackerspace* (lugar donde personas en un ambiente colaborativo se realizan procesos de aprendizaje en temas relacionados con seguridad informática) allí se realizaron reuniones entre expertos y estudiosos en temas de seguridad digital pero también al parecer en estas mismas oficinas funcionarios de las fuerzas militares llevaban a cabo actividades de inteligencia a través de interceptaciones de comunicaciones de distintas personalidades del ámbito nacional, lo cual según lo manifestado por los comandantes responsables, se realizan bajo el marco de una operación militar denominada Andrómeda, sin embargo, el mismo ejercito reconoce que estas actividades no se realizaron bajo un entorno controlado lo que propendió a la comisión de delitos indicados en la Ley 1279 del 2009 tanto del personal militar como civil que hizo parte de esta operación.

Desde el ámbito legal se puede ver que en la realización de esta operación de inteligencia militar se incurrieron en varios delitos consagrados en la Ley 1279 del 2009[46], en los siguientes artículos:

"Artículo 269A: Acceso abusivo a un sistema informático".

"Artículo 269C: Interceptación de datos informáticos".

"Artículo 269F: Violación de datos personales".

Sumado a estos delitos se incurre de igual manera con las siguientes conductas agravantes teniendo en cuenta la utilización de terceros de buena fe para la realización de actividades ilegales en el caso de las personas captadas por la organización delictiva y que se están afectados sistemas informáticos estatales, esto descrito en el artículo "269H: Circunstancias de agravación punitiva en los numerales 1, 2, 4, 5, 6 y 7".

[46] COLOMBIA. SECRETARIA SENADO. Ley 1273 de 2009. (5, enero, 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. En: Diario oficial. Enero, 2009. Nro. 47.223

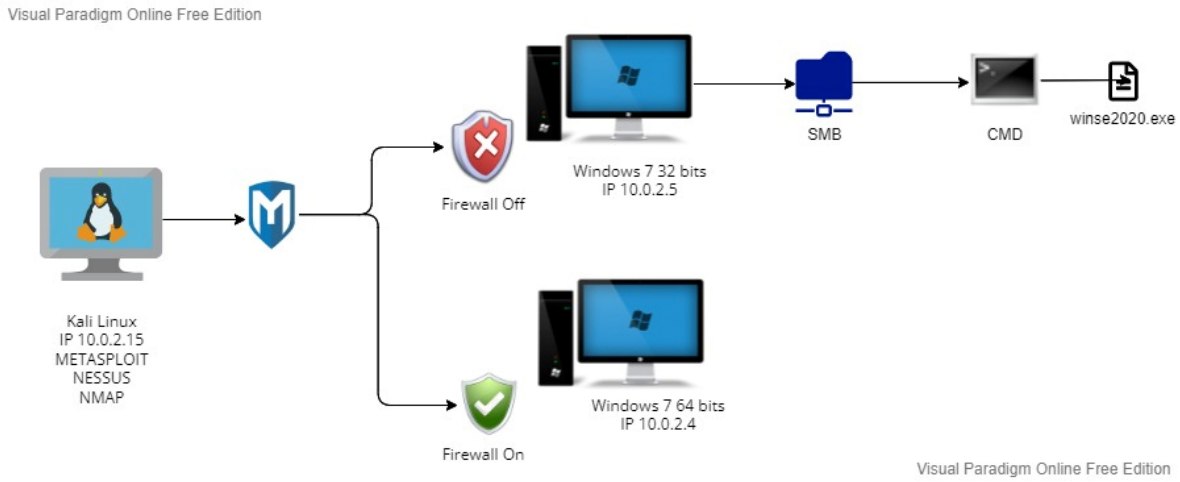
Respecto al código de ética para el ejercicio de la profesión de ingeniería de *COPNIA*, las personas involucradas en esta operación si bien no es claro si estas personas son profesionales en ingeniería en caso de que lo fueran, las sanciones a las que se vieran expuestos van hasta la perdida de la tarjeta profesional lo que acarrea el no ejercicio de la profesión.

5.2 DESARROLLO OBJETIVO 2 – ELABORAR PRUEBAS DE *PENTESTING* CON EL FIN DE IDENTIFICAR POSIBLES FALLOS Y VULNERABILIDADES.

5.2.1 Descripción del ataque. El ataque que se plantea para el desarrollo de este caso de estudio consiste en primer lugar en identificar los puertos abiertos en cada una de las maquinas mediante el uso de *NMAP*, se inicia con un escaneo de la red para de esta manera identificar cada una de las maquinas mediante su *IP*, posteriormente se realiza con la ayuda de *NMAP* una revisión a cada una de las *IP* identificadas, de esta manera se establece que maquina *Windows* de 64 bits se encuentra con el *Firewall* arriba, lo que nos ubica en la maquina *Windows* de 32 bits allí también se realiza escaneo de puertos, en caso de encontrar puertos abiertos en cualquiera de las maquinas con la ayuda de *Nessus* se procederá a revisar las vulnerabilidades presentes en cada una, validando si existe alguna vulnerabilidad relacionada con el servicio *SMB* o su puerto por defecto el 445, esto de acuerdo con el escenario planteado en el caso de estudio, lo que nos daría indicio si es por allí que la información se está filtrando. Una vez identificada la maquina con la vulnerabilidad asociada al puerto 445 y con la información suministrada de esta por la herramienta *Nessus* se procede a ejecutar el *exploit* con la herramienta *Metasploit* y el correspondiente *payload*, allí se debe evidenciar la falla reportada en el anexo escenario de la “pantalla azul” y posteriormente se debe realizar una instrucción efectiva en el equipo, con el apoyo de la herramienta *CMD* que permite navegar y ejecutar comandos dentro de la estructura de archivos del equipo vulnerable hasta llegar al archivo “*winse20w0.exe*” con el fin de demostrar la fuga de información que se estaría presentando.

La siguiente imagen ilustra el proceso realizado en el desarrollo del test de penetración según el caso de estudio planteado.

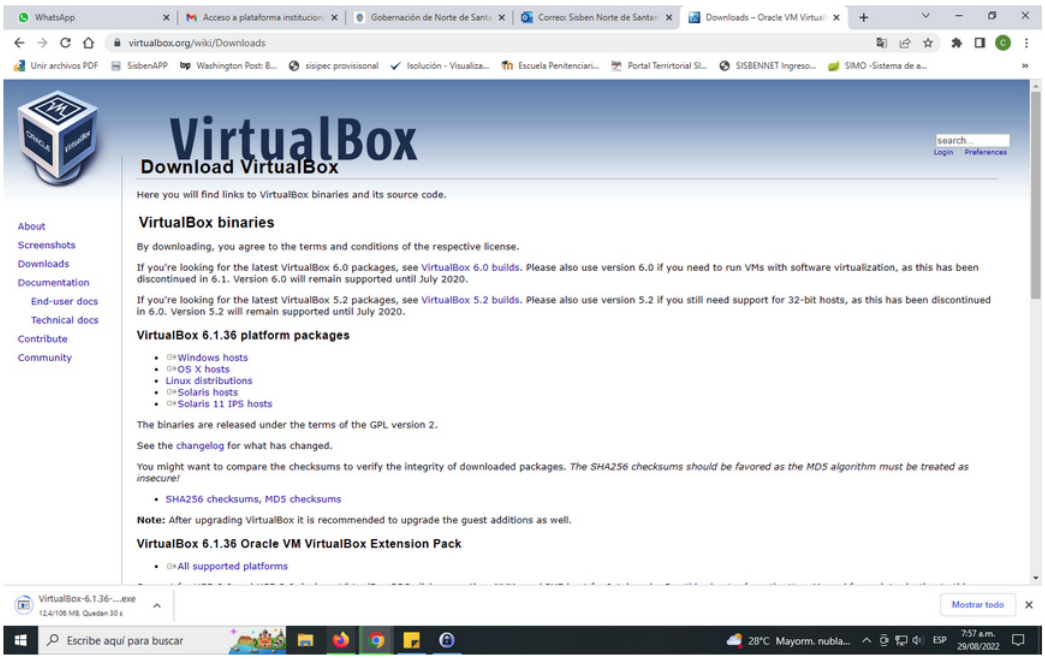
Figura 1. Diagrama de ataque



Autor. Propia

5.2.2 Montaje del Banco de Trabajo. Teniendo en cuenta lo planteado en el caso de estudio se procede a realizar el montaje de un entorno virtual de las maquina necesarias para la realización del ejercicio. Se realizó la instalación del *software* virtualizador "*Virtual Box"* en su versión 6.1.36

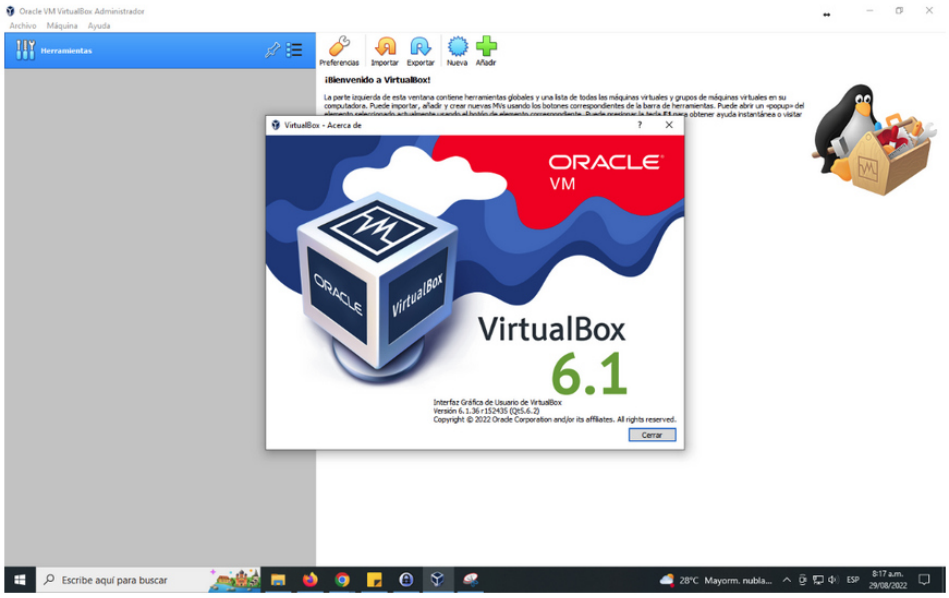
Figura 2. Descarga de Virtual Box versión 6.1.36



Autor. Propia

Posteriormente se procede a la instalación del software virtualizador “Virtual Box”.

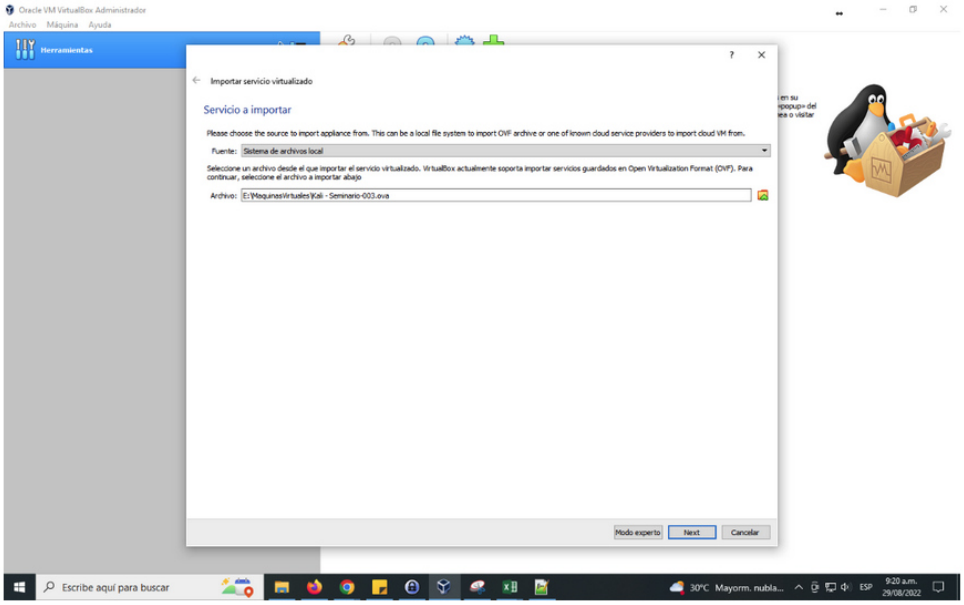
Figura 3. Virtual Box instalado en su versión 6.1.36



Autor. Propia

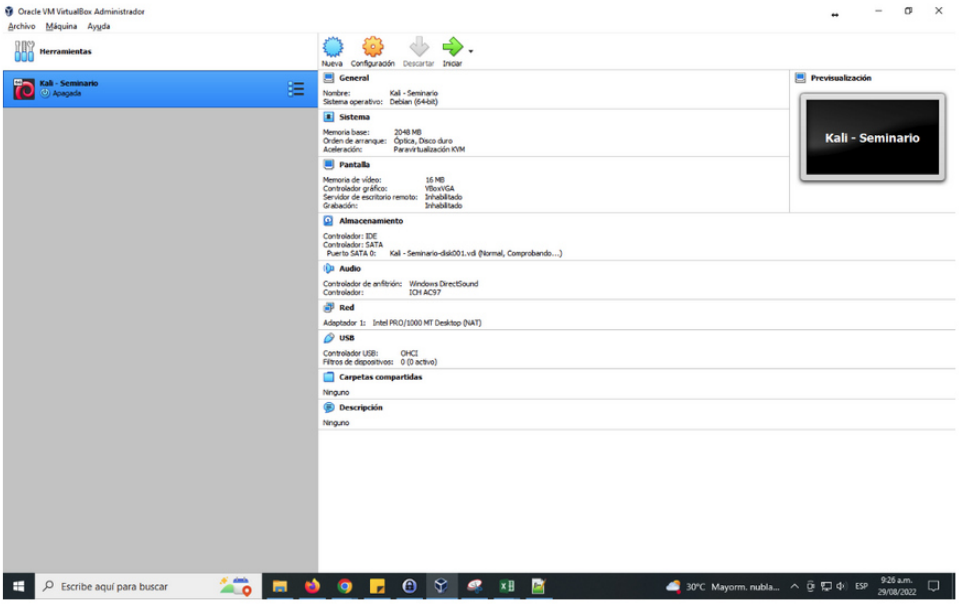
Se realiza el montaje de la máquina virtual “*Kali Linux*” del banco de trabajo.

Figura 4. Instalación maquina Kali en Virtual Box



Autor. Propia

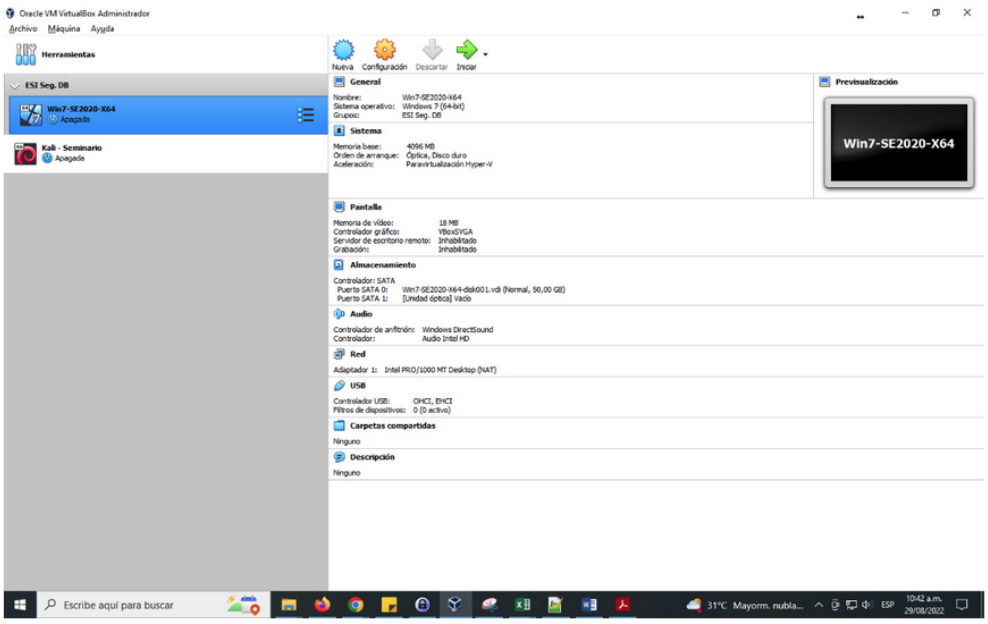
Figura 5. Maquina Kali en Virtual Box instalada



Autor. Propia

Se realiza el montaje de la máquina virtual "*Windows* 7 64 *Bits"* del banco de trabajo.

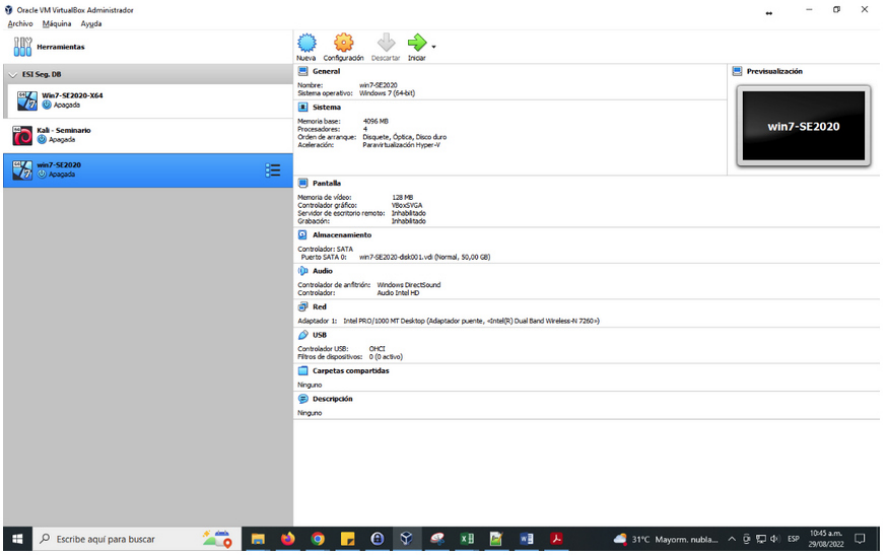
Figura 6. Maquina *Windows* 7 64 bits en *Virtual Box* instalada



Autor. Propia

Se realiza el montaje de la máquina virtual "*Windows 7 de 32 bits*" del banco de trabajo.

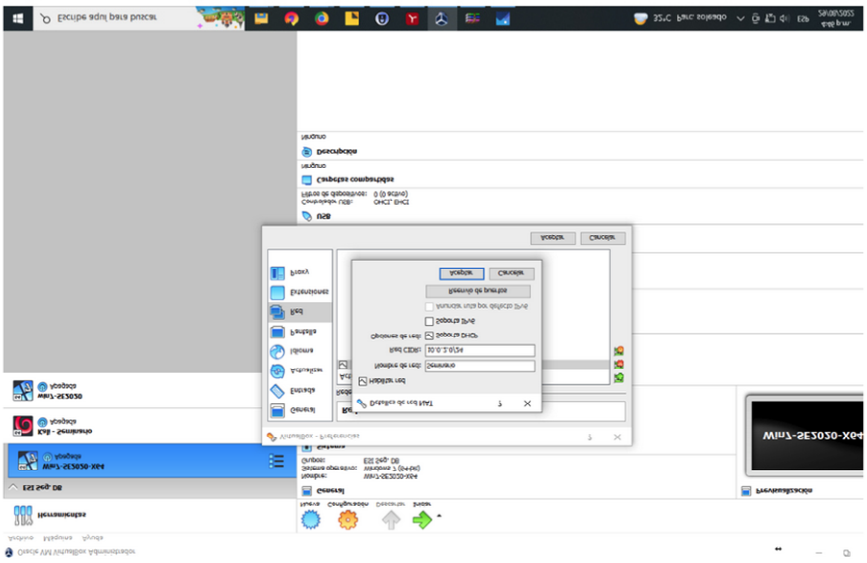
Figura 7. Instalación maquina *Windows 7 32 Bits* en *Virtual Box*



Autor. Propia

Con el propósito de llevar al entorno virtualizado la situación planteada en el caso de estudio se realiza la creación de una red NAT denominada "Seminario".

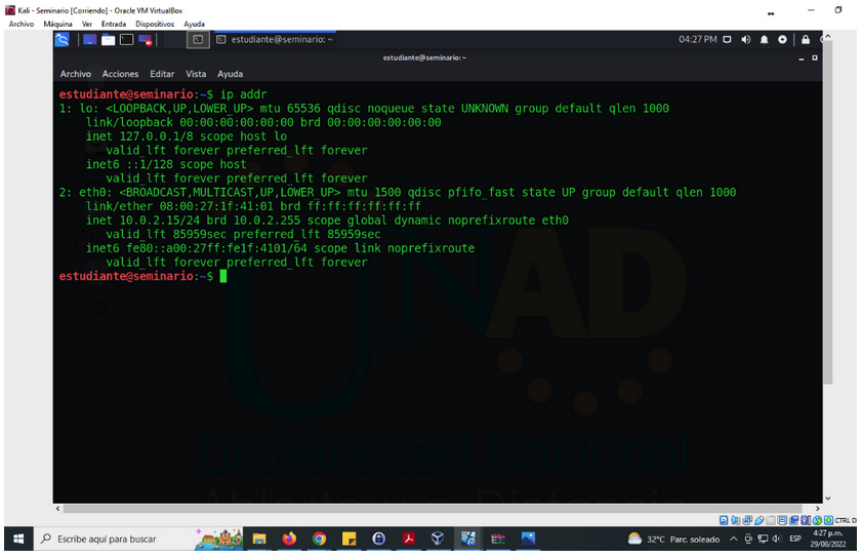
Figura 8. Configuración del segmento de red del Banco de Trabajo



Autor. Propia

Se verifica la asignación de IP de la maquina “Kali Linux” la cual corresponde a 10.0.2.15/24

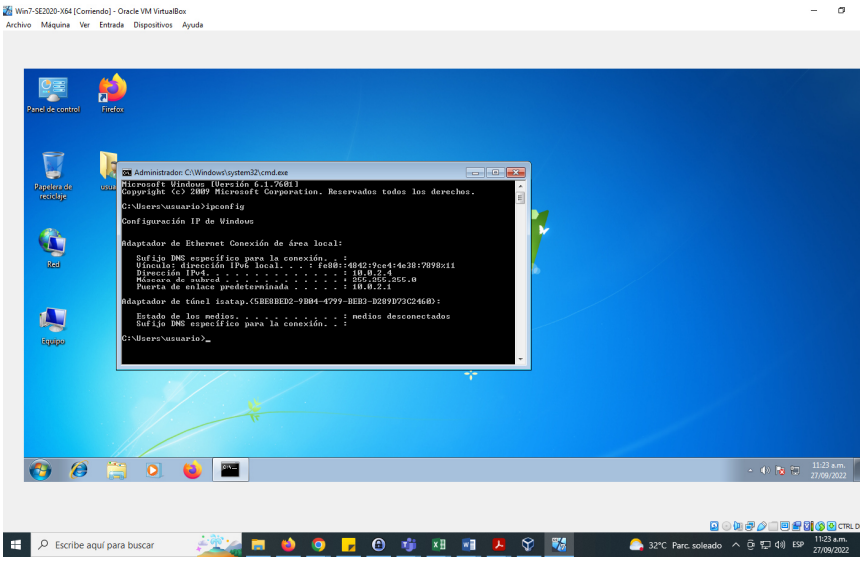
Figura 9. IP Kali Linux



Autor. Propia

Se verifica la asignación de IP de la maquina “Windows 7 64 bits” la cual corresponde a 10.0.2.4/24

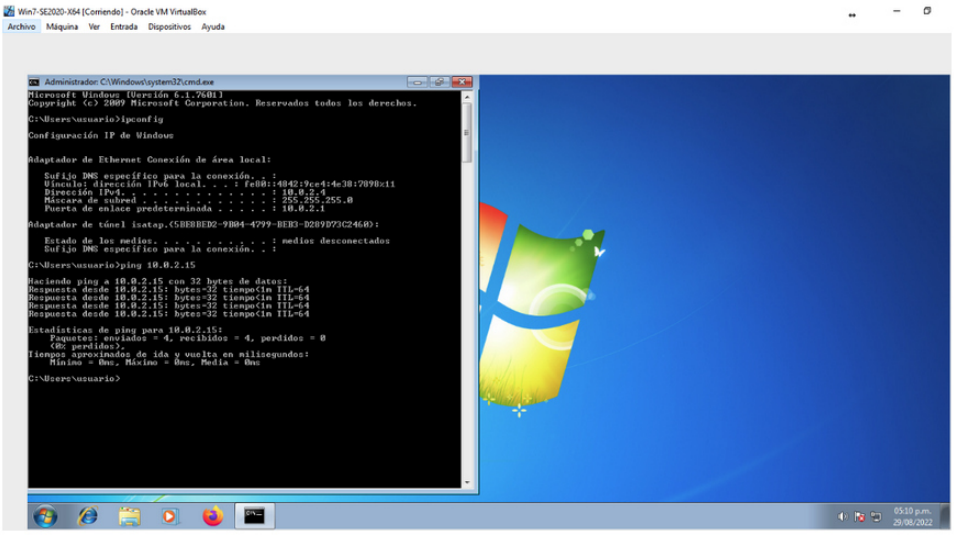
Figura 10. IP Windows 7 64 bits



Autor. Propia

Se verifica la comunicación de la maquina “Windows 7 64 bits” con la maquina “*Kali Linux*” mediante la ejecución del comando *PING* el cual se ejecuta correctamente.

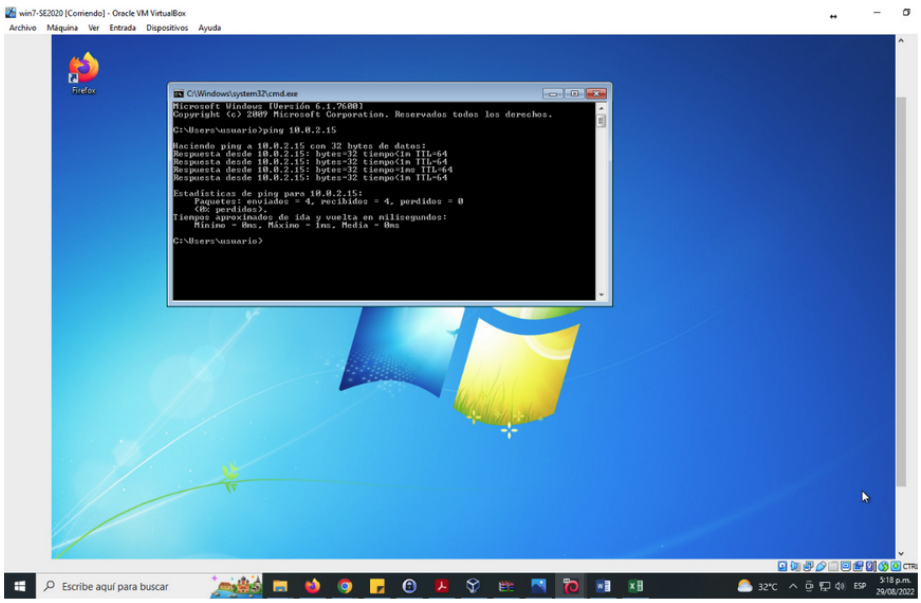
Figura 11. Ejecución comando *PING* en la maquina *Windows 7 64 bits*



Autor. Propia

Se verifica la comunicación de la maquina “*Windows 7 32 bits*” con la maquina “*Kali Linux*” mediante la ejecución del comando *PING* el cual se ejecuta correctamente.

Figura 12. Ejecución comando *PING* en la maquina *Windows 7 32 bits*



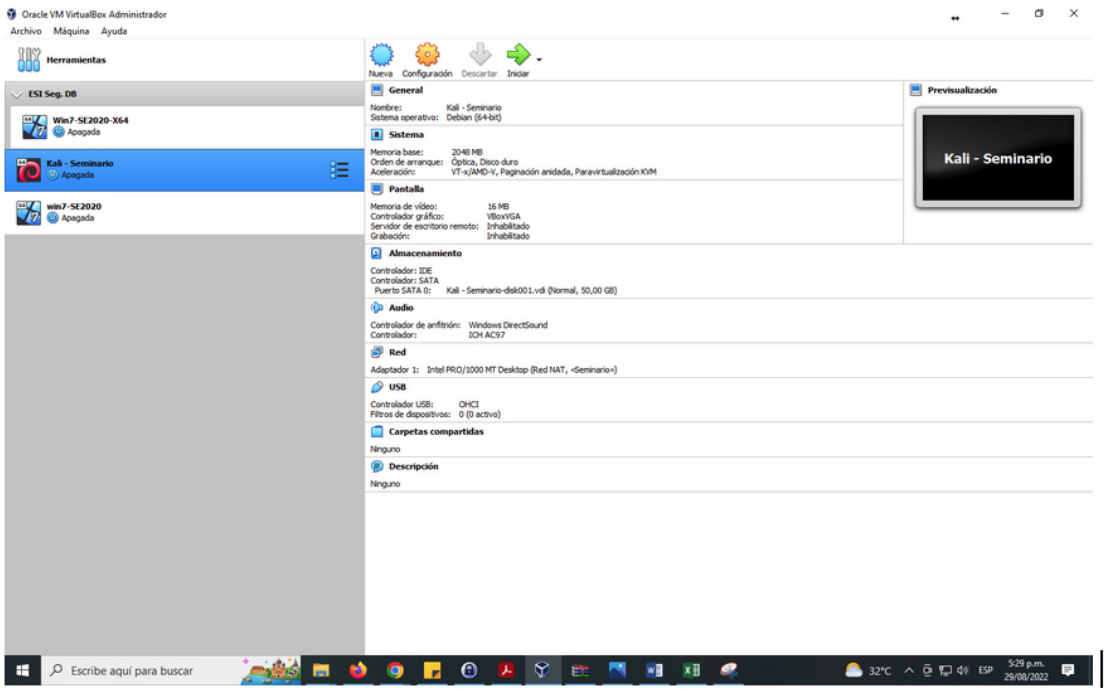
Autor. Propia

Se realiza una revisión de las características de cada una de las maquinas del banco de trabajo.

Características técnicas maquina "*Kali Linux*"

Nombre de la maquina: Kali – Seminario
Sistema Operativo: Debian 64 bits
Memoria: 2048 MB
Disco Duro: 50 GB
Adaptador de Red: 1

Figura 13. Características técnicas maquina *Kali Linux*

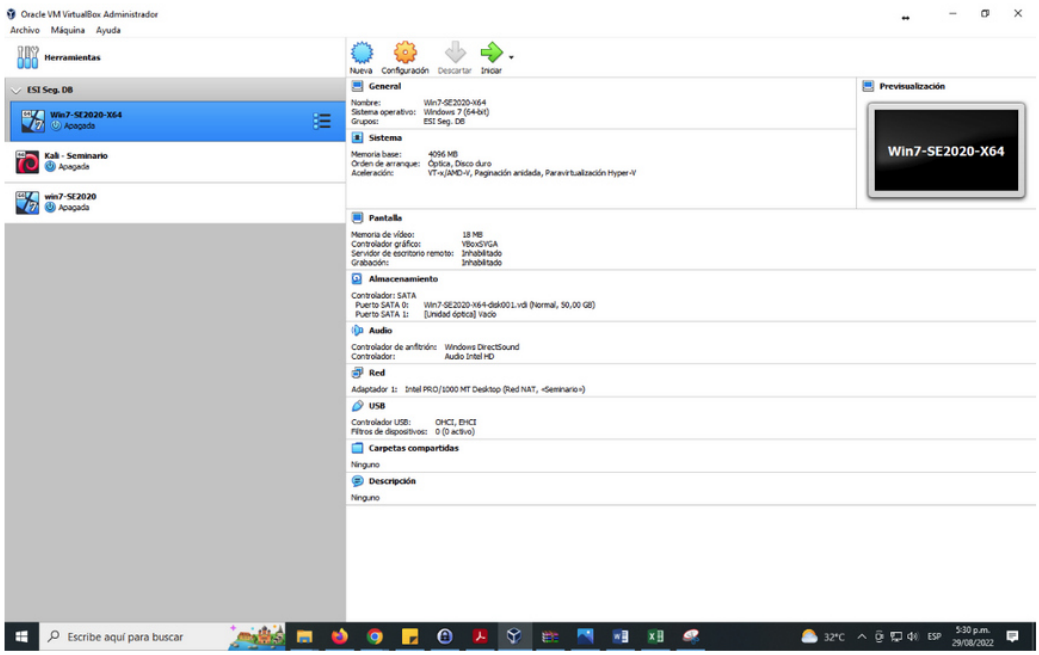


Autor. Propia

Características técnicas maquina *Windows 7 64 bits*

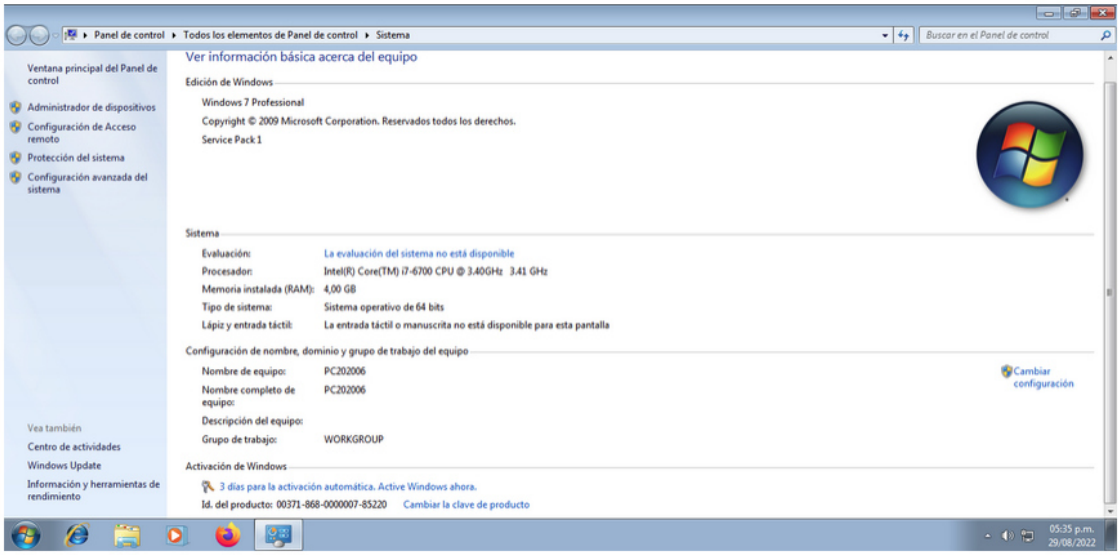
Nombre de la maquina: Win7-SE2020-X64
Nombre del equipo: PC202006
Sistema Operativo: Windows 7 Professional 64 bits
Procesador: Intel(R) Core (TM) i7-6700 CPU 3.40 GHz
Memoria: 4 GB
Disco Duro: 50 GB
Adaptador de Red: 1

Figura 14. Características técnicas maquina *Windows* 7 64 *bits*



Autor. Propia

Figura 15. Configuración sistema *Windows 7 64 bits*

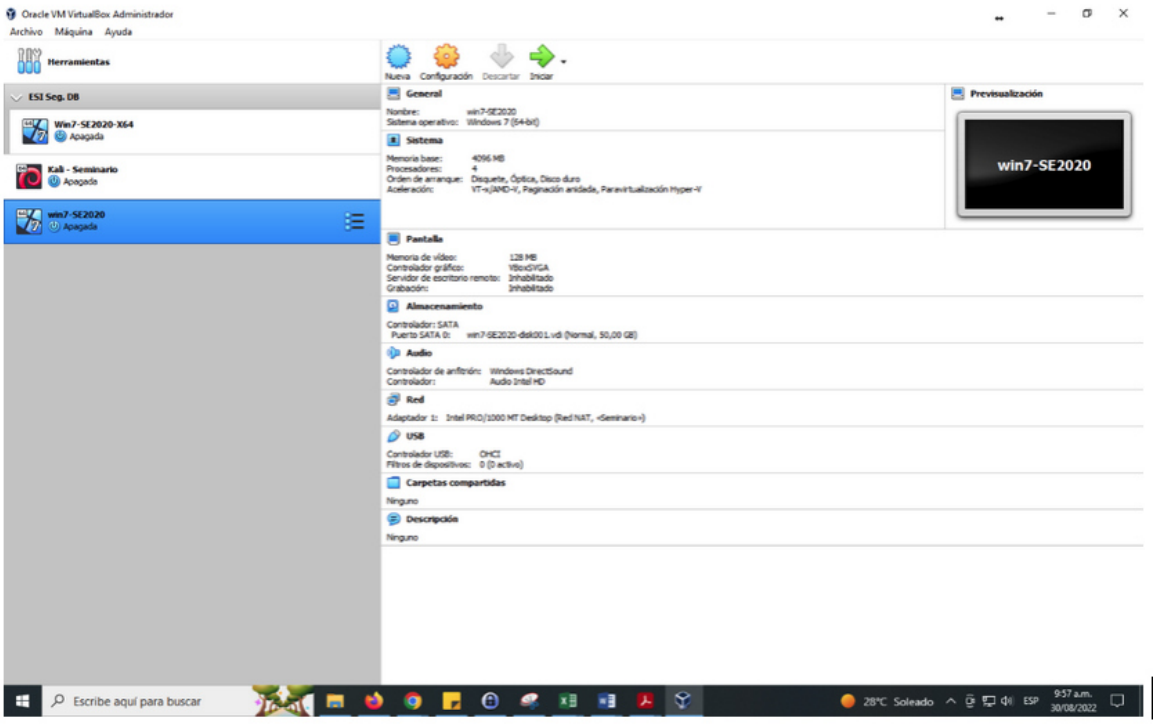


Autor. Propia

Características técnicas maquina "*Windows 7 32 bits*"

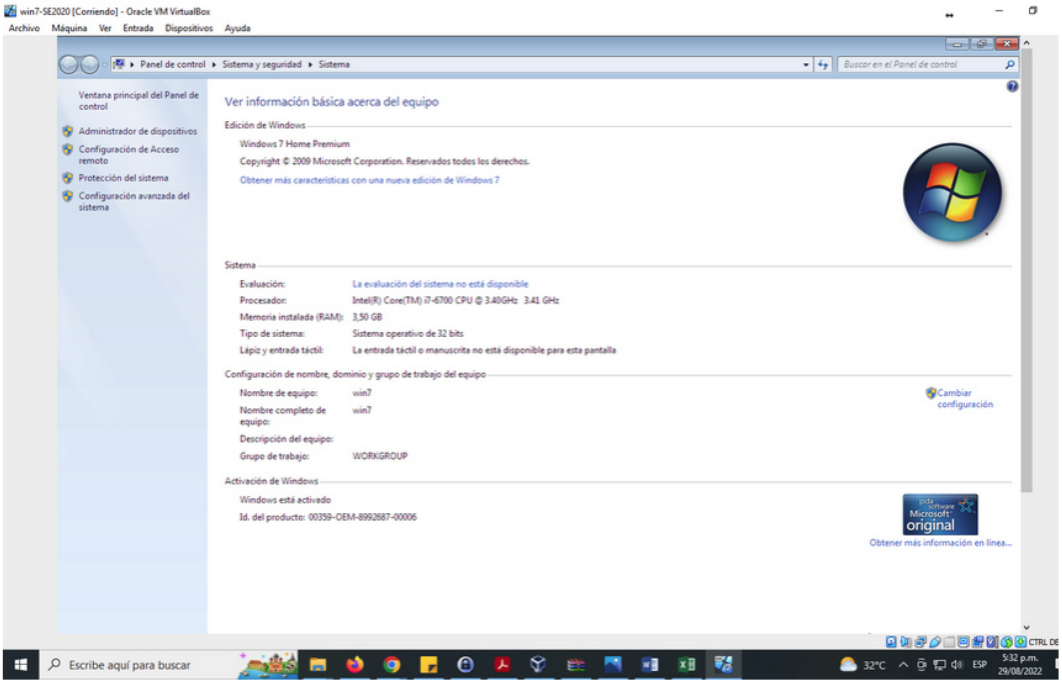
Nombre de la maquina: Win7-SE2020
Nombre del equipo: win7
Sistema Operativo: Windows 7 Home Premium 32 bits
Procesador: Intel(R) Core (TM) i7-6700 CPU 3.40 GHz
Memoria: 3.50 GB
Disco Duro: 50 GB
Adaptador de Red: 1

Figura 16. Características técnicas maquina *Windows 7 32 bits*



Autor. Propia

Figura 17. Configuración sistema *Windows 7 32 bits*



Autor. Propia

5.2.3 Fases del Test de Penetración. Con fin de establecer las circunstancias que dieron a lugar al caso de estudio, se debe dar inicio con el desarrollo de las fases del *test* de Penetración las cuales se describen a continuación:

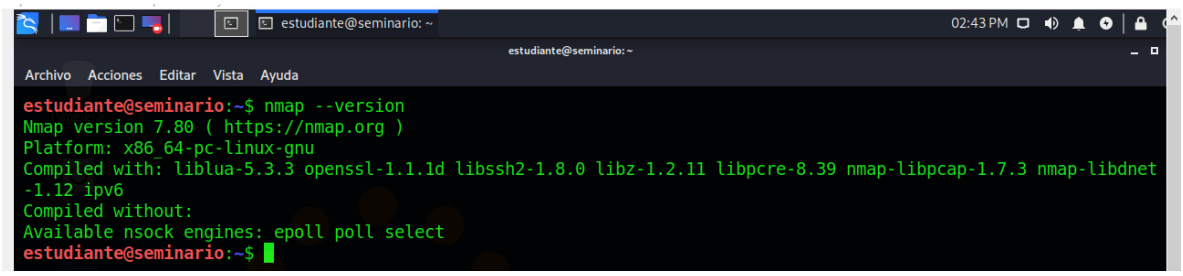
Tabla 1. Fases del Test de Penetración

Fase *pentesting*	Descripción del proceso
Recolección de Información	Aquí se realiza el reconocimiento de los sistemas a auditar, mediante la recolección total de la información del sistema que será atacado. Es de suma importancia analizar de manera correcta la información recolectada para llevar a cabo exitosamente las etapas posteriores. Dentro de las herramientas que pueden servir de apoyo para llevar a cabo esta etapa esta *NMAP* que permite el escaneo de puertos y la recolección de algunos metadatos para así recolectar la mayor cantidad de información que nos pueda ser útil en la ejecución de las pruebas.
Búsqueda de Vulnerabilidades	Partiendo de la información obtenida en la etapa anterior en esta fase se realiza la identificación de las posibles vulnerabilidades y las herramientas que pueden ser útil al momento de su explotación mediante la ejecución de los ataques. Para llevar a cabo esta fase se puede hacer uso de herramientas como *Nessus* o *Acunetix* que mediante el uso de interfaces sencillas nos permiten realizar la identificación de vulnerabilidades.
Explotación de Vulnerabilidades	En esta fase se intenta conseguir la mayor cantidad de información o accesos de los sistemas atacados de la organización, a menudo esta actividad se realiza a través de la ejecución de *exploits*. Esta fase se puede desarrollar a través del uso de herramientas como *Metasploit* o *SQL Inyector*.
Post - Explotación	El propósito principal en esta fase es acceder a información que sea relevante de la organización o adquirir privilegios de nivel de administrador mediante el uso de técnicas como *pivoting*.
Elaboración de Informe	Llevadas a cabo las fases anteriores en esta fase es de suma importancia realizar la documentación de los hallazgos, especificando el proceso elaborado, las técnicas que fueron usadas y las herramientas y vulnerabilidades identificadas. Los informes se puede realizar tanto de carácter técnico como gerencial donde sea posible exponer de manera clara los resultados obtenidos.

Autor. Sánchez Ávila, Miguel Ángel. HACKING ETICO: IMPACTO EN LA SOCIEDAD. [En línea]. [2015]. Consultado el 10 de septiembre del 2021. Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4919/00005096.pdf?sequence=1&isAllowed=y

5.2.3.1 Recolección de Información. Teniendo en cuenta que para llevar a cabo esta fase se hará uso de la herramienta *NMAP*, se valida su instalación y versión existente en la maquina *Kali Linux* mediante el uso del comando *nmap - -versión*

Figura 18. Versión nmap instalada en la maquina *Kali Linux*



Autor. Propia

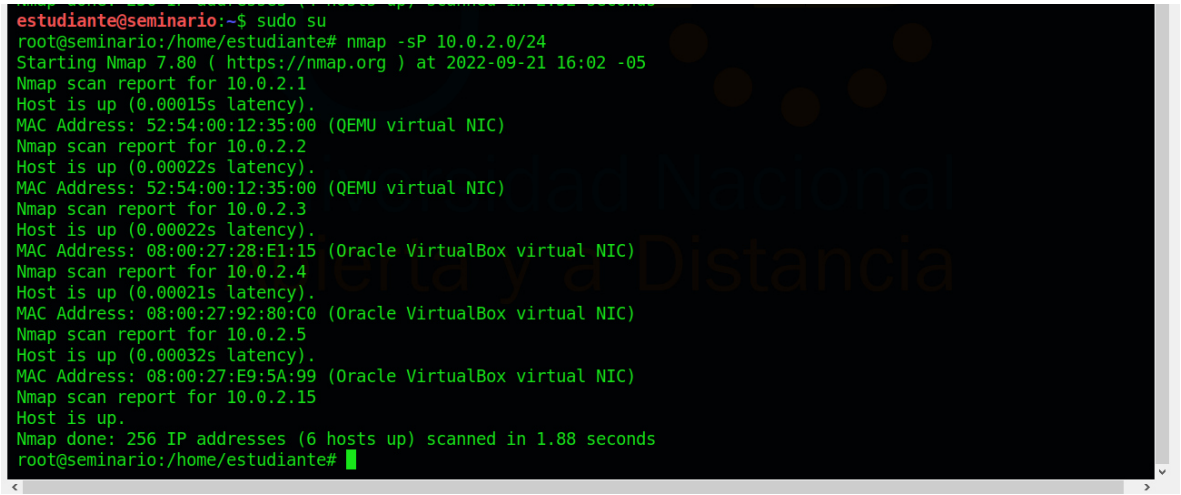
Como se observa en la anterior imagen la herramienta se encuentra instalada en la maquina *Kali Linux* y cuenta con la versión 7.80.

Con el objetivo de realizar la identificación de los puertos abiertos en las maquinas objeto de análisis del ejercicio se hace uso de la herramienta *NMAP* desde la maquina *Kali Linux*.

En primer lugar, se realiza un escaneo de la red para identificar los equipos en la red, esto mediante el comando *nmap –sP10.0.2.0/24* en usuario *root*, esto teniendo en cuenta la IP identificada del equipo *Kali Linux* es 10.0.2.15/24.

En la salida del comando se observa que arroja cuatro *IPs* por lo que se puede suponer que allí se pueden encontrar las maquinas objeto del análisis.

Figura 19. Salida del comando NMAP para el escaneo de la red

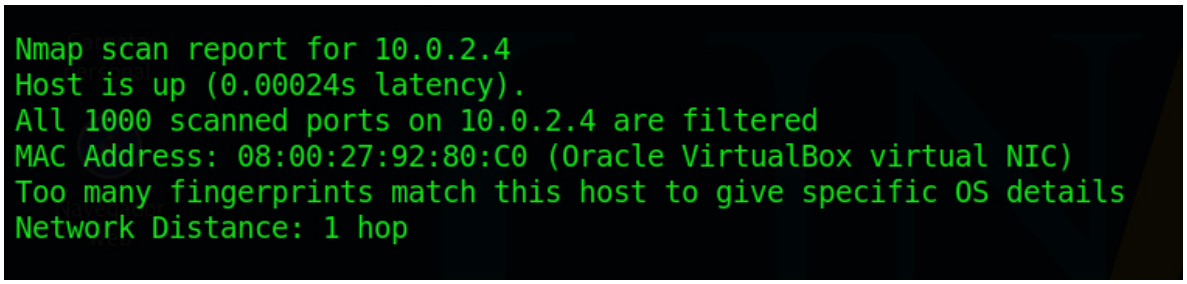


Autor. Propia

Como se observa en la imagen se tienen las *IP* de las máquinas virtuales que hacen parte del ejercicio, lo que permite identificar las IPs 10.0.2.4 y 10.0.2.5 de las maquinas *Windows*.

Con esta información se procede a revisar los puertos de cada una de estas *IPs*, con la instrucción *nmap 10.0.2.4/24 –sV –O*

Figura 20. Salida del comando NMAP para la IP 10.0.2.4

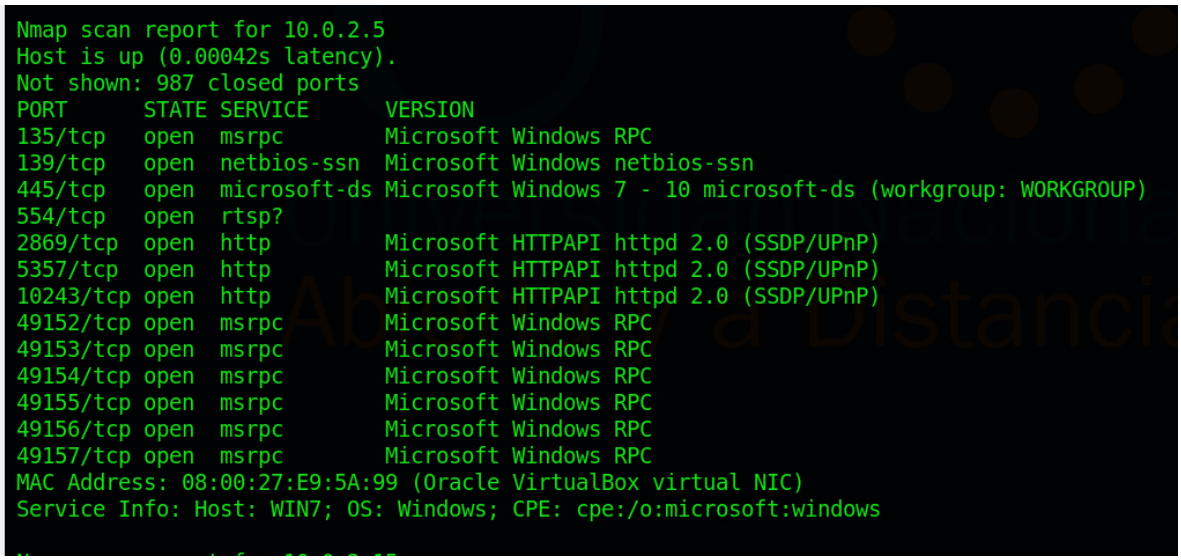


Autor. Propia

Como se puede observar este equipo cuenta con protección ya que no es posible acceder mediante la herramienta a información de puertos abiertos y sistema operativo.

Caso contrario se observa en la siguiente imagen correspondiente al otro equipo *Windows* de 32 *bits* analizado, donde se pueden observar varios puertos y servicios abiertos.

Figura 21. Salida del comando *NMAP* para la IP 10.0.2.5



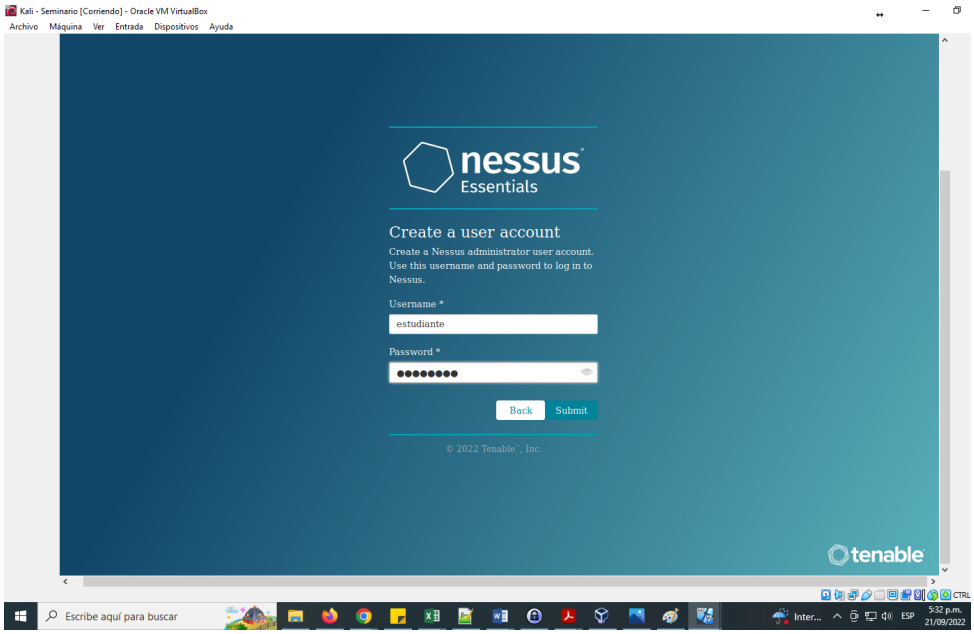
Autor. Propia

Dentro de los puertos y servicios abiertos, se encuentra el puerto 445 que según la documentación del sistema operativo *Windows*, es el utilizado para el servicio SMB, "a partir de Windows Vista y Windows Server 2008 con SMB 2.0.2, requiere TCP/IP sobre el puerto 445"[47]

5.2.3.2 Búsqueda de Vulnerabilidades. Aquí partiendo de información obtenida en la fase anterior se realiza la identificación de las vulnerabilidades a haciendo uso de la herramienta denominada *Nessus,* la cual *es* desplegada desde la maquina *Kali Linux*.

[47] MICROSOFT. [Sitio Web]. SMB de host directo a través de TCP/IP. [Consultado el día 21 de septiembre de 2022]. Disponible en: https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/direct-hosting-of-smb-over-tcpip

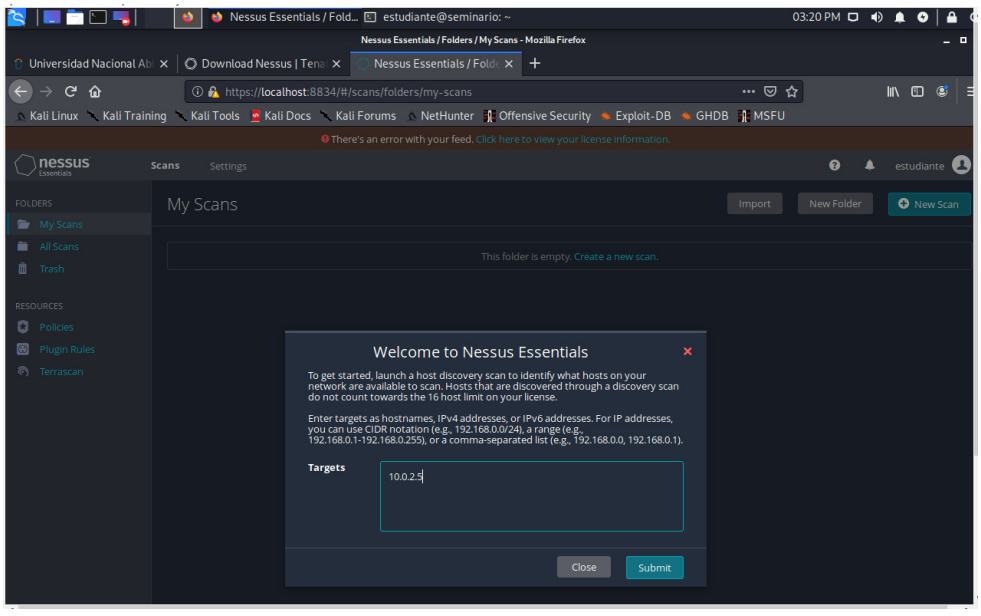
Figura 22. Herramienta *Nessus* instalada en la maquina *Kali Linux*



Autor. Propia

Con el propósito de realizar el análisis de la maquina identificada como vulnerable se procede a ingresar la *IP* en la herramienta.

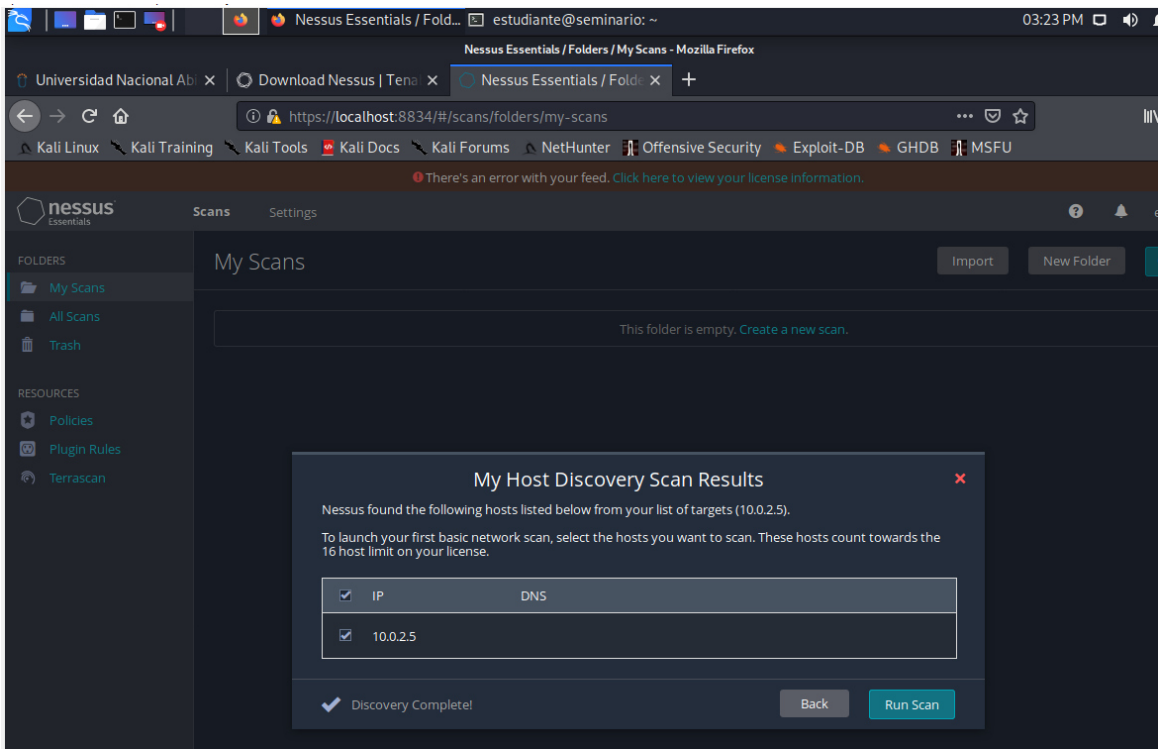
Figura 23. Ingreso de la IP a analizar en la herramienta *Nessus*



Autor. Propia

Se envía el análisis a la IP 10.0.2.5 ingresada en la herramienta para que ella arroje el análisis de vulnerabilidades en la maquina indicada.

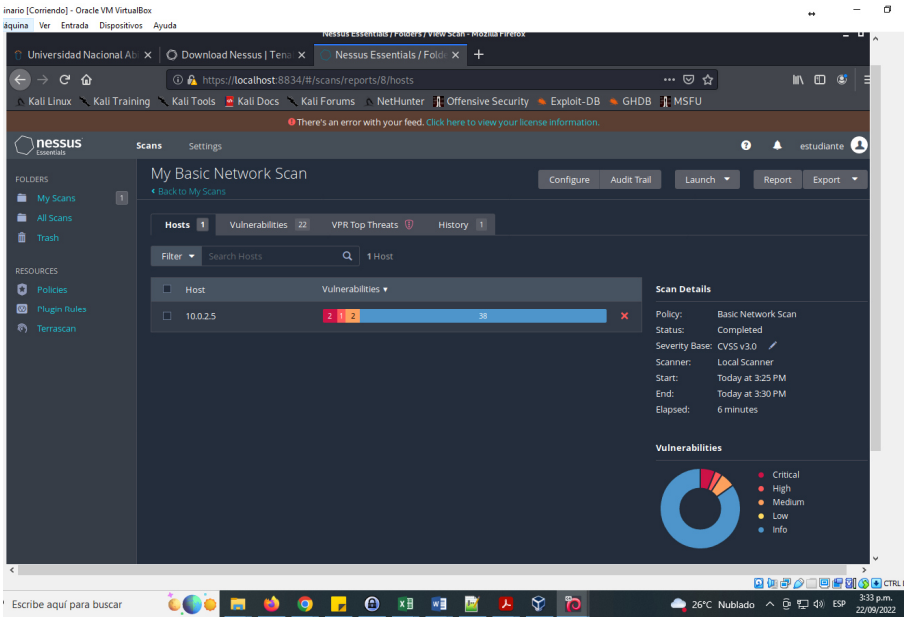
Figura 24. Envío de análisis a la maquina indicada



Autor. Propia

El reporte de la herramienta arroja un total de 38 vulnerabilidades informativas, 2 críticas, 1 vulnerabilidad Alta y 2 de grado medio, para la máquina de IP 10.0.2.5, tal como se observa en la siguiente imagen.

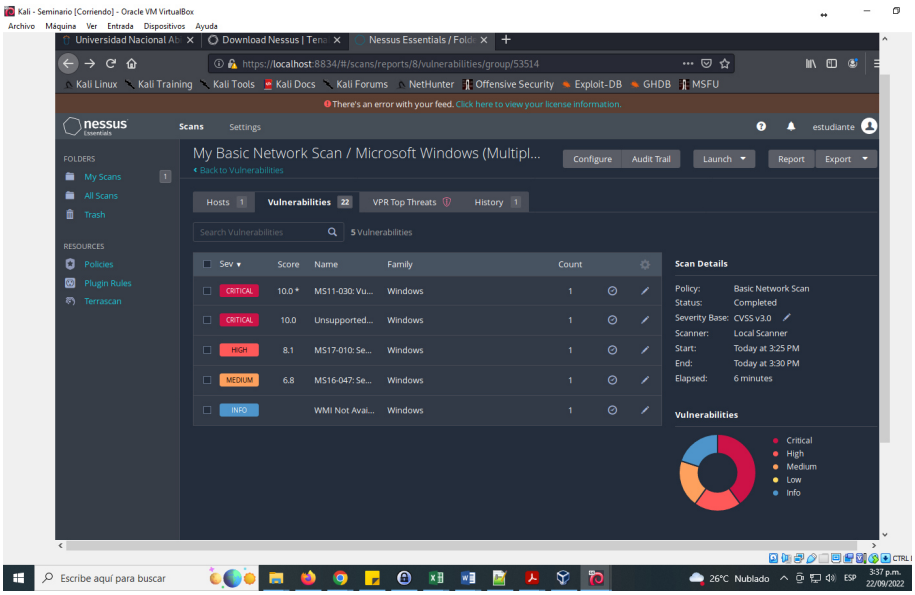
Figura 25. Resumen de análisis de vulnerabilidades maquina 10.0.2.5



Autor. Propia

En la siguiente imagen se puede observar el informe que arroja la herramienta, donde listas las vulnerabilidades halladas de una manera más detallada indicando un puntaje que establece su criticidad.

Figura 26. Reporte detallado de las vulnerabilidades halladas

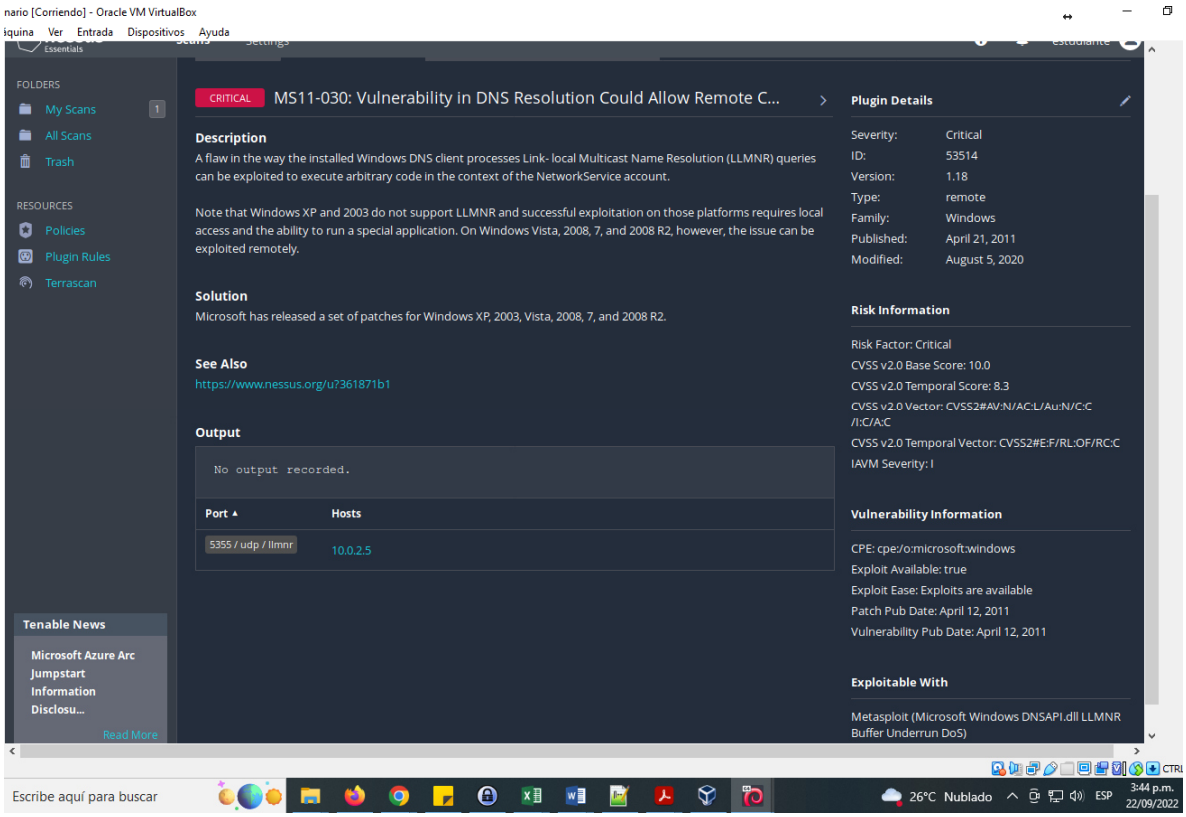


Autor. Propia

- **Vulnerabilidad MS11-030**

Se realiza revisión uno a uno de las vulnerabilidades halladas por la herramienta con el fin de determinar el estado de la maquina evaluada, en la primera vulnerabilidad critica se tiene "*MS11-030 Vulnerability in DNS Resolution Could Remote Control*" allí la herramienta explica las consecuencias de esta vulnerabilidad que permite el control remoto del equipo, su solución, el cual consiste en aplicar parches de actualización y que es posible aplicar *exploits* con la herramienta *Metasploit*, tal como se observa en la siguiente imagen.

Figura 27. Vulnerabilidad MS11-030

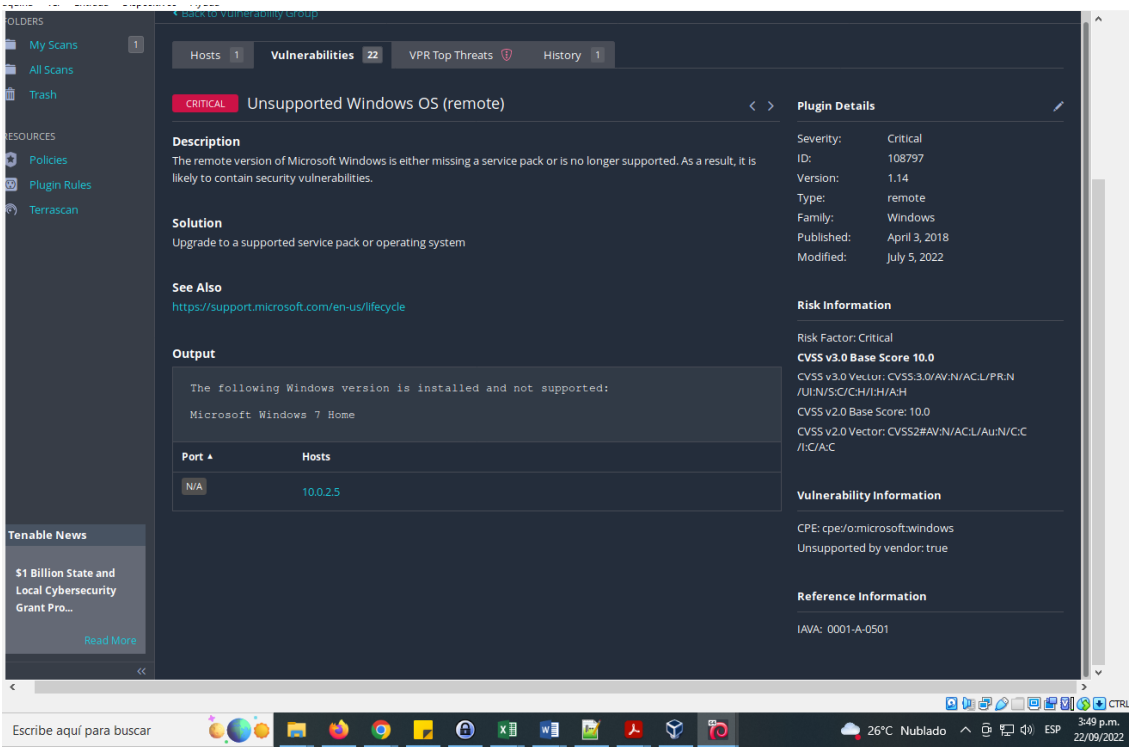


Autor. Propia

- **Vulnerabilidad Sistema Operativo sin soporte**

La siguiente vulnerabilidad critica hace referencia a la falta de soporte del sistema operativo de la maquina analizada, esta versión ya no cuenta con soporte y por tanto es posible que se encuentre expuesta a vulnerabilidades, por lo que la herramienta sugiere actualizar el sistema operativo a una versión que cuente con soporte.

Figura 28. Vulnerabilidad sistema operativo sin soporte

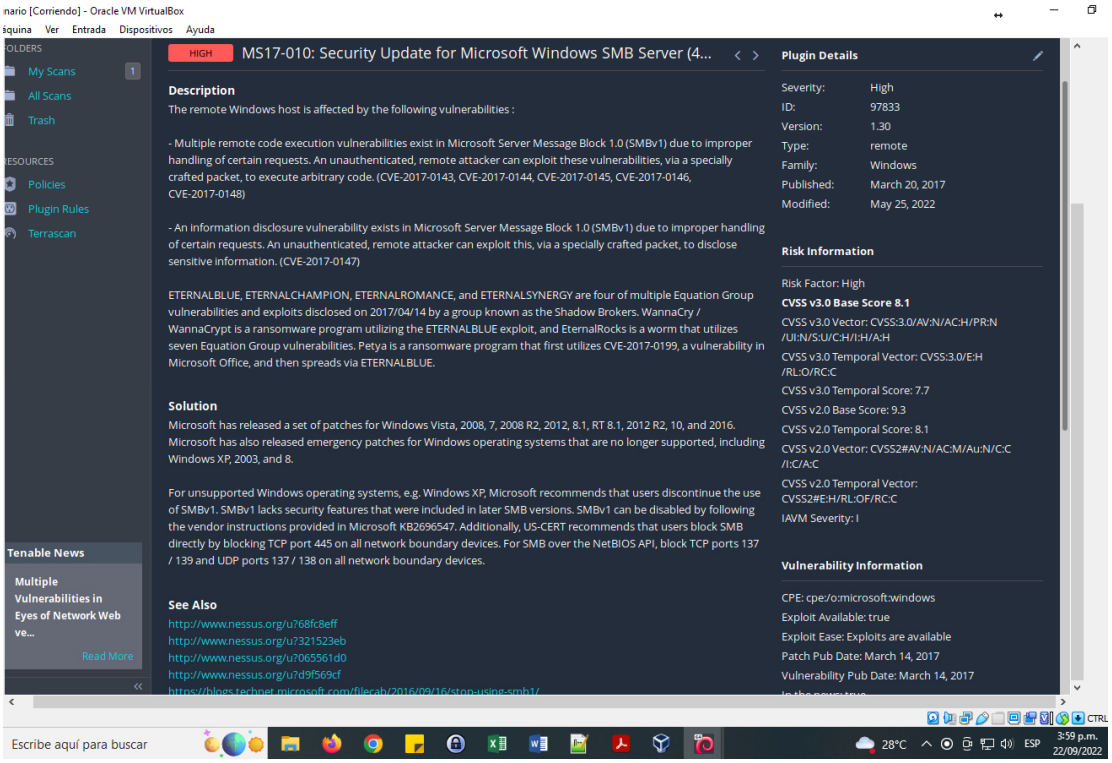


Autor. Propia

- **Vulnerabilidad SMB *Remote Windows***

A continuacion la herramienta arroja la siguiente vulnerabilidad catalogada como alta y relacionada con el servicio *Samba* del sistema operativo *Windows* que hace referencia a un repositorio de informacion compartida y que consiste en la posibildiad de acceder y ejecutar codigo de manera remota en la maquina, se puede aplicar *exploits* a traves de la herramienta *Metasploit* y tiene como solucion la aplicación de parches en el sistema operativo de la maquina, este reporte tambien arroja los codigos CVE de las vulnerabilidades.

Figura 29. Vulnerabilidad *SMB Remote Windows*

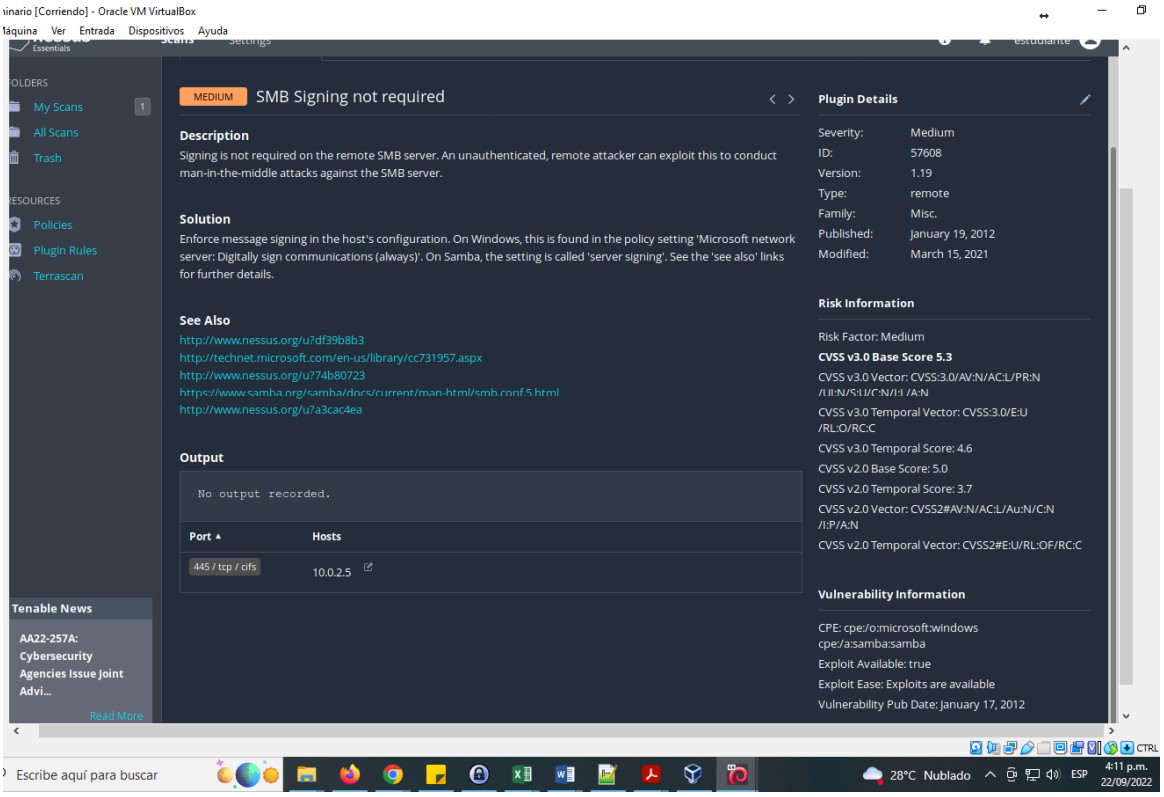


Autor. Propia

- **Vulnerabilidad *SMB signing not required***

La siguiente vulnerabilidad se encuentra catalogada como media y hace referencia a la posibilidad de acceder al servicio samba sin necesidad de autenticación mediante firma, que implica que no es posible garantizar la autenticidad de paquetes *SMB* lo que genera riesgo de ataques de hombre en el medio. Esta vulnerabilidad permite mediante el uso de *Metasploit* ejecutar los *exploits* asociados.

Figura 30. Vulnerabilidad *SMB signing not required*

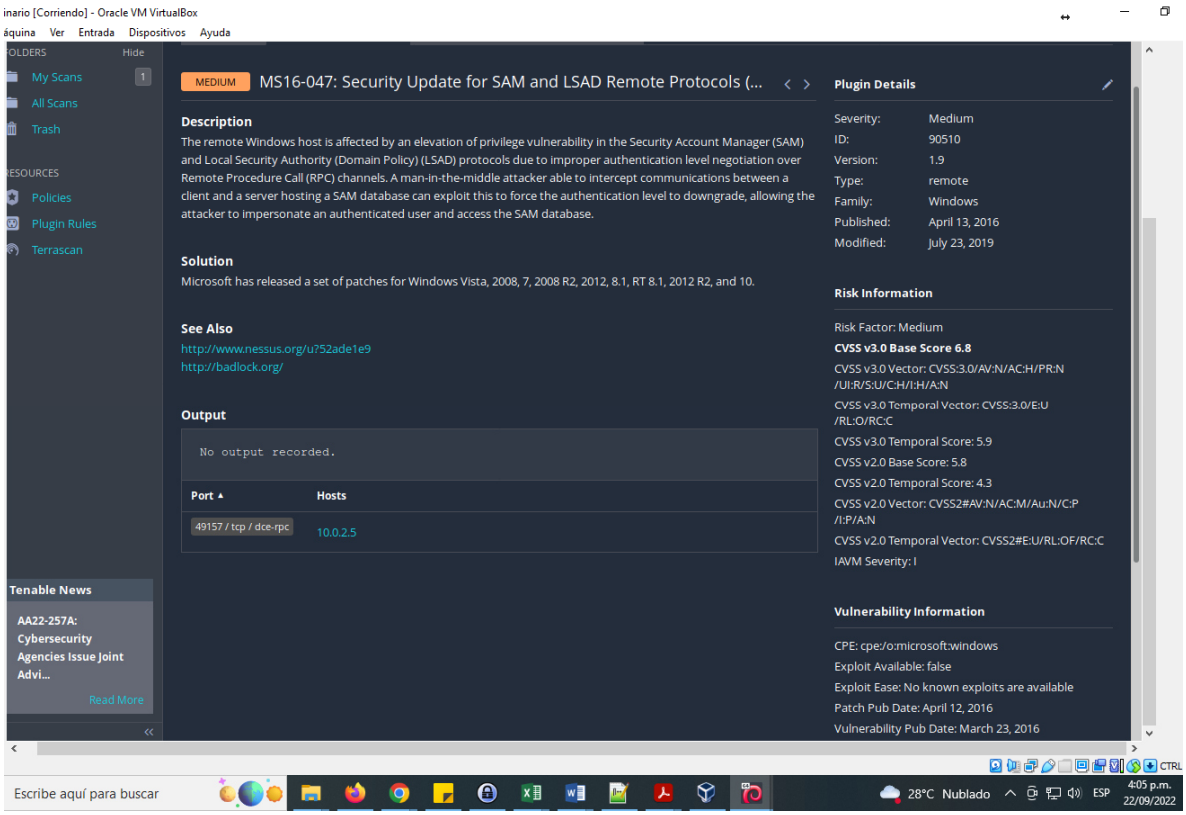


Autor. Propia

- **Vulnerabilidad *MS16-047 Security Update for SAM and LSAD Remote Protocols B signing not required***

Por último, la siguiente vulnerabilidad identificada como "*MS16-047 Security Update for SAM and LSAD Remote Protocols*" y catalogada como Media tiene relación con la elevación de privilegios, no se tienen *exploit* conocidos aplicables a esta vulnerabilidad.

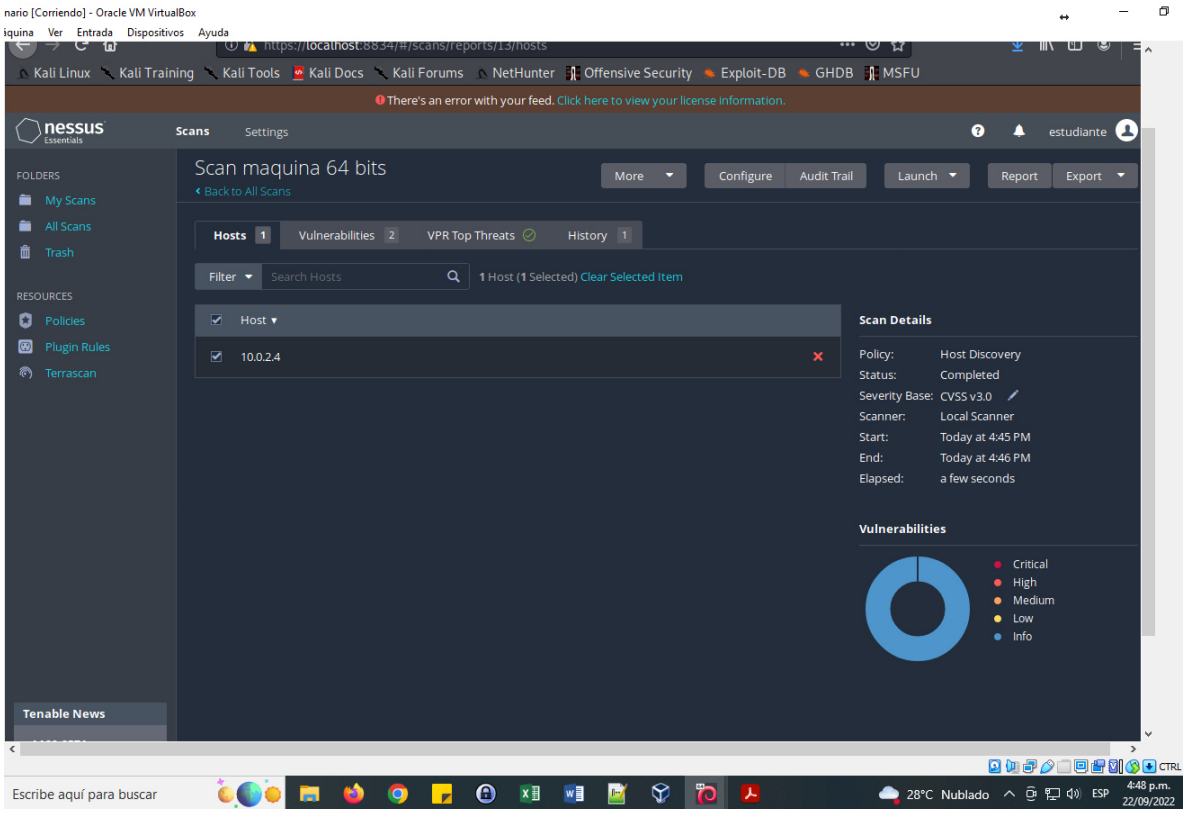
Figura 31. Vulnerabilidad MS16-047 *Security Update for SAM and LSAD Remote Protocols*



Autor. Propia

Por proceso de validación se procedió a ejecutar la herramienta en la maquina *Windows* de 64 *Bits* con *IP* 10.0.2.4, la cual arroja como resultado que no cuenta con vulnerabilidades críticas, solo informativas.

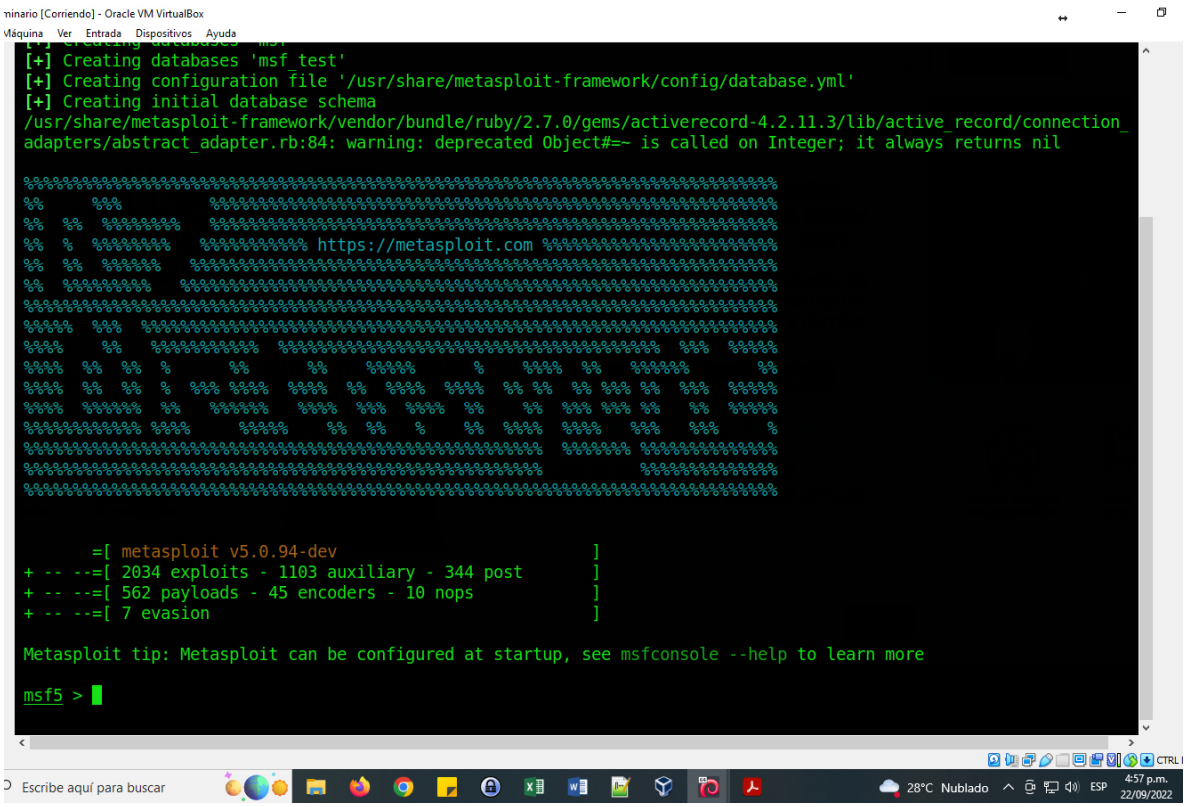
Figura 32. Reporte vulnerabilidades maquina *Windows* de 64 *bits* con IP 10.0.2.4



Autor. Propia

5.2.3.3 Explotación de Vulnerabilidades. Posterior a la identificación de Vulnerabilidades se realiza su explotación mediante el uso de la herramienta *Metasploit* desplegada desde la maquina *Kali Linux* en la máquina *Windows* de 32 *bits* debido a que esta arrojo la existencia de vulnerabilidades.

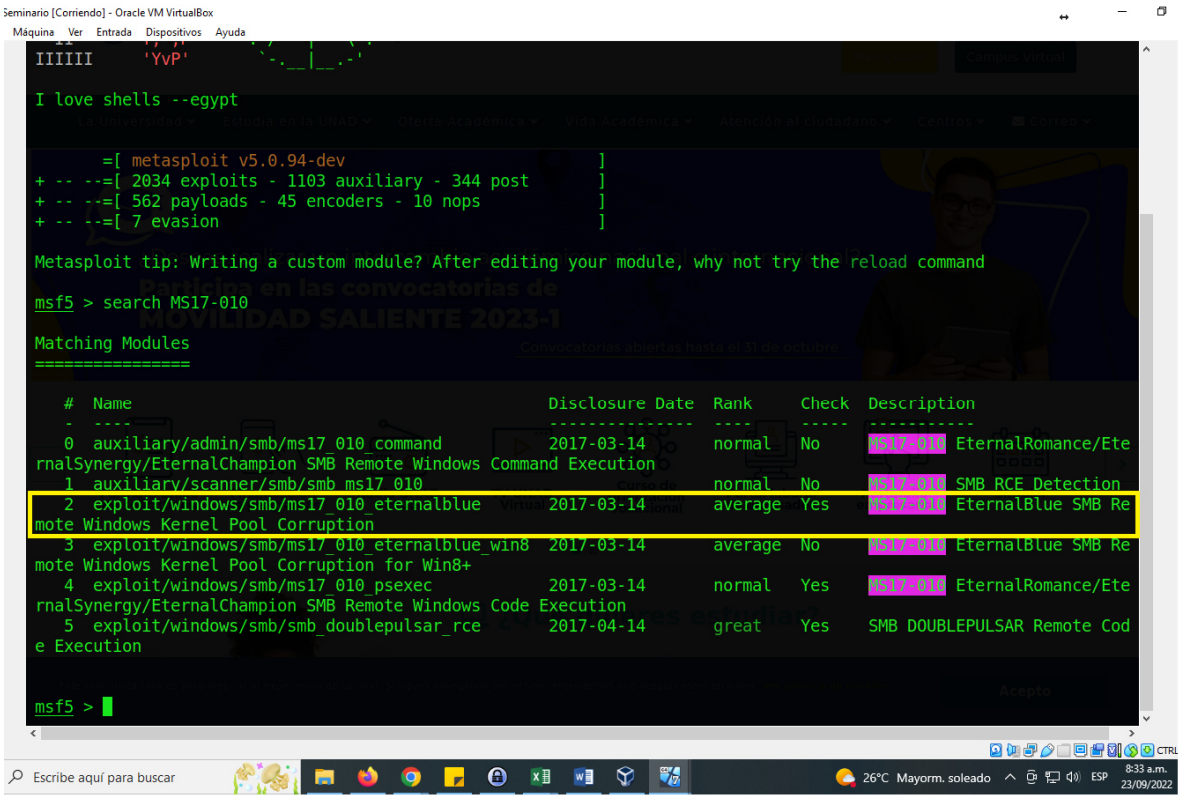
Figura 33. Herramienta *Metasploit* desplegada en la maquina *Kali Linux*



Autor. Propia

Se realiza en la herramienta la búsqueda mediante el comando *search* de los *exploits* asociados a la vulnerabilidad *MS17-010 SMB Remote Windows*. Para el desarrollo del ejercicio se selecciona la vulnerabilidad número 2 denominada "*Eternalblue SMB Remote Windows Kernel Pool Corruption.*"

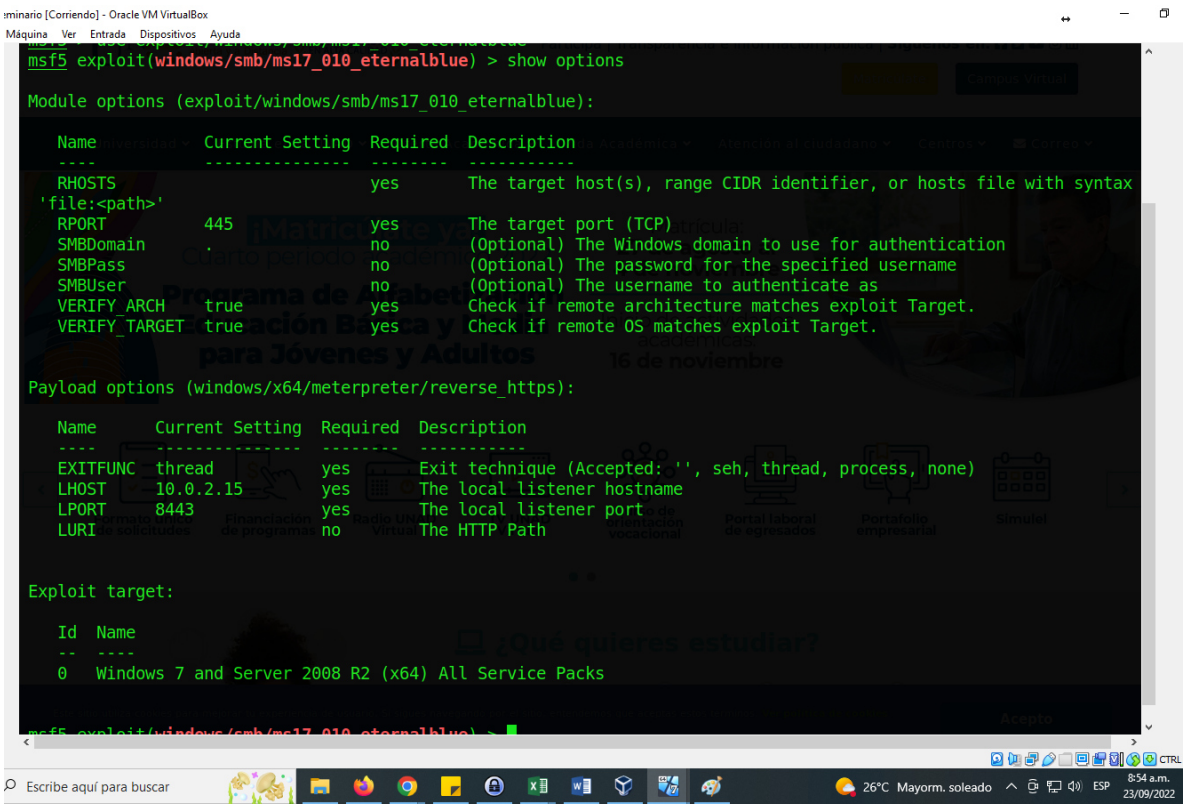
Figura 34. Listado de *exploits* asociados a la vulnerabilidad MS17-010 SMB *Remote Windows*



Autor. Propia

Se realiza la selección del *exploit* mediante la ejecución del comando *use exploit/windows/smb/ms17_010_eternalblue* y a través del comando *show options* se observa los parámetros necesarios para la ejecución del *exploit*.

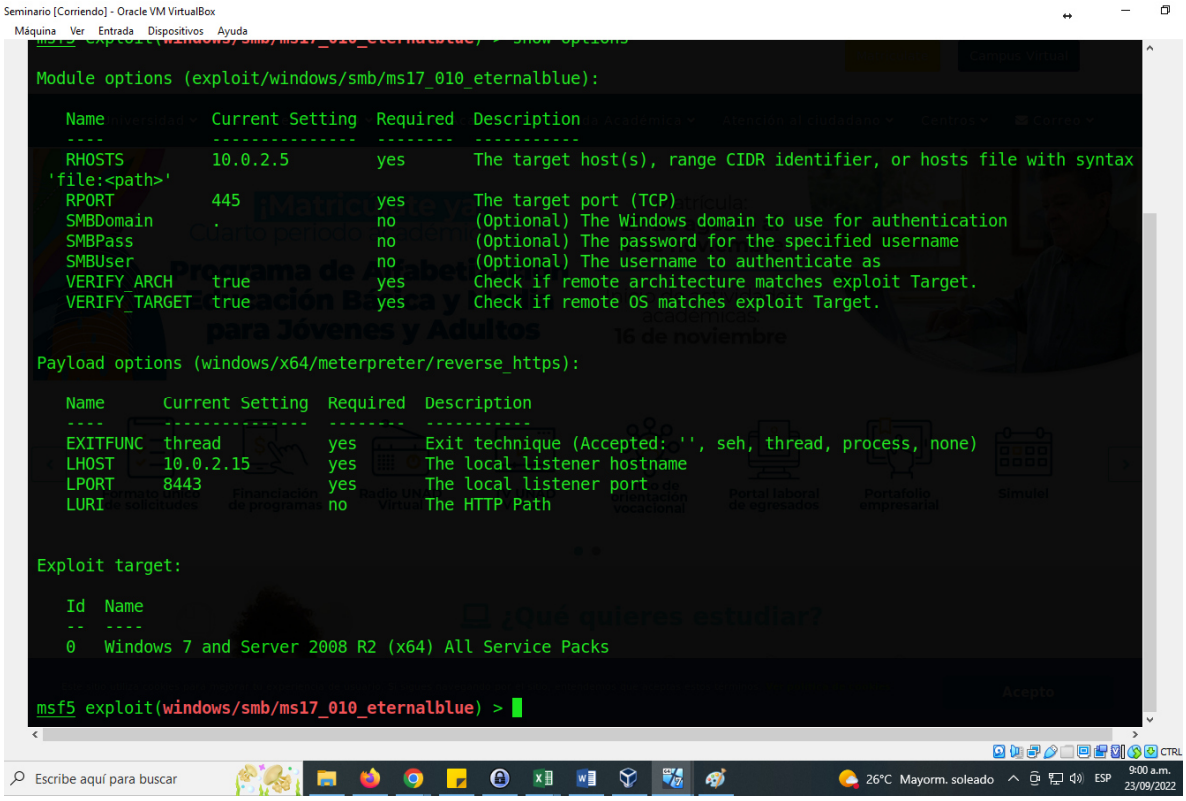
Figura 35. Opciones de configuración del *exploit*



Autor. Propia

Como se observa en la imagen anterior, el parámetro *RHOSTS* se encuentra sin asignar por lo que se procede a realizar la asignación de la variable, la cual hace referencia a la IP de la máquina que será atacada, en este caso 10.0.2.5, con la ejecución del comando *show options* se verifica el proceso realizado.

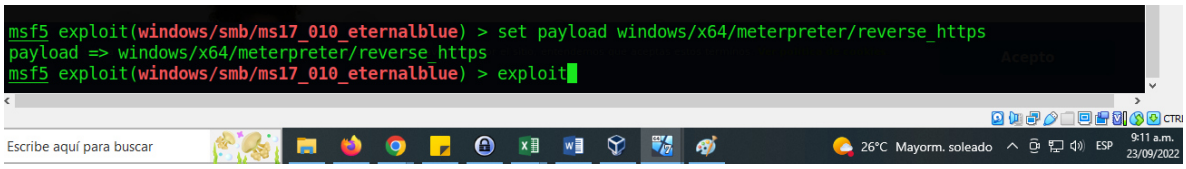
Figura 36. Parámetro RHOTS asignado



Autor. Propia

Una vez se han configurado los parámetros necesarios se procede al cargue del *payload windows/meterpreter/reverse_https* y a su ejecución mediante la instrucción *exploit*

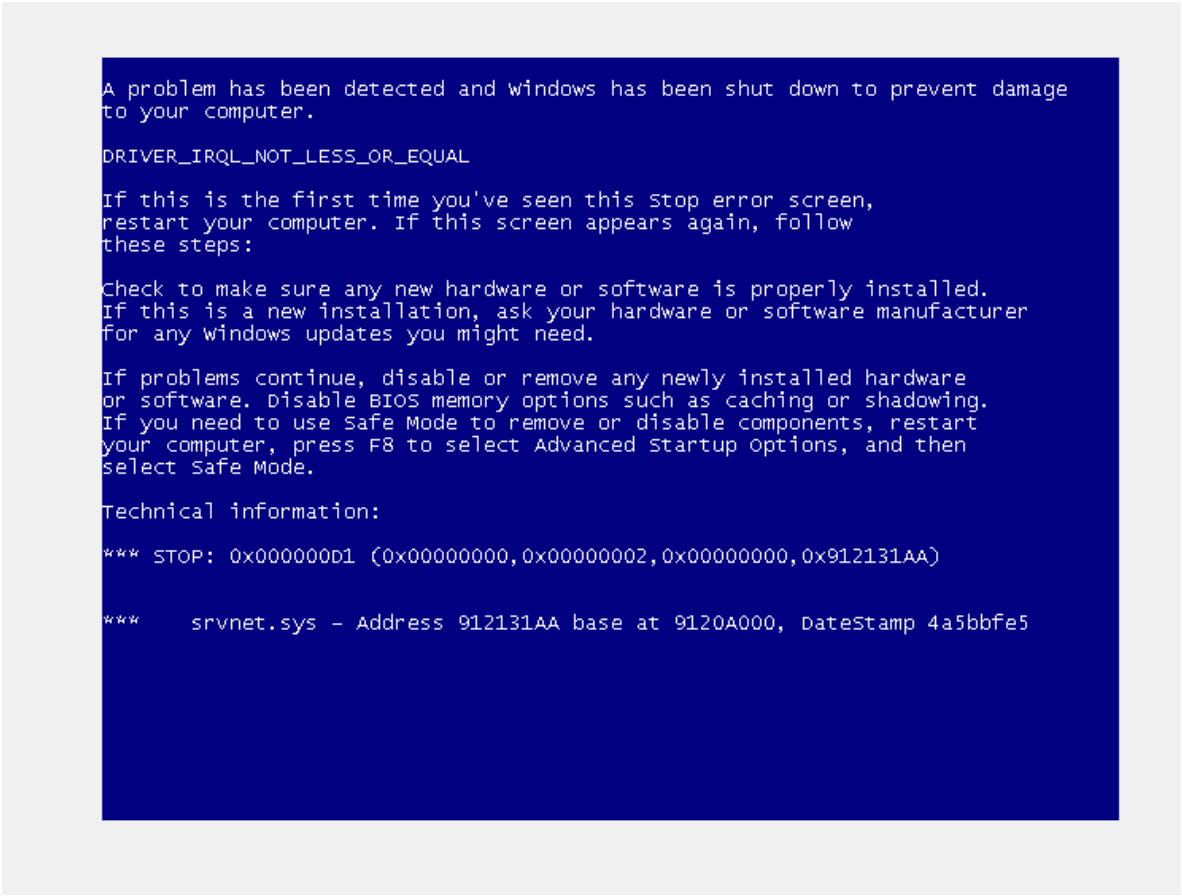
Figura 37. Cargue y ejecución del *exploit*



Autor. Propia

Se realiza la ejecución del *exploit,* como se puede observar en la siguiente imagen, se genera una pantalla azul con el error y que evidencia que efectivamente el *payload* logra acceder a la maquina objetivo.

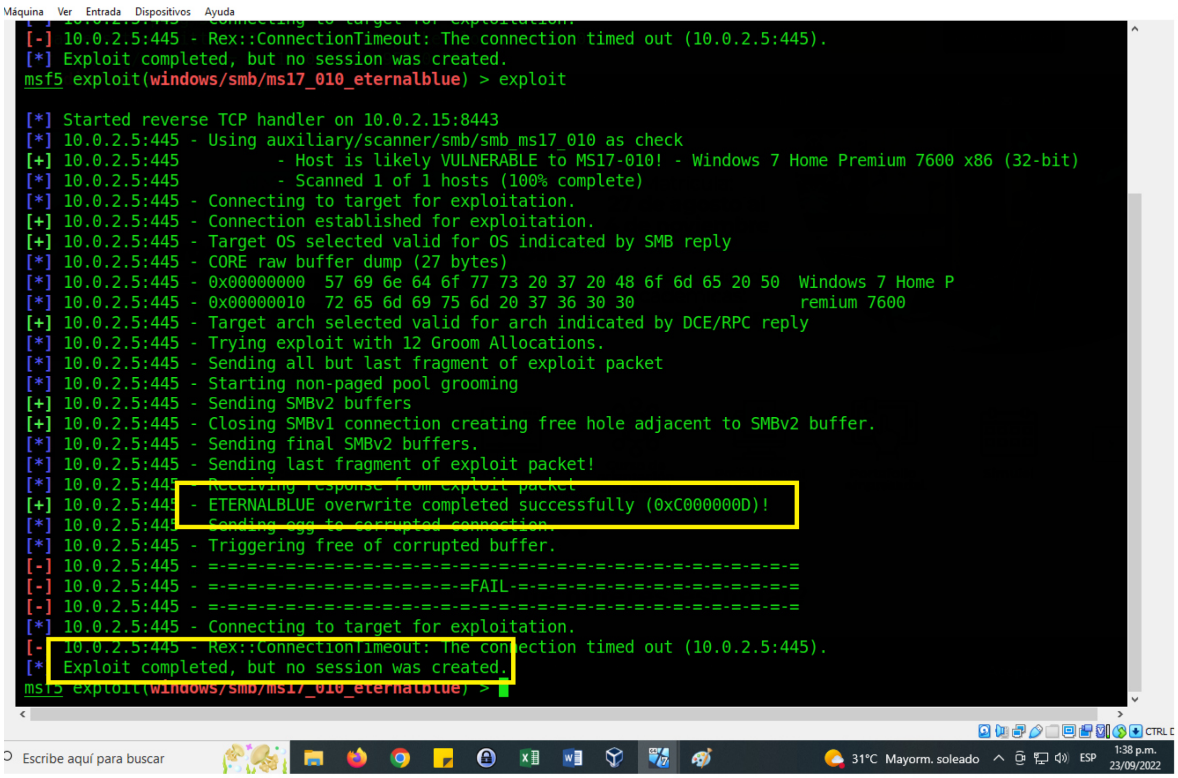
Figura 38. Pantalla azul generada por la ejecución del *payload*



Autor. Propia

Sin embargo, como se observa en la siguiente imagen a pesar de que el *payload* se ejecuta correctamente a este no le es posible establecer una sesión con el equipo objetivo, esto debido a la incompatibilidad entre la arquitectura *X64* que tiene el *payload* y la maquina objetivo que se encuentra bajo una arquitectura *X86*.

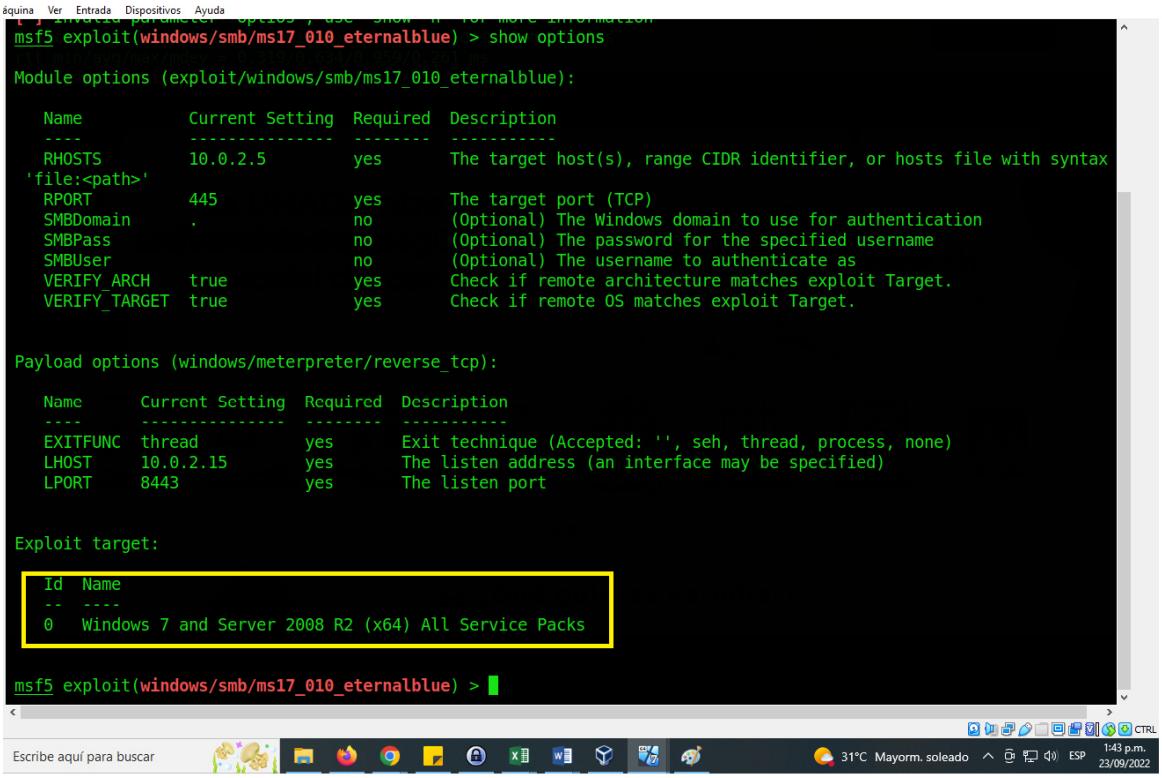
Figura 39. ***Payload*** **ejecutado sin establecer sesión con maquina objetivo**



Autor. Propia

Es posible verificar con la opción *show options* que el *payload* ejecutado se encuentra habilitado para arquitecturas *X64*, tal como lo muestra la siguiente imagen.

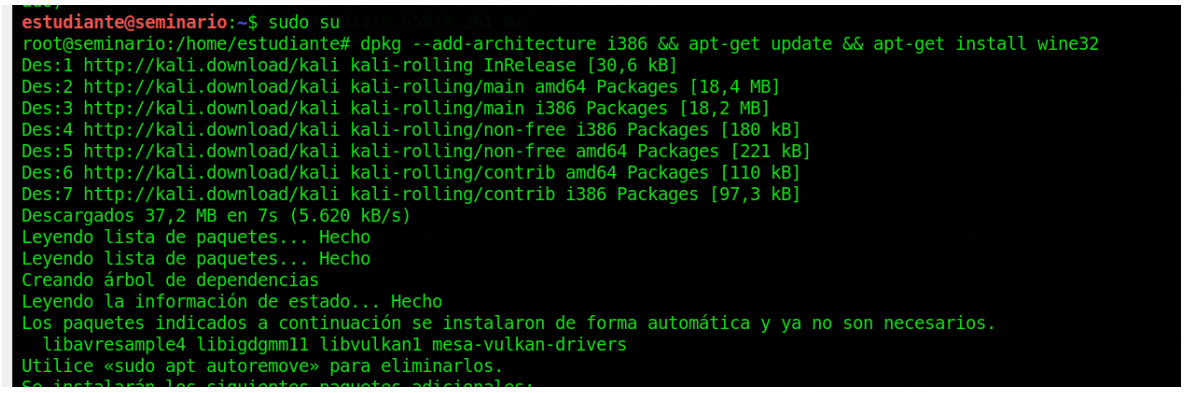
Figura 40. Arquitectura del *payload* ejecutado



Autor. Propia

Sin embargo, con el fin de conseguir el acceso a la maquina objetivo se realizarán las siguientes acciones, iniciando con la instalación en la maquina *Kali Linux* de la herramienta *wine32* la cual permite la ejecución de aplicaciones en arquitecturas de *X86* de *Windows* con usuario *root*.

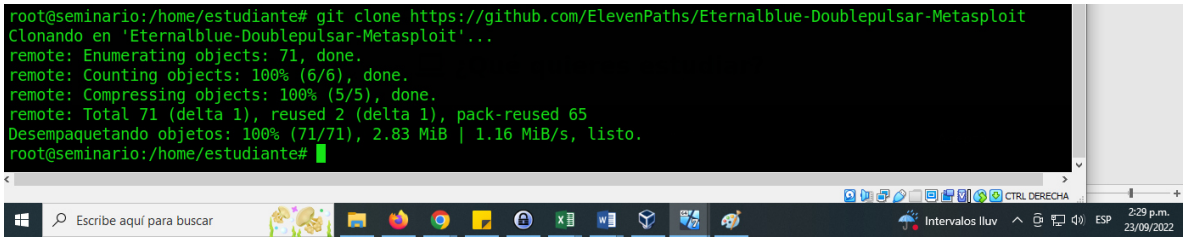
Figura 41. Instalación herramienta *wine32*



Autor. Propia

Se descarga en la maquina *Kali Linux* el repositorio *Git,* el script a ejecutar.

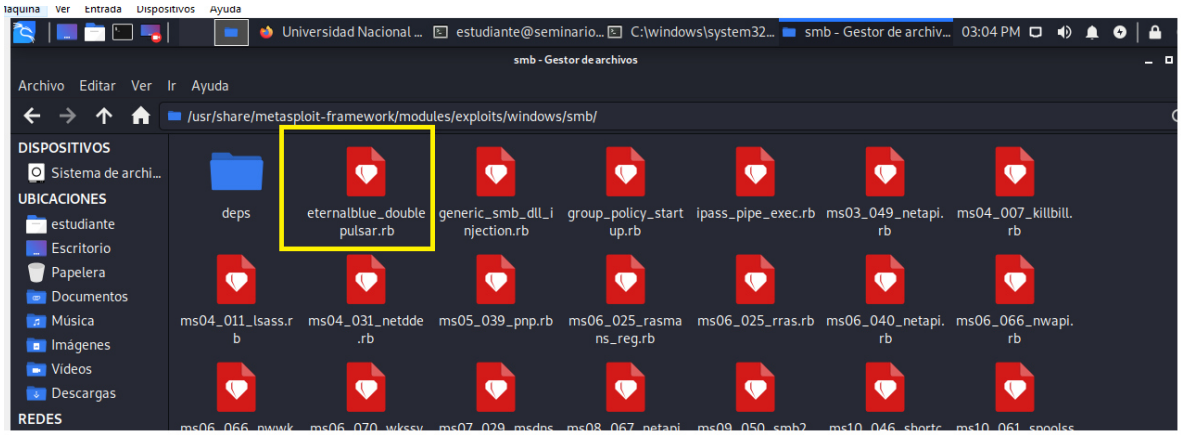
Figura 42. Descarga desde *Git* el script a ejecutar



Autor. Propia

Se valida la descarga realizada y se procede a copiar el *script* descargado en la carpeta de archivos del *Framework Metasploit*. En la siguiente imagen se observa el archivo en el respectivo directorio.

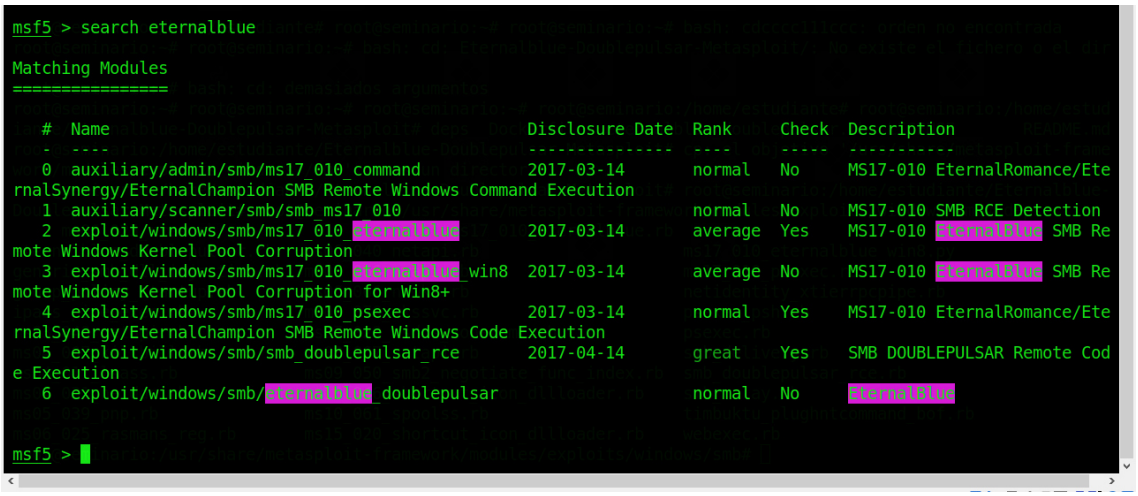
Figura 43. *Script* en la ruta del *framework Metasploit*



Autor. Propia

Se inicia el *Framework Metasploit* y se procede a ingresar al *exploit* descargado y a realizar la asignación de los parámetros requeridos para su ejecución.

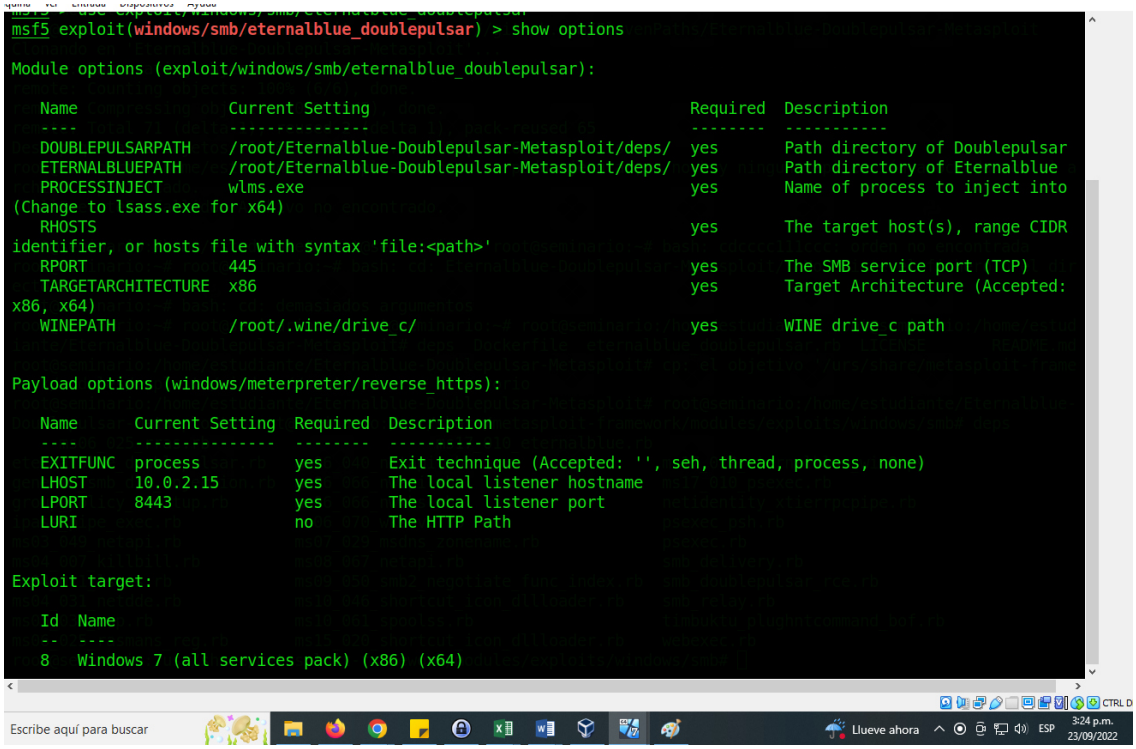
Figura 44. *Exploit* descargado *eternalblue_doublepulsar*



Autor. Propia

En la siguiente imagen se observa el *exploit* descargado y sus parámetros requeridos, así como que este soporta arquitecturas *x86*.

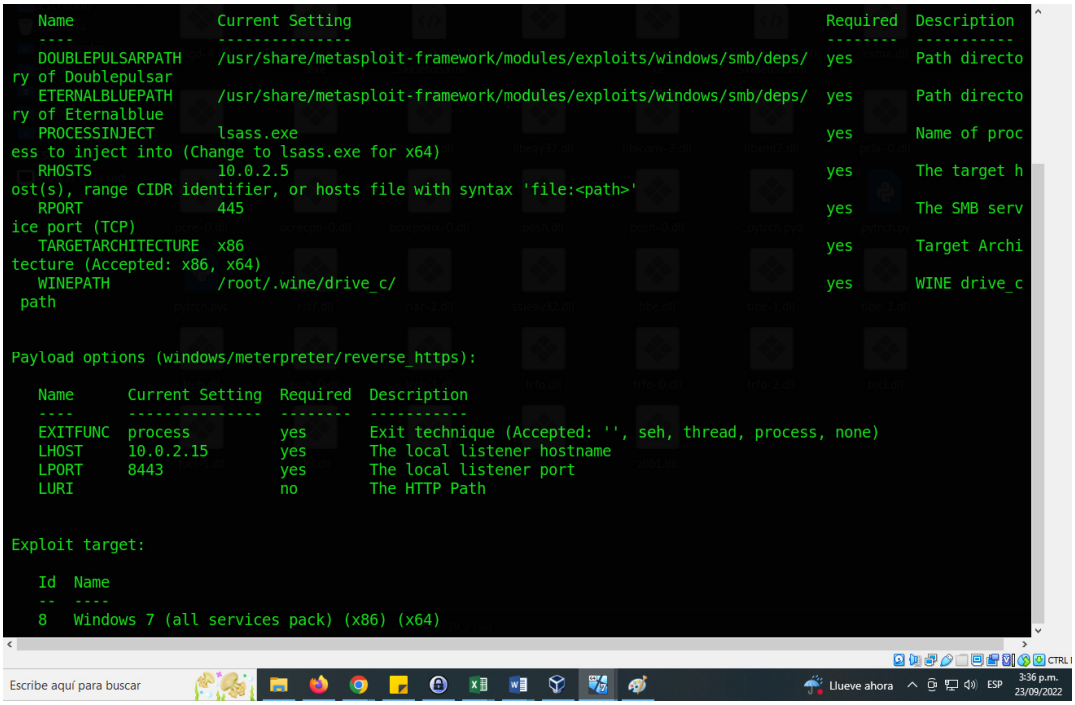
Figura 45. Parámetros *exploit eternalblue_doublepulsar*



Autor. Propia

Se realiza la asignación de los parámetros requeridos para la ejecución del *exploit*.

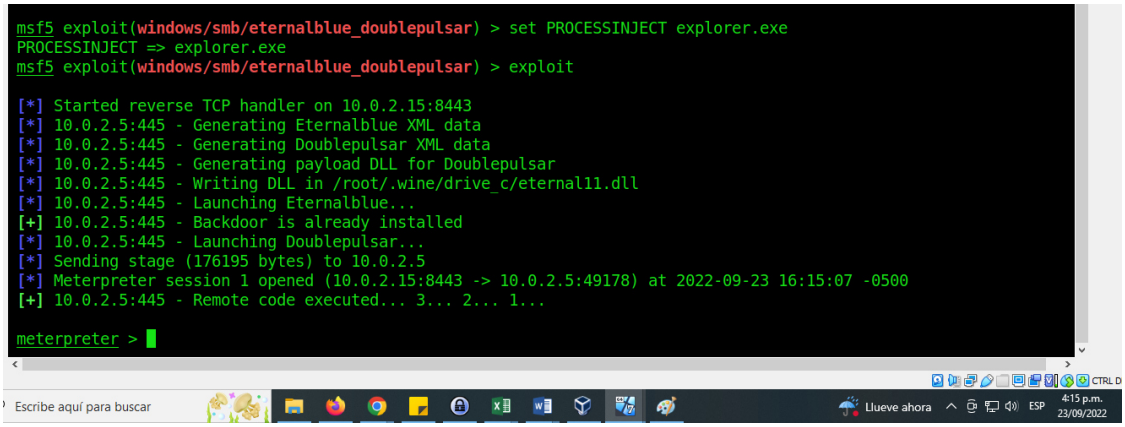
Figura 46. Asignación de parámetros *eternalblue_doublepulsar*



Autor. Propia

Una vez realizadas las configuraciones de los parámetros requeridos por el *payload* se realiza su ejecución lo cual permite acceder a través de la consola *meterpreter* y acceder a la información en el equipo.

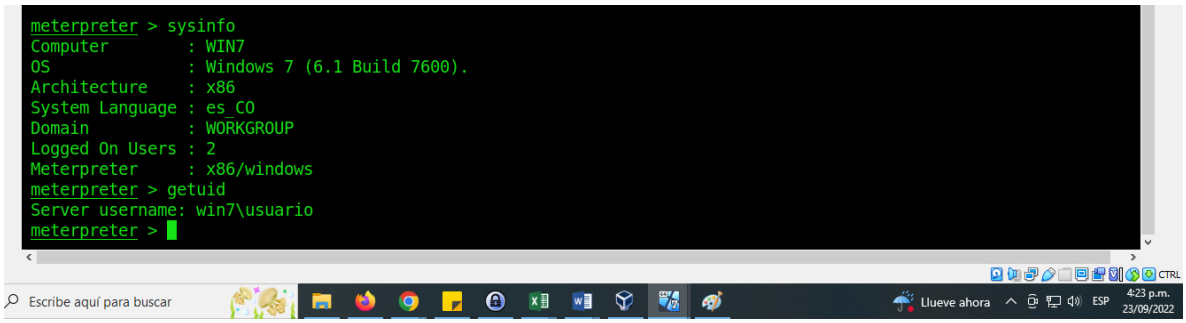
Figura 47. Maquina objetivo vulnerada



Autor. Propia

Se ejecutan comandos que permiten conocer las características del equipo atacado y el nivel de acceso obtenido.

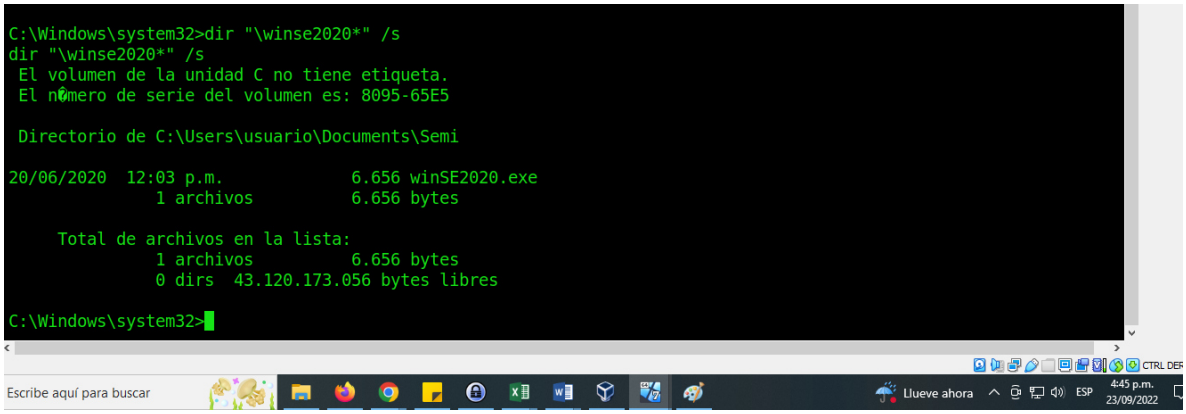
Figura 48. Ejecución de instrucciones con información de la maquina objetivo



Autor. Propia

Se procede a ingresar a CMD del equipo objetivo el comando *dir "\winse2020*" /s* con el propósito de ubicar en el equipo el archivo "*winse2020.exe*" indicado en el anexo escenario.

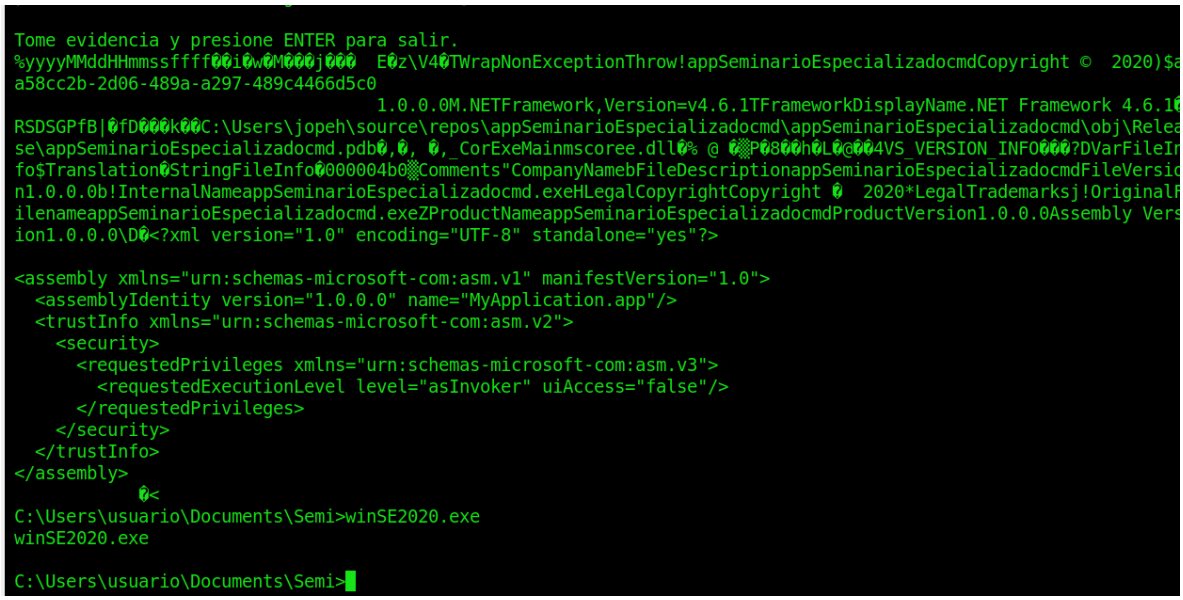
Figura 49. Búsqueda del archivo "*winse2020.exe*"



Autor. Propia

Se procede a la ejecución del archivo ubicado en el directorio *C:\users\Usuario\Documents\Semi* el cual no genera ninguna salida a pesar de contar con líneas de código.

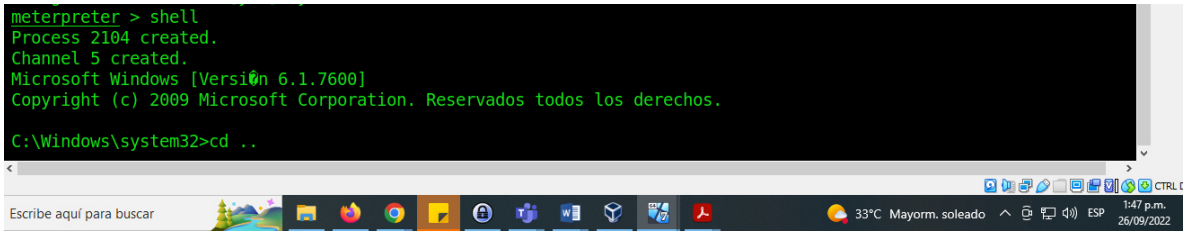
Figura 50. Pantalla del contenido del archivo “winse2020.exe”



Autor. Propia

5.2.3.4 Post explotación. En esta fase para demostrar las acciones que se pueden realizar al acceder al equipo, se procede a crear un archivo en la maquina afectada, para ello, se abre una consola desde *meterpreter* con el comando *Shell.*

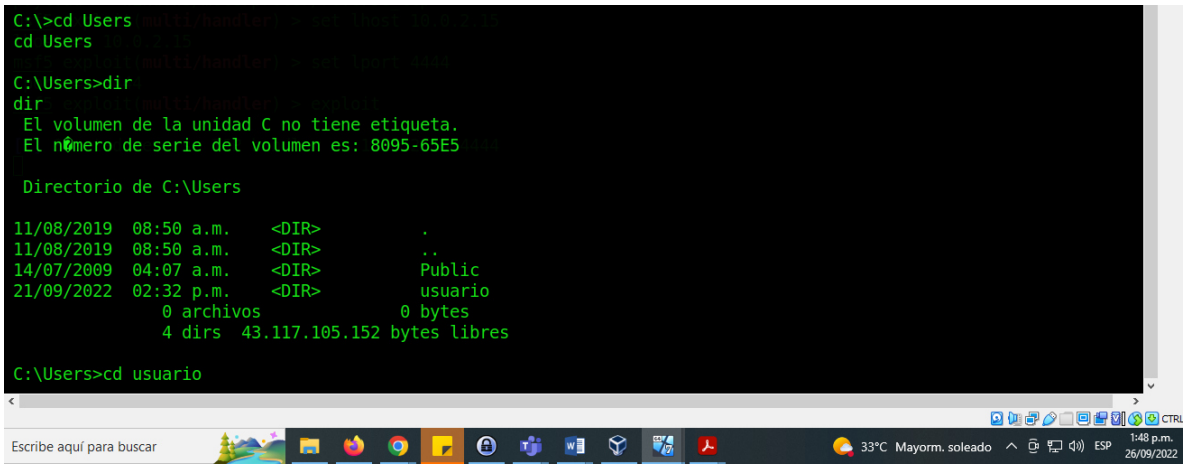
Figura 51. Consola *Shell* en la maquina atacada



Autor. Propia

Se verifica el directorio con el fin de identificar otros archivos almacenados allí.

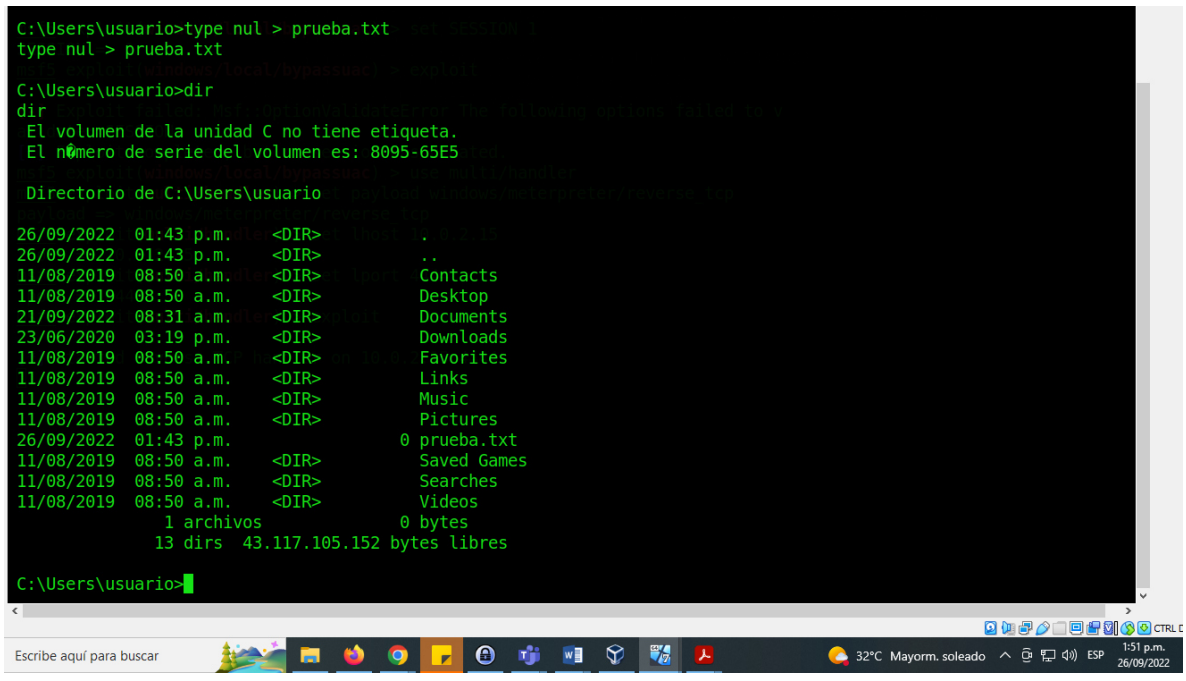
Figura 52. Verificación directorio usuario



Autor. Propia

Posteriormente se realiza la creación del archivo en el directorio del usuario con el comando *type nul > prueba.txt* y se verifica su existencia en el respectivo directorio.

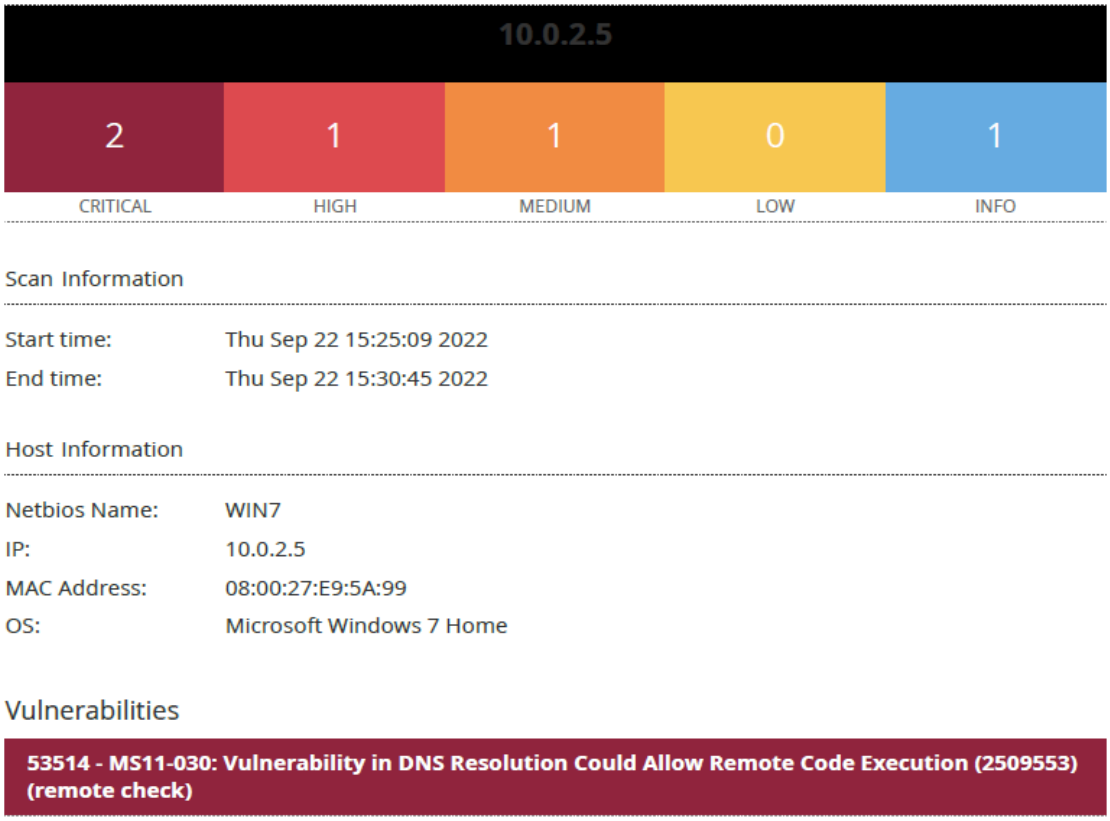
Figura 53. Archivo creado en directorio de usuario



Autor. Propia

5.2.3.5 Informe. Para esta fase se hace uso de manera complementaria de los informes generados por la herramienta *Nessus*, en la siguiente imagen se puede visualizar la información que arroja la herramienta en estos informes. Para más detalle puede revisarse en Anexo A del presente documento.

Figura 54. Informe generado por la herramienta *Nessus*



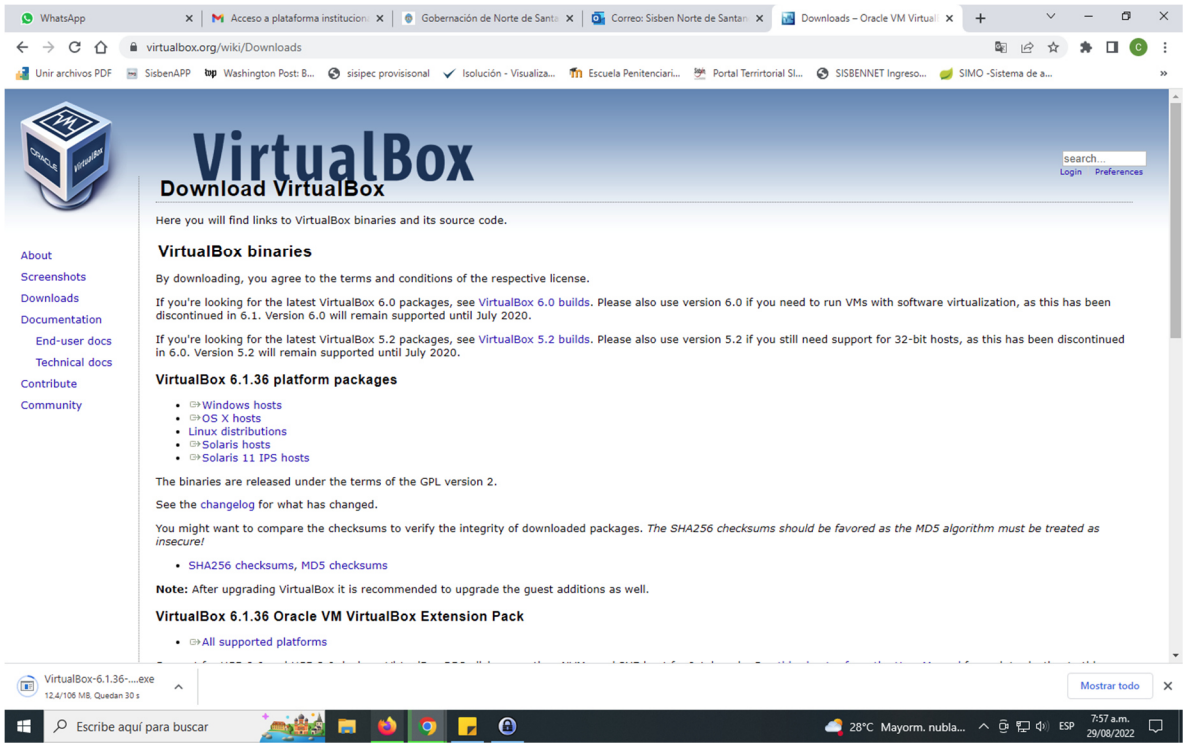
Autor. Propia

5.2.4 Herramientas para ejecución del Test de Penetración. Para llevar a cabo esta actividad se realiza el uso de las siguientes herramientas en cada una de las fases:

5.2.4.1 Pre – Ataque o Recolección de Información

Virtual Box: esta es una herramienta *software* a través de la cual se realiza la creación de máquinas virtuales, lo que permite realizar la simulación de la situación planteada en el caso de estudio bajo un entorno controlado sin afectar a los demás equipos de la red, la versión utilizada corresponde a la versión 6.1.36

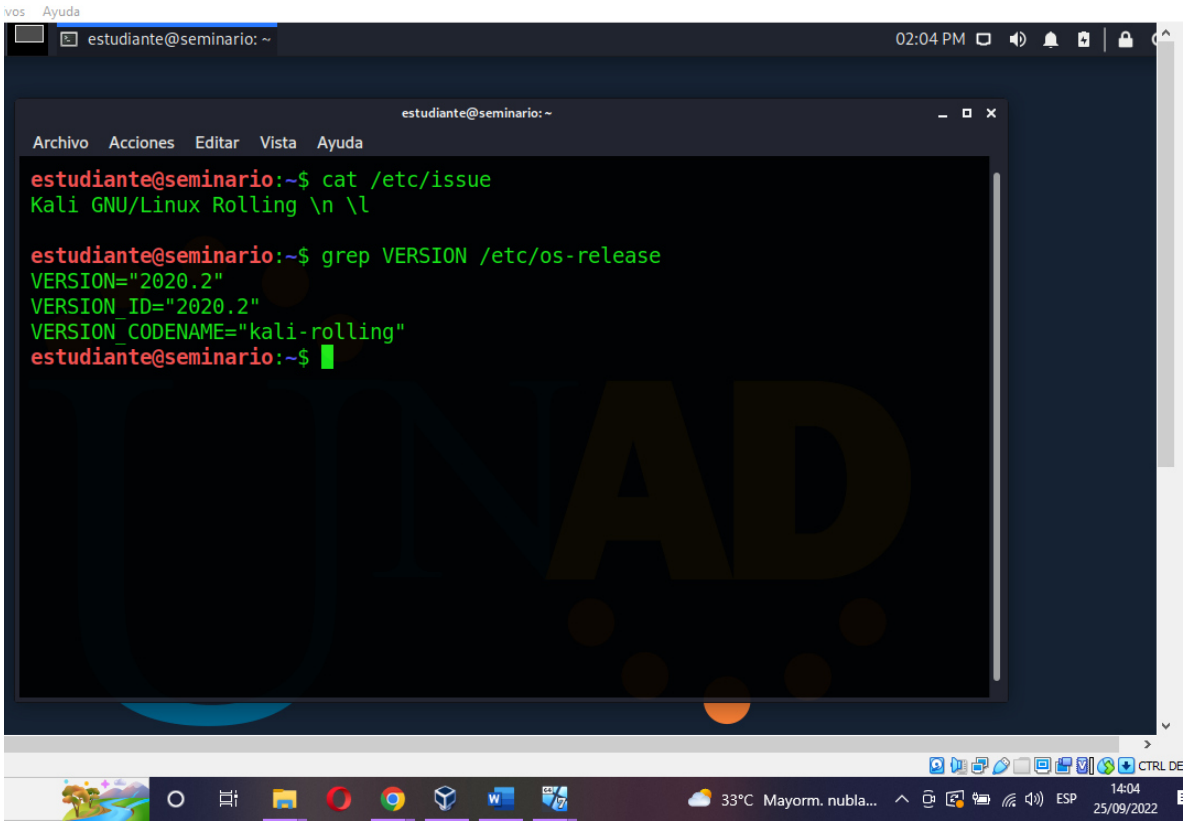
Figura 55. *Virtual Box* versión 6.1.36



Autor. Propia

Kali Linux: corresponde a una distribución de *Linux* basada en *Debian* que incorpora herramientas especializadas en temas de seguridad informática que permite realizar tareas de auditoría. Para el desarrollo del caso de estudio esta distribución se instaló en una máquina virtual independiente y dentro de la misma red de los equipos afectados bajo en entorno virtual. La máquina utilizada cuenta con la versión 2020 esto se obtuvo mediante la ejecución del comando *cat /etc/issue* y posteriormente *grep VERSION /etc/os-release* tal como se muestra en la siguiente imagen.

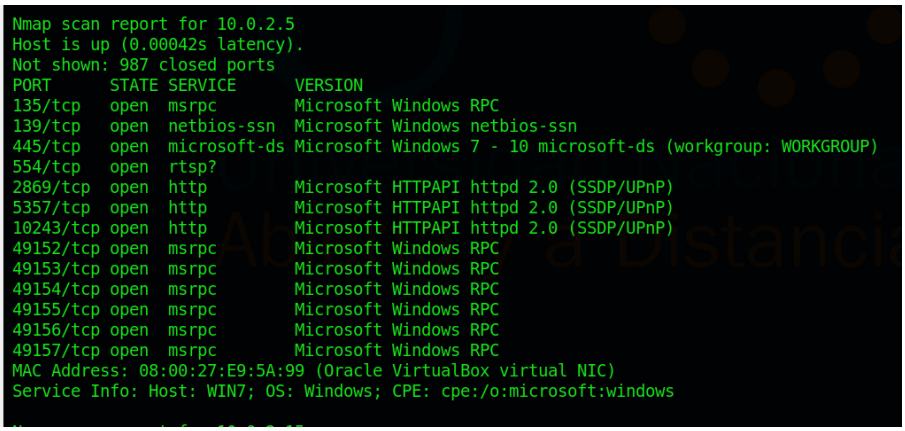
Figura 56. Maquina *Kali Linux* versión 2020



Autor. Propia

NMAP: es una herramienta gratuita a través de la cual es posible identificar vulnerabilidades de los equipos conectados a una red, así como sus características, servicios y puertos abiertos. Para el análisis del caso de estudio esta herramienta se despegó en la maquina *Kali Linux* sobre las maquinas *Windows* objetivo. Se ejecutaron comandos como *nmap 10.0.2.5/24 –sV –O* para identificar información del sistema operativo en la maquina objetivo y versión de los servicios instalados en los puertos abiertos, también *nmap 10.0.2.0/24* que permite revisar los equipos en la red.

Figura 57. Comando *NMAP* ejecutado

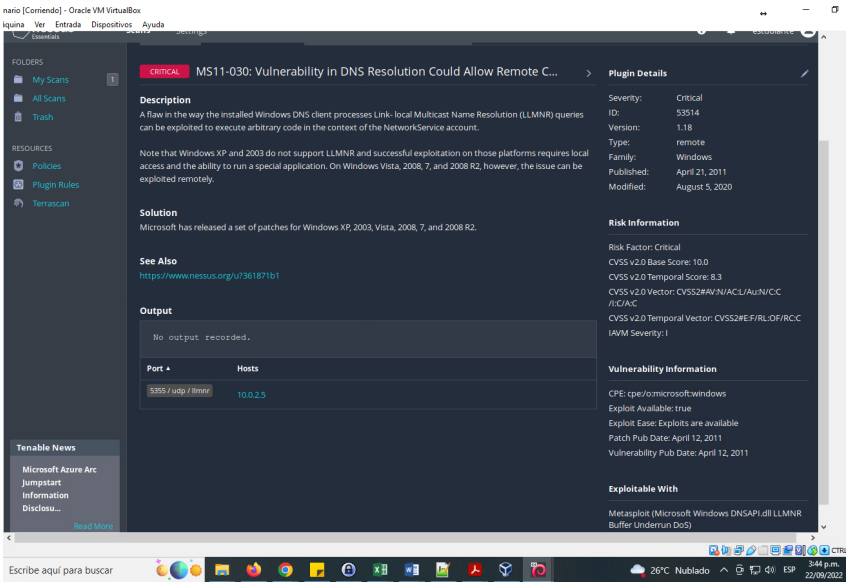


Autor. Propia

5.2.4.2 Búsqueda de vulnerabilidades

Nessus: es una herramienta *software* que permite la identificación de vulnerabilidades, muy útil en tareas de *Red Team* ya que no solo identifica la vulnerabilidad, sino que ofrece un reporte muy completo de la misma indicando entre otros la causa, posible solución, herramienta para explotación de la vulnerabilidad, existencia de *exploits* e información como código *CVE* de la vulnerabilidad.

Figura 58. Herramienta *Nessus* instalada y ejecutada

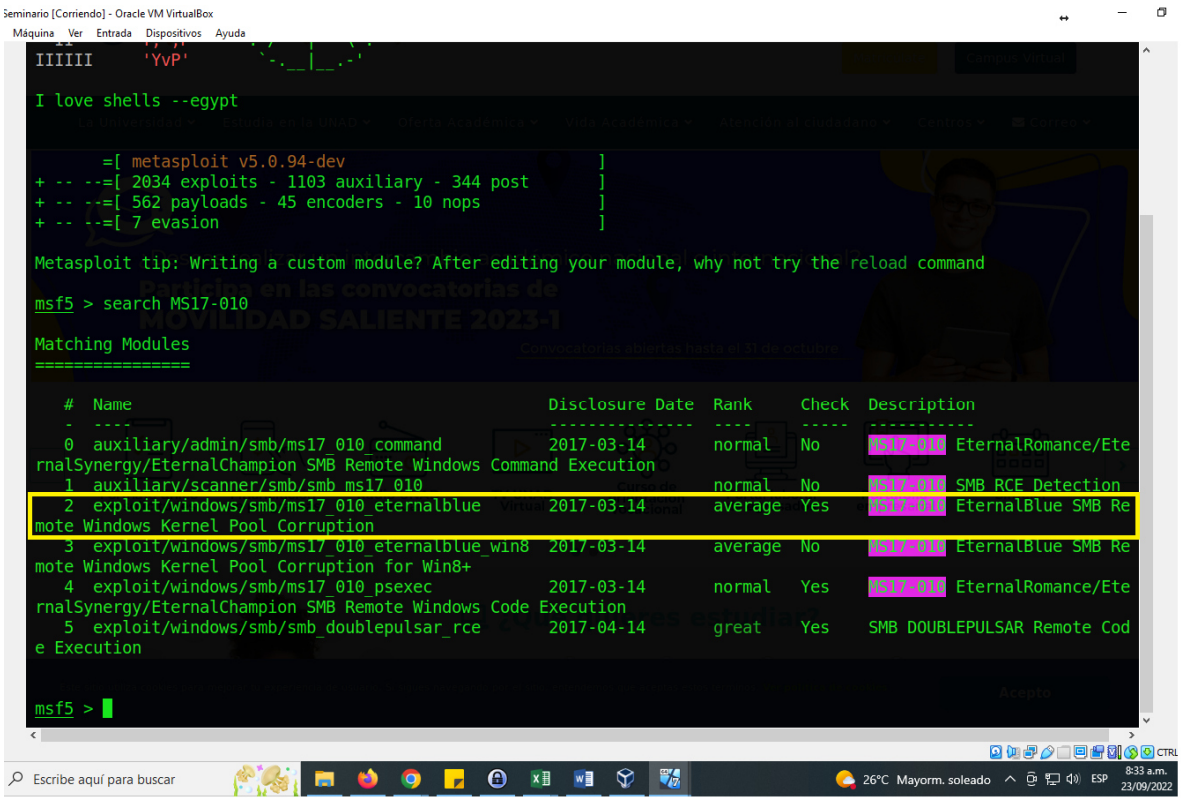


Autor. Propia

5.2.4.3 Explotación de vulnerabilidades

Metasploit: es una herramienta especializada en seguridad informática que cuenta con módulos llamados *payloads* que permiten la explotación de vulnerabilidades. Para el desarrollo del caso de estudio la herramienta fue despagada en la maquina *Kali Linux* ingresando las variables respectivas que solicita cada *payload* utilizado. Se realizó la ejecución de varios comandos como el *search* que ayuda a ubicar los *exploits* de una vulnerabilidad especifica.

Figura 59. Ejecución de comandos en *Metasploit*



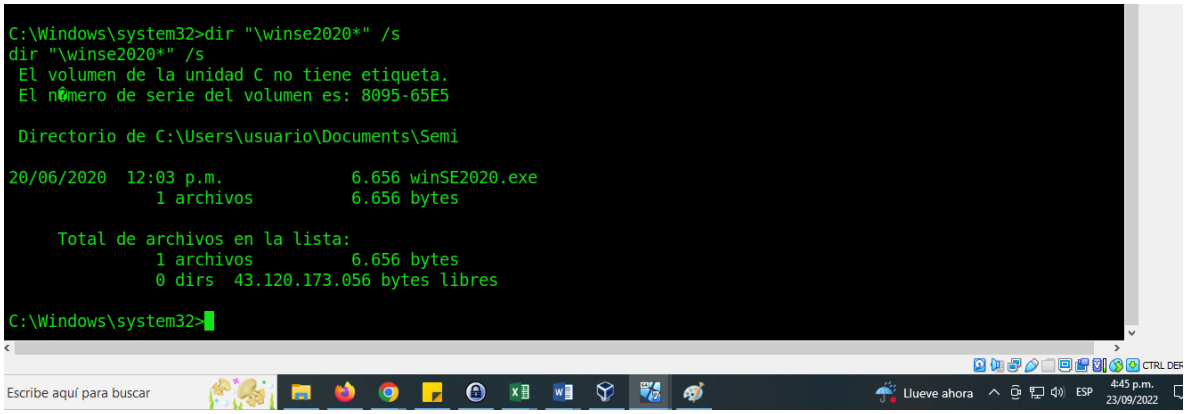
Autor. Propia

5.2.4.4 Post explotación

CMD: o símbolo del sistema es un intérprete de comandos en OS/2 y en sistemas basados en Windows NT[48], a través de esta herramienta de realiza el proceso de elevación de privilegios ya que permite ejecutar instrucciones en la maquina objetivo.

[48] WIKIPEDIA. [Sitio Web]. Símbolo del sistema de Windows. [Consultado el día 20 de septiembre del 2022]. Disponible en: https://es.wikipedia.org/wiki/S%C3%ADmbolo_del_sistema_de_Windows

Figura 60. Ejecución de comandos con la herramienta CMD

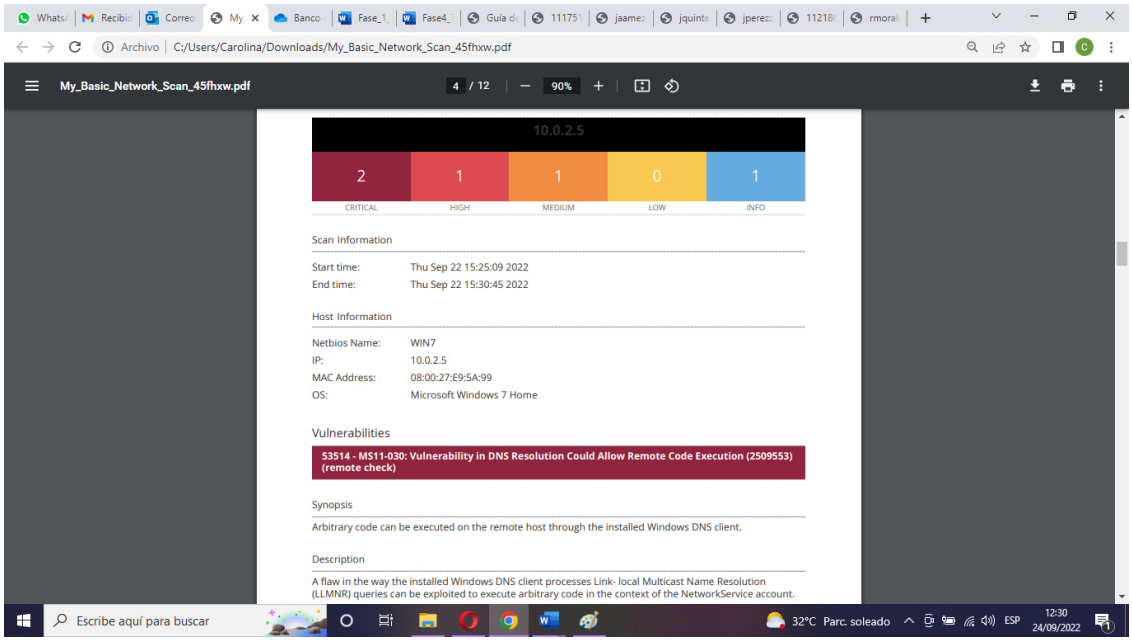


Autor. Propia

5.2.4.5 Informe

Nessus: esta herramienta cuenta con la ventaja de que en su versión gratuita ofrece informes en distintos tipos de formato, los cuales son de suma importancia a la hora de realizar el informe técnico del proceso realizado, la herramienta arroja información de la causa, posible solución, criticidad con un mapa de calor etc. de las vulnerabilidades identificadas.

Figura 61. Informe herramienta *Nessus*



Autor. Propia

6.3 DESARROLLO DEL OBJETIVO 3 – DESARROLLAR EL ANÁLISIS E IDENTIFICACIÓN DE VULNERABILIDADES CON EL FIN DE DETERMINAR LAS ACTIVIDADES DE CONTENCIÓN NECESARIAS PARA MITIGARLAS.

6.3.1 Análisis de Vulnerabilidades y Acciones de Contención

6.3.1.1 Análisis de Vulnerabilidades. Para el proceso de Análisis de las Vulnerabilidades identificadas en el caso de estudio, se utiliza el apoyo de los reportes generados por la herramienta *Nessus* los cuales se puede observar en el apartado Anexos del presente documento, la cual no solo identifica la vulnerabilidad, sino que también indica sus características y su posible solución.

- Vulnerabilidad *MS11-030 Vulnerability in DNS Resolution Could Remote Control*

Clasificación: Critica.
Código CVE: CVE-2011-0657
Descripción: es una falla respecto a la manera que un cliente DNS Windows realiza el procesamiento de las consultas del servicio *Link- local Multicast Name Resolution (LLMNR)* que permite la ejecución de código remoto con una cuenta del servicio de red.
Solución: Realizar tareas de ejecución de actualización en las maquinas afectadas.

- *Unsupported Windows OS (remote)*

Clasificación: Critica.
Código CVE: No aplica
Descripción: La versión remota de *Windows* ya no es soportada o le faltan paquetes, debido a esto es probable que se presenten múltiples vulnerabilidades.
Solución: Actualizar el Sistema Operativo o un *Service Pack*.

- *MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)*

Clasificación: Alta.
Código CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
Descripción: esta vulnerabilidad es bastante importante ya que permite a través del servicio *Microsoft Server Message Block* 1.0 (SMBv1) que un usuario sin autenticación realice accesos al sistema y ejecutar código. Está relacionada con el malware *WannaCry*, *WannaCrypt*, *Petya* utilizados para el secuestro de información a distintas organizaciones a nivel mundial.

Solución: Teniendo en cuenta la gravedad de la vulnerabilidad, Microsoft desarrolló parches de actualización para todos sus sistemas operativos incluso para algunos que no cuentan con soporte. En caso de no poder realizar el proceso de actualización es recomendable deshabilitar el servicio SMBv1

- *SMB Signing not required*

Clasificación: Media.
Código CVE: No aplica
Descripción: Esta vulnerabilidad permite la ejecución de ataques de hombre en el medio al no requerir de firma al acceso a un SMB remoto.
Solución: Configurar la política "Servidor de red de *Microsoft*: firmar digitalmente las comunicaciones" en Siempre.

- *MS16-047 Security Update for SAM and LSAD Remote Protocols B signing not required*

Clasificación: Media.
Código CVE: CVE-2016-0128
Descripción: Esta vulnerabilidad permite la ejecución de ataques de elevación de privilegios a través de la interceptación de las comunicaciones entre un cliente y un servidor por un error en la negociación de los niveles de autenticación en el servicio RPC (Llamado de Procedimientos Remotos) que permite pasar al usuario como autenticado y acceder a la base de datos SAM (Administrador de Cuentas de Seguridad)
Solución: Realizar tareas de ejecución de actualización en las maquinas afectadas.

Es importante indicar que tal y como se observa en la descripción de las vulnerabilidades identificadas, es claro que en su mayoría se deben a la falta de actualización de equipos y algunas configuraciones específicas de algunos servicios que se pueden desarrollar sin mayor contratiempo. A su vez se observa que a pesar de que la principal solución es únicamente la ejecución de parches de actualización en los equipos, el impacto de la ejecución de estas vulnerabilidades es bastante alto y puede configurar para la empresa graves pérdidas de información cuyas consecuencias pueden ser catastróficas sino se cuenta con respaldo.

6.3.1.2 Acciones de Contención. Dentro de las acciones de contención ante un ataque en tiempo real se tendría las siguientes:

- Retirar de la Red: identificados los equipos afectados inicialmente y teniendo en cuenta que el ataque se realiza a través de la red, desconectar de la red a dichos equipos, aislarlos de la red de la organización y tomar imagen de estos para posterior análisis del incidente.

- Deshabilitar el puerto 445: El puerto 445 es el puerto por defecto para el servicio SMB y es el puerto a través del cual se realiza el acceso a la maquina objetivo por lo que es necesario deshabilitarlo y proceder a habilitar el servicio en otro puerto distinto.

- Activar *Firewall*: Teniendo en cuenta que la máquina afectada contaba con el *firewall* deshabilitado, lo que facilitó el acceso en el momento del ataque, se debe realizar la activación de *Firewall* a todos los dispositivos conectados a la red de la empresa.

- Ejecutar Actualizaciones: teniendo en cuenta que las maquinas poseen *Windows 7* como sistema operativo a causa de una aplicación que solo soporta este sistema operativo y tal como lo recomienda el informe de la herramienta *Nessus* se debe realizar la ejecución de las actualizaciones y los *service pack* últimos generados por *Microsoft*.

- Informar el Incidente: es necesario denunciar el incidente ante las autoridades policiales del país, además del CSIRT gobierno.

- Documentar: se debe recopilar a través del establecimiento de un formato o herramienta establecida para tal fin, todos los hechos ocurridos en el evento, activos de información afectados, datos como archivos, IP de las maquinas involucradas y las medidas que se llevaron a cabo para la mitigación de incidente, como instrumento de gestión de conocimiento para el equipo de seguridad de la organización.

- Comunicar: es importante dar a conocer a todos los integrantes de la organización la situación presentada y las causas que permitieron que el ataque se diera con el fin de concientizar tanto a la Alta Dirección como a todo el personal de los riesgos en Seguridad y su impacto en la organización.

- Copias de Seguridad: ubicar las copias de seguridad con las que cuenten los equipos afectados, las cuales debe estar verificadas y validadas, que garanticen la recuperación de la información libre de infecciones y garantizando la continuidad del negocio.

- Gestión de Antivirus: validar el estado del software antivirus inicialmente en las maquinas afectadas para posteriormente aplicar este proceso a todos los equipos conectados a la red de la organización, ejecutar actualizaciones en caso de ser necesario.

- Gestión de Equipos Invitados: Deshabilitar el acceso como invitado a la red de la organización hasta tanto el incidente haya sido superado.

- Gestión de *Firewall* Físico: así como se realiza el bloqueo del puerto a través del cual se llevó a cabo el ataque en la máquina afectada, es necesario realizar la configuración de estos servicios en el *Firewall* de la organización, bloqueando los puertos por defecto de algunos servicios y estableciendo reglas para el filtrado de paquetes de comunicación.

6.3.2 Medidas de Hardenización. El proceso de "*Hardenizacion*" es aquel a través del cual se pretende asegurar un sistema con el fin de reducir lo más posible sus vulnerabilidades realizando las configuraciones de todos los componentes de la infraestructura de TI de una organización.

Para el caso de estudio se proponen las siguientes actividades:

- Configuraciones para evitar ataques físicos o de *hardware*: realizar actualización de firmware, generar contraseñas fuertes para el arranque del equipo y la configuración de la *BIOS*, configurar el inicio del sistema para que únicamente se ejecute en la unidad de disco duro principal, en los servidores de la organización en el centro de datos, inhabilitar las unidades ópticas y *USB* para evitar la instalación de *malware* desde dispositivos de almacenamiento externos.

- Procedimiento de Instalación de Sistema Operativo en Terminales: establecer un procedimiento para la instalación de sistemas operativos de manera segura en el cual se disponga de mínimo dos particiones, una para el sistema operativo y otra para los archivos de gestión del usuario, restringir el usuario administrador y la instalación de *software* en los equipos al personal de tecnología e instalar únicamente el software necesario para las actividades del usuario sistema.

- Configuración de actualizaciones: Incorporar sistemas de administración de cambios y configuraciones de la infraestructura de TI a través cual es posible contar con un inventario en tiempo real de la infraestructura, desplegar actualizaciones de manera masiva, administrar la configuración de los equipos de la infraestructura de manera controlada y organizada, por lo que se puede tener al día en actualizaciones a todos los equipos de la organización de manera automática e incluso silenciosa.

- Política de Gestión de Contraseñas: establecer una política de gestión de contraseñas a través de la cual se definan lineamientos de complejidad de contraseñas (uso de contraseñas fuertes), periodicidad de cambio, almacenamiento de históricos de contraseñas para evitar su repetición, uso de autenticación de doble factor.

- Procedimiento de gestión de usuarios: contar con un procedimiento a través del cual, con la información provenida desde el área de recursos humanos, se realice según el estado de la vinculación del personal y características de las

actividades a realizar, la creación, actualización y eliminación de usuarios, así como la gestión de los privilegios de acceso según su perfil.

- Política de Acceso remoto: restringir el acceso remoto a aquellos equipos que lo requieran, mantener el inventario de los equipos con acceso remoto compartido y establecer un lineamento de comunicaciones seguras vía *VPN* o *SSH*.

- Procedimiento de *Backup*: establecer un procedimiento de generación y verificación de los *Backups* de los equipos donde se establezca periodicidad y medios externos de almacenamiento de dichas copias que incluyan en lo posible resguardo en instalaciones ubicadas fuera de las instalaciones de la empresa.

- Solución *Firewall*: adquirir una solución *Firewall* de última generación con capacidades de detección y contención de amenazas, anti *malware*, filtrado *web* y administración de *VPN*.

- Capacitación: se debe establecer planes de capacitación a todos los integrantes de la organización con el fin de concientizar en materia de seguridad y establecer canales de comunicación a través de los cuales los usuarios informen anomalías al equipo de seguridad, esto teniendo en cuenta que el factor humano es el más vulnerable a la hora de realizar ataques.

- Plan de Respuesta a incidentes de ciberseguridad: establecer un "Plan de Respuesta a Incidentes de Ciberseguridad"[49] a través del cual se establezca una metodología que indique las actividades a realizar el caso de un ciberataque.

- Contar con Proveedores en Ciberseguridad: contar con un equipo de Servicios Administrador de Seguridad – MSSP[50] por medio de un proveedor especializado a través de los cuales se generen estrategias para la disminución de vulnerabilidades, el riesgo y el impacto de los ataques.
- Gestión de Dispositivos Móviles: adquirir una solución para gestión de los dispositivos móviles conectados a la red de la organización mediante la cual se controlen las aplicaciones instaladas, localización y protección en caso de robo o pérdida.

[49] NETDATANETWORKS. [Sitio Web]. Plan de respuesta a incidentes de ciberseguridad: lo que debes hacer en caso de un ciberataque. Consultado el día 29 de Septiembre del 2022. Disponible en https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

[50] FORTINET. [Sitio Web]. Servicios administrados de seguridad – MSSP. Consultado el día 29 de Septiembre del 2022. Disponible en: https://www.fortinet.com/lat/solutions/service-provider/communications-service-provider/mssp

- Aplicación de Estándares de Ciber Seguridad: es importante que la organización realice las acciones pertinentes a la adopción y certificación de estándares en materia de ciber seguridad como ISO 27000 o el *framework* NIST.

6.3.3 Diferencias entre equipos de Blue Team y el de Respuesta a Incidentes Informáticos. Tanto los equipos *Blue Team* y los Equipos de respuestas a incidentes (CSIRT) tienen funciones o roles muy específicos, la siguiente tabla comparativa los ilustra.

Tabla 2. Comparativo *Blue Team Vs*. Equipo de Respuesta a Incidentes

Blue Team	Equipo de Respuesta a Incidentes
Dar recomendaciones para prevenir ataques y ponen a disposición de la comunidad la información recogida para que otros puedan saber reconocer y mitigar ataques futuros.	Recibir, analizar y responder ante los incidentes recibidos desde las comunidades colaboradoras.
Monitorea y realiza controles de seguridad frecuentes. Vigilancia constante contra los ataques.	Realiza acciones detener el impacto en el momento de identificado el ataque.
Realiza análisis de vulnerabilidades y amenazas.	Realiza análisis forenses.
Desarrollar parches para dar solución a errores.	Solucionar incidentes.
Papel más preventivo.	Labor es reactiva, porque se actúa cuando el hecho ha sucedido.

Autor. Propia

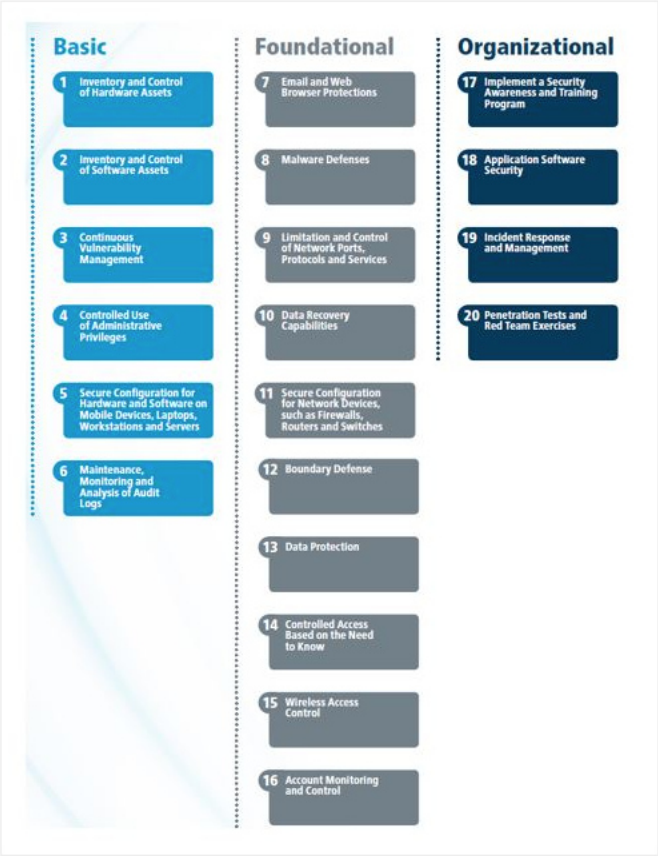
6.3.4 Análisis CIS "*Center for Internet Security*". El *Center for Internet Security (CIS)* es una organización sin fines de lucro formada en octubre de 2000. Su misión es "identificar, desarrollar, validar, promover y mantener soluciones de mejores prácticas para la defensa cibernética y construir y liderar comunidades para permitir un entorno de confianza en el ciberespacio"[51].
El *CIS* cuenta con una serie de controles críticos de seguridad que permiten reducción de riesgos antes ciber ataques. Para un equipo *Blue Team* sería de gran importancia trabajar de la mano de la implementación de estos controles CIS ya que permite fortalecer la seguridad en las organizaciones. Estos controles representan una serie de buenas prácticas en materia de ciber seguridad formuladas por un

[51] KIPPEO. Adoptar las Mejores Prácticas del CIS (Center For Internet Security) En Tiempos De COVID-19. Consultado el día 29 de Septiembre del 2022. Disponible en:https://kippeo.com/adoptar-las-mejores-practicas-del-cis-center-for-internet-security-en-tiempos-de-covid-19/

grupo de expertos resultado de experiencias y en la gestión de la respuesta ante incidentes.

Los controles CIS contienen un listado 20 recomendaciones en ciber seguridad que según *Center for Internet Security*, "*Las Organizaciones que solo adoptan los primeros 5 Controles, pueden reducir los Riesgos hasta en un 85%"* y otorgan acciones en materia de ciber seguridad de fácil entendimiento para los profesionales de tecnología divididas en tres grandes grupos.

Figura 62. Controles *CIS*



Tomado de https://blog.isecauditors.com/2019/11/novedades-version-7-1-controles-cis.html

También es importante decir que se debe ubicar el grupo de implementación al que pertenece la organización, el CIS define 3, donde 1 es aquel que cuenta con recursos en ciber seguridad y conocimientos en el tema limitados y 3 donde la organización es mucho más madura en temas de ciber seguridad. La implementación de los controles CIS debe realizarse de la mano de firmas expertas en Seguridad ya que tiene algunas falencias en el tema del alcance del marco de trabajo.

Para cualquier equipo de seguridad de una organización implementar estos controles siempre representará mejoras en la seguridad de las organizaciones, así como en los procesos que ello conlleva, por lo que es un marco de trabajo que ayuda a mejorar notablemente varios aspectos de seguridad.

6.3.5 Características y Funciones de un SIEM. Los Sistemas SIEM (*Security Information and Event Management*) que en español traduce "Información sobre Seguridad y Gestión de Eventos" les proporciona a las organizaciones las capacidades para identificar dar respuesta a las amenazas de un sistema informático.

SIEM proviene de una evolución de sus antecesores, los SEM ("Gestión de eventos de seguridad") encargados de la detección de patrones sospechosos en tiempo real y los SIM ("Gestión de información de seguridad") que centralizan datos de registros de seguridad para su almacenamiento y análisis en tiempo real permitiendo realizar acciones en tiempo real.

SIEM recopila de manera permanente grandes volúmenes de registro de información y dispositivos de una organización con el fin de proporcionar una fuente de información para los equipos de seguridad que les permite identificar de manera temprana comportamientos, tendencias, explotación de vulnerabilidades que pueden llegar a ser futuros ataques, realizando el análisis en tiempo real y emitiendo alertas para que se tomen las salvaguardas necesarias.

El SIEM trabaja de la mano de los SOAR (Orquestación, automatización y respuesta de seguridad) quienes son los que reciben las alertas de seguridad emitidas por el SIEM y es el que a través del cual los equipos de respuesta pueden investigar las causas y realizar los correctivos necesarios.

En síntesis, un SIEM es una solución en términos de seguridad que le permite a las organizaciones identificar posibles amenazas o vulnerabilidades antes de que estas sean explotadas o que generen algún impacto en la organización todo esto en tiempo real mediante la revisión permanente y el registro de información de seguridad con propósitos de cumplimiento o de ser auditados.

6.3.5.1 Características. La gran mayoría de las soluciones SIEM cuentan con las siguientes características:

- Identificación de amenazas reales y falsos positivos.
- Monitoreo permanente de manera centralizada de posibles amenazas.
- Alerta al personal con capacidades para dar solución al incidente.
- Gestión de conocimiento sobre incidentes de seguridad para su rápida solución.

- Documentación de las actividades de gestión de incidentes, tales como identificación, acciones realizadas y solución.
- Cumplimiento de normatividad vigente respecto a protección de datos y seguridad de la información.

6.3.5.2 Funciones. Toda solución SIEM posee básicamente las siguientes funciones las cuales varían según la capacidad de la solución adquirida:

- Gestión de Registros: el sistema recopila datos de registros y de comportamiento de un sinnúmero de sistemas y componentes de una red de datos los cuales son almacenados en tiempo real.

- Correlación de Eventos y Análisis: a través del análisis de datos complejos permite identificar e interpretar patrones de comportamiento que son una herramienta fundamental para la identificación y mitigación de amenazas potenciales, mejorando los tiempos de detección y de respuesta ante incidentes.

- Monitoreo de incidentes y alertas de Seguridad: SIEM tiene la capacidad de monitorear en tiempo real todos elementos de la infraestructura, usuarios y sistemas de una organización conectados a la red identificando patrones de comportamiento de los mismos y mediante la configuración de reglas de correlación emitir alertas al personal con el fin de realizar acciones de mitigación previo a la consecución de un incidente de seguridad con mayor impacto.

- Gestión de conformidad e informes: son una gran opción para aquellas organizaciones que requieren presentar alto cumplimiento de tipo regulatorio ya que permite a través de la recopilación de información en tiempo real verificar datos de conformidad en toda la organización a través de la generación de reportes automatizados.

6.3.5.3 Ventajas. Los sistemas SIEM son una gran herramienta a través de la cual las organizaciones pueden salvaguardar tanto su infraestructura como su información de cualquier tipo de amenazas externa o interna, mediante el monitoreo en tiempo real, disminuyendo tiempos tanto en la identificación como gestión de los mismos. Dentro de las ventajas de los sistemas SIEM existen las siguientes:

- Identificación de manera avanzada de amenazas en tiempo real: reducen de manera significativa los tiempos de identificación y reacción ante posibles amenazas.

- Automatización a través de IA: los SIEM de próxima generación tiene capacidades de integración con los SOAR y utilizan técnicas de *machine learning* que se adaptan de manera rápida al comportamiento de la red, permitiendo el uso de protocolos complejos de identificación y reacción ante amenazas potenciales.

- Mejoramiento de la gestión organizativa: permite la colaboración entre equipos para la mejora de respuesta a incidentes.

- Identificación de amenazas avanzadas conocidas y desconocidas: mediante el uso de tecnologías de IA, estas soluciones permiten realizar acciones de mitigación de amenazas tales como: Amenazas internas, *phishing*, inyección de código *SQL*, ataques de Denegación de Servicio Distribuido y robo de datos.

- Investigaciones Forenses: permiten la aplicación de técnicas forenses mediante la recopilación de datos de registro de los activos de información, por lo que se puede establecer todo el historial que antecedió el incidente con el fin de establecer acciones de prevención.

- Monitoreo de Usuarios y aplicaciones: estas soluciones permiten el monitoreo del comportamiento de usuarios y aplicaciones que accedan a activos de información de la organización independiente mente de su ubicación.

- Base de Conocimiento: permiten afianzar la gestión de conocimiento en materia de detección y reacción ante incidentes de seguridad toda vez que ofrecen la capacidad de documentar constantemente los incidentes de manera centralizada permitiendo mejoras en los tiempos de solución y actuación.

- Reducción de Costos: a través de la automatización de procesos permite mejora la gestión de recursos tanto tecnológicos como humanos representando ahorro para las organizaciones.

6.3.6 **Herramientas de contención *Hardware* y *Software.*** El mercado actual ofrece una serie de herramientas que le ayudan a los equipos de seguridad en las organizaciones en la mitigación y contención de incidentes de seguridad algunas se listan a continuación.

6.3.6.1 Hardware

- Firewall de Próxima Generación: son una evolución de los *firewalls* tradicionales cuyas actividades van más allá de su actividad tradicional de bloques de paquetes y puertos al conformar un sistema IPS, con capacidad de prevención y protección antivirus, *malware*, monitoreo de aplicaciones, *ransomware* basándose en la definición de políticas que permiten la realización de acciones ante actividades sospechosas. Los *Firewall* de Próxima Generación de *Fortigate* frecen capacidades de IPS, Antivirus, configuración de políticas, análisis de dispositivos IoT y móviles.

- Cisco ASA 5500 edición Anti-X: es un *firewall* de próxima generación cuyo principal objetivo es la gestión de amenazas de Internet en el *Gateway*, tales como o *spyware*, *spam*, virus entre otras asociadas a contenido de internet.

6.3.6.2 Software

- *McAfee Enterprise Security Manager*: es una herramienta SIEM provista por *McAfee* con capacidades de monitoreo de infraestructura tecnológica, usuarios y aplicaciones que realiza actividades de recopilación, análisis y contraste con una robusta base de registros identificando amenazas de manera inteligente.

- Herramientas EDR (*Endpoint Detection and Response*): es una evolución a los antivirus de *endpoints* ya que permite el monitoreo permanente e los dispositivos y la red cuyo principal objetivo es la identificación, prevención, detección de amenazas avanzadas (APT) llegando incluso a tomar acciones de manera inmediata si así se requiere realizando la reparación del *endpoint* afectado. Como solución de cogido abierto como *Snort*, creado por *Cisco Systems* cuya actividad se basa en el monitoreo de paquetes.

- Herramientas MDR (Servicio de detección y respuesta gestionadas): *Kaspersky Managed Detection and Response* (MDR) es un servicio que permite la búsqueda, detección y eliminación de amenazas dirigidas a una organización.

7 LINK VIDEO DE SUSTENTACION

El siguiente enlace corresponde a la sustentación del trabajo realizado.
https://youtu.be/Jw7_vjjYlKQ

8 CONCLUSIONES

Es claro que las organizaciones hoy en día se enfrentan a una nueva amenaza la denominada ciber delincuencia, es necesario entonces que las organizaciones cuenten con equipos de seguridad que propendan por salvaguardas su información.

En Colombia existe una serie de Legislación en materia de Seguridad y protección de datos personales, entre otros, aplicable a los equipos *Blue* y *Red Team*, siendo pionera en el desarrollo de esta normativa donde se ha definido penalmente una serie delitos en relación a la seguridad informática estableciendo penas y agravantes para estas acciones, los datos personales y su gestión, sin embargo, la tecnología y ciber delincuencia avanza aún más rápido que la generación de normativa por lo que es necesario que el país avance en este sentido ya que la delincuencia informática avanza a pasos agigantados y la justicia se queda algo corta.

Las pruebas de *Pentesting* le permitió al equipo de seguridad *Red Team* conocer la manera a través de la cual es posible realizar un ataque a la organización, este ejercicio permitió establecer y simular las técnicas que pueden llegar a ser aplicadas por los delincuentes informáticos para la explotación de vulnerabilidades.

A través de las pruebas de *Pentesting* fue posible identificar las vulnerabilidades presentadas en las maquinas objeto del análisis y esto permite trazar una hoja de ruta en relación a los ataques que se pueden realizar midiendo de esta manera su alcance y su impacto, con el fin de ilustrar a la organización de los riesgos que se evidencian en los distintos elementos de la infraestructura de TI.

Los equipos *Blue Team* tienen como principal propósito establecer los lineamientos necesarios para la protección de los activos de información de las organizaciones, una vez identificadas las vulnerabilidades y conocidos los métodos de ataque y su impacto, se desarrollaron desde un rol *Blue Team* una serie de propuestas que permiten endurecer la infraestructura de TI y mejorar las condiciones de seguridad para prevenir ataques futuros, seleccionando una serie de herramientas *hardware* y *software* así como medidas en pro de la mejora de la seguridad.

9 RECOMENDACIONES

Uno de los aspectos más vulnerable y que se puede estudiar en un futuro es el factor humano. Sin duda alguna los ataques de ingeniería social donde el principal objeto de ataque utilizado como puerta de entrada son las personas. Como responsables de la seguridad es necesario trabajar en la concientización y educación en materia de seguridad en las personas a nuestro alrededor ya que como se sabe con un talento humano capacitado y alerta es posible identificar oportunamente actividades sospechosas.

Es importante para las organizaciones contar con Planes en materia de ciber seguridad a través de los cuales se puede reducir el riesgo de impacto de ataques informáticos, establecer Procedimientos de *Backups*, Gestión de usuarios y permisos, Gestión de Contraseñas, Actualización periódica de equipos, Cronograma de Capacitación, acciones que no implican mayores costos y que de llevarse a cabo ayudan a

Definir la realización periódica de Análisis de Riesgos informáticos ya que el riesgo no es estático, con el fin de estar al tanto de las posibles eventualidades en materia de identificación de nuevas vulnerabilidades que se pueden estar presentando en la organización, como por ejemplo copias no validadas, controles no aplicados y nuevas tendencias en ataques.

Es importante estudiar la inversión en ciber seguridad requerida para el endurecimiento de la infraestructura de la organización y teniendo en cuenta los recursos económicos en una organización deben invertirse de manera adecuada, se debe establecer el retorno sobre la inversión que para la organización implica la adquisición de nueva tecnología en materia de seguridad, se debe determinar el valor del impacto de ataques en dinero y en reputación para que la alta dirección identifique la importancia de estas inversiones.

10 BIBLIOGRAFÍA

ACOSTA, David. Guía rápida para entender el marco de trabajo de ciberseguridad del NIST [En Línea]. 2017. [Consultado el 8 de Octubre del 2022]. Disponible en: https://www.deacosta.com/guia-rapida-para-entender-el-marco-de-trabajo-de-ciberseguridad-delnist/#A_que_tipo_de_organizaciones_aplica

ALEGSA. Definición de Red de computadoras. [Sitio Web]. [Consultado el 27 de Noviembre del 2021]. Disponible en: https://www.alegsa.com.ar/Dic/red_de_computadoras.php

CARACTERÍSTICAS.CO. Investigación documental. [Sitio Web]. [Consultado el 6 de octubre del 2021]. Disponible en: https://www.caracteristicas.co/investigacion-documental/

CHOWDAPPA, K.Bala, LAKSHMI, S.Subba. Ethical Hacking Techniques with Penetration Testing. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3389-3393. [Consultado el 27 de Noviembre del 2021]. ISSN: 0975-9646. Disponible en: http://ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503161.pdf

CIC Consulting Informático. Seguridad de la Información y Ciberseguridad ¿es lo mismo? [Sitio Web]. [2021]. [Consultado el 5 de octubre del 2021]. Disponible en: https://www.cic.es/seguridad-de-la-informacion-y-ciberseguridad-es-lo-mismo/

CISCO. What Is a Firewall? [Sitio Web]. [Consultado el 6 de octubre del 2021]. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

CISET. Firewall o cortafuegos. [Sitio Web]. [Consultado el 5 de octubre del 2021]. Disponible en: https://www.ciset.es/glosario/444-firewall?dt=1633550425620

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 127. (5, enero, 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. En: Diario Oficial. Enero, 2009. Nro. 47.223.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1032. (22, junio, 2006). Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal. En: Diario Oficial. Junio, 2006. Nro. 46.307

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (18, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial. Octubre, 2012. Nro. 48.587.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES. CRC presenta informe sobre comportamiento del servicio de Internet desde el inicio del estado de Emergencia por COVID-19. [En Línea]. [2021]. [Consultado el 8 de Octubre del 2022] Disponible en: https://www.crcom.gov.co/es/noticias/comunicado-prensa/crc-presenta-informe-sobre-comportamiento-servicio-internet-desde-inicio

COMUNIDAD DRAGONJAR. ¿Cómo se realiza un Pentest? [Sitio Web]. [Consultado el 4 de octubre del 2021]. Disponible en: https://www.dragonjar.org/como-realizar-un-pentest.xhtml

COPNIA [En Línea]. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [2015]. [Consultado el 6 de octubre del 2021]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

COPNIA. Ley 842 del 2003. (9, octubre, 2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. En: Diario Oficial. Octubre, 2003. No. 45.340.

EC-Council (n.d.). Ethical Hacking and Countermeasures: Attack Phases, 1st Edition, Estados Unidos: EC-Council Press, 2012. ISBN-13: 978-1-43548-360-6, ISBN-10: 143548360X

ERICKSON, Jon. Hacking: The Art of Exploitation, 2nd Edition, San Francisco CA: No Starch Press Inc., 2003. ISBN-13: 978-1-59327-144-2, ISBN-10: 1- 59327-144-1

FADIA, Ankit. The Ethical Hacking: Guide to Corporate Security, 1st Edition, Estados Unidos: Edition, Macmillan, 2005. ISBN-13: 978-14-0392-445-2, ISBN-10: 1-40392-445-7

FORTINET. [Sitio Web]. Servicios administrados de seguridad – MSSP. [Consultado el día 29 de Septiembre del 2022]. Disponible en: https://www.fortinet.com/lat/solutions/service-provider/communications-service-provider/mssp

FRANCO, David A; PEREA, Jorge L y PUELLO, Plinio. Metodología para la Detección de Vulnerabilidades en Redes de Datos. *Inf. tecnol.* [En línea]. 2012, vol.23, n.3 [citado 2022-10-08], pp.113-120. Disponible en:

http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014&lng=es&nrm=iso . ISSN 0718-0764. http://dx.doi.org/10.4067/S0718-07642012000300014.

FRANCO, David A; PEREA, Jorge L y TOVAR, Luis C. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. *Inf. tecnol.* [En línea]. 2013, vol.24, n.5 [citado 2022-10-08], pp.13-22. Disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003&lng=es&nrm=iso. ISSN 0718-0764.

FUNCIÓN PÚBLICA. Decreto 1377 de 2013. [Sitio Web]. [Consultado el 8 de Diciembre del 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

FUNCIÓN PÚBLICA. Ley 1581 de 2012. [Sitio Web]. [Consultado el 5 de octubre del 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [Sitio Web]. [Consultado el 25 de Noviembre del 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INCIBE. ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. [Sitio Web]. [Consultado el 5 de octubre del 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

INFOLAFT. Cibercrimen en Colombia: todo lo que debe saber. [Sitio Web]. [Consultado el 6 de octubre del 2021]. Disponible en: https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/

INTELEQUIA. Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad. [Sitio Web]. [Consultado el 4 de Octubre del 2021] Disponible en: https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

ISO. ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements. [Sitio Web]. [Consultado el 27 de Noviembre del 2021]. Disponible en https://www.iso.org/standard/42103.html

KIPPEO. Adoptar las Mejores Prácticas del CIS (Center For Internet Security) En Tiempos De COVID-19. [Sitio Web]. [Consultado el día 29 de Septiembre del 2022]. Disponible en: https://kippeo.com/adoptar-las-mejores-practicas-del-cis-center-for-internet-security-en-tiempos-de-covid-19/

MCAFEE. ¿Qué es un firewall? [Sitio Web]. [Consultado el 25 de Noviembre del 2021]. Disponible en: https://www.mcafee.com/es-co/antivirus/firewall.html

NETDATANETWORKS. Plan de respuesta a incidentes de ciberseguridad: lo que debes hacer en caso de un ciberataque. [Sitio Web]. [Consultado el día 29 de Septiembre del 2022]. Disponible en https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

MEJÍA LONDOÑO Cesar Augusto, RAMÍREZ GALVIS Nini Johana y RIVERA CARDONA Juan Sebastián. Vulnerabilidad, Tipos de Ataques y Formas de Mitigarlos en las Capas del Modelo OSI en las Redes de Datos de las Organizaciones. [En línea]. [2012]. Trabajo de Grado. Universidad Tecnológica de Pereira, Facultad de Ingenierías Eléctrica, Electrónica, Física y Ciencias de la Computación. PP. 30 – 32. Consultado el 27 de Noviembre del 2021. Disponible en: http://recursosbiblioteca.utp.edu.co/tesisd/textoyanexos/0058R173.pdf

MICROSOFT. [Sitio Web]. SMB de host directo a través de TCP/IP. [Consultado el día 21 de septiembre de 2022]. Disponible en: https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/direct-hosting-of-smb-over-tcpip

MINTIC. Guía de gestión de riesgos. P 17-30. [En Línea]. [2016]. [Consultado el 6 de octubre del 2021]. Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MINTIC. Guía Metodológica de Pruebas de Efectividad. P 14-15. [En Línea]. [2016]. [Consultado el 5 de octubre del 2021]. Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. P 14-29. [En Línea]. [2016]. [Consultado el 6 de octubre del 2021]. Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

OEA. Ciberseguridad Marco NIST Un abordaje integral de la Ciberseguridad. [En Línea]. [2019]. [Consultado el 5 de octubre del 2021]. Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

OJEDA-PEREZ, Jorge Eliécer; RINCON-RODRIGUEZ, Fernando; ARIAS-FLOREZ, Miguel Eugenio and DAZA-MARTINEZ, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. *Cuad. Contab.* [En Línea]. 2010, vol.11, n.28 [Consultado el 8 de octubre del 2022], pp.41-66. Disponible en:

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=en&nrm=iso . ISSN 0123-1472.

PANDASECURITY. Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. [Sitio Web]. [Consultado el 6 de octubre del 2021]. Disponible en: https://www.pandasecurity.com/es/mediacenter/seguridad/pentesting-herramienta-empresa/

PENSEMOS. Análisis de riesgo informático: 4 pasos para implementarlo. [Sitio Web]. [Consultado el 4 de octubre del 2021]. Disponible en: https://gestion.pensemos.com/analisis-de-riesgo-informatico-4-pasos-para-implementarlo

POLICÍA NACIONAL DE COLOMBIA. Normatividad sobre delitos informáticos Ley 1273 de 2009. [Sitio Web]. [Consultado el 5 de octubre del 2021]. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

QUESTIONPRO. ¿Qué es la investigación documental? [Sitio Web]. [Consultado el 6 de octubre del 2021]. Disponible en: https://www.questionpro.com/blog/es/investigacion-documental/

REDHAT. El concepto de CVE. [Sitio Web]. [Consultado el 25 de Noviembre del 2021]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

REVISTA SEGURIDAD UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. [Sitio Web]. [2018]. [Consultado el 5 de Octubre del 2021]. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

SÁNCHEZ Ávila, Miguel Ángel. Hacking Ético: Impacto en la Sociedad. [En línea]. Trabajo de Grado. Universidad Piloto de Colombia, 2019. Consultado el 10 de septiembre del 2021. Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4919/00005096.pdf?sequence=1&isAllowed=y

SANABRIA, Luis Eduardo. Conceptualización jurídica del plagio en Colombia. rev. colomb. cir. [En línea]. 2014, vol.29, n.2 [Consultado el día 8 de octubre del 2022], pp.88-97. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2011-75822014000200002&lng=en&nrm=iso. ISSN 2011-7582.

SOFTWARELAB. ¿Qué es un firewall? La definición y los 5 tipos principales. [Sitio Web]. [Consultado el 4 de octubre del 2021]. Disponible en: https://softwarelab.org/es/que-es-un-firewall/

TECNOZERO. Tipos de firewall. [Sitio Web]. [Consultado el 5 de octubre del 2021]. Disponible en: https://www.tecnozero.com/firewall/tipos-de-firewall/

UNIR. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? [Sitio Web]. [Consultado el 4 de Octubre del 2021] Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

VALORDATA. El Marco de Ciberseguridad del NIST y su área recuperación. [Sitio Web]. [Consultado el 5 de octubre del 2021]. Disponible en: https://www.valoradata.com/blog/el-marco-de-ciberseguridad-del-nist-y-su-area-recuperacion/

WIKIPEDIA. Análisis de riesgo informático [Sitio Web]. [Consultado el 5 de octubre del 2021] Disponible en: https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

WIKIPEDIA. Símbolo del sistema de Windows [Sitio Web]. [Consultado el día 20 de septiembre del 2022]. Disponible en: https://es.wikipedia.org/wiki/S%C3%ADmbolo_del_sistema_de_Windows

WILHELM, Thomas. Professional Penetration Testing, 2nd Edition, Estados Unidos: Syngress Press. ISBN-13: 978-1-59749-993-4, ISBN-10: 1-59749-993-5

11 ANEXOS

ANEXO A. Caso de estudio

Situación problema: Análisis Red team

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo en la dependencia. La información con la que cuenta usted como experto de ciberseguridad es la siguiente: Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2022) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Para agilizar el proceso de investigación Hackers Security facilitará los dos escenarios controlados idénticos al de los equipos de cómputo sospechosos y un escenario controlado con un S.O orientado al testeto de seguridad para que realice el trabajo de investigación sin alterar la infraestructura de producción de la organización; usted como parte de un equipo Red team deben analizar la información suministrada, y seguir los pasos para encontrar si existe un fallo de seguridad a nivel de S.O, validar que vulnerabilidad podría encontrar y posterior a ello buscar el método de explotación por medio de algún framework o exploit. Hackers Security le recuerda que no tienen conocimiento cuál de los dos equipos de cómputo es el que está generando la fuga de información, y mencionan también, que en ocasiones uno de esos dos equipos de cómputo suele mostrar pantalla azul error de Windows de una manera constante. Recuerde que su misión es confirmar y evidenciar las posibles explotaciones paso a paso, el archivo que contiene la información que han estado extrayendo tiene el nombre de "winse20w0.exe", si usted logra acceder al equipo de cómputo de manera intrusiva deberá encontrar el archivo mencionado y tomar pantalla de la información allí

generada, y además validar por qué uno de esos equipos de cómputo suele mostrar pantalla azul error de windows. Si obtiene esta información podremos decir: BIENVENIDO AL RED TEAM HACKERS SECURITY, este mensaje se destruirá en 3, 2, 1, ... kernel panic....

Situación problema: Análisis Blue team

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

ANEXO B. Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y HACKERS SECURITY

Por la parte reveladora
Nombre: Hackers Security
Dirección: EE.UU
Teléfono: 1100011100
E-mail: Info@Thewhitehousesecurity.com

Por la parte receptora de la información
Nombre: Nombre estudiante
Dirección:
Teléfono:
E-mail:

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

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

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

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

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

Primera. Objeto: en virtud del presente **acuerdo de**

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

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

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

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos". **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

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

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

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

De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Hackers Security, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

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

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

5. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

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

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

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

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

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto

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

Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo**. En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Hackers Security.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

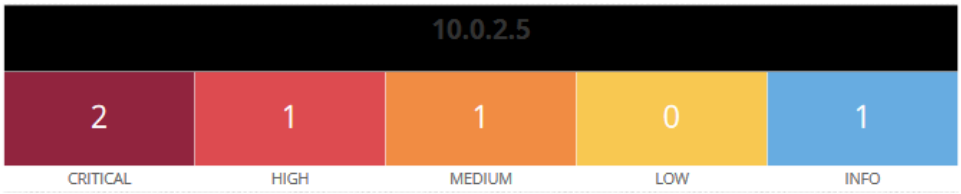
Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

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

Como Parte Receptora:	Por la parte reveladora:
_____	_____
Nombre del estudiante. Estudiante UNAD. C.C. No. de	Nombre Gerente de la empresa Hackers Security C.C. No. de

ANEXO C. Reporte Herramienta *Nessus*

Vulnerabilities by Host



Scan Information

Start time:	Thu Sep 22 15:25:09 2022
End time:	Thu Sep 22 15:30:45 2022

Host Information

Netbios Name:	WIN7
IP:	10.0.2.5
MAC Address:	08:00:27:E9:5A:99
OS:	Microsoft Windows 7 Home

Vulnerabilities

53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Synopsis

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

See Also

https://www.nessus.org/u?361871b1

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

I

References

BID	47242
CVE	CVE-2011-0657
MSKB	2509553
XREF	IAVA:2011-A-0039-S
XREF	MSFT:MS11-030

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2011/04/21, Modified: 2020/08/05

Plugin Output

udp/5355/llmnr

108797 - Unsupported Windows OS (remote)

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF IAVA:0001-A-0501

Plugin Information

Published: 2018/04/03, Modified: 2022/07/05

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:

Microsoft Windows 7 Home
```

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

http://www.nessus.org/u?68fc8eff

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?065561d0

http://www.nessus.org/u?d9f569cf

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

http://www.nessus.org/u?b9d9ebf9

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions.

SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.1 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CISA-KNOWN-EXPLOITED:2022/08/10
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CISA-KNOWN-EXPLOITED:2022/04/27
XREF	CISA-KNOWN-EXPLOITED:2022/06/14

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/03/20, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Sent:
00000054ff534d4225000000001803c800000000000000000000000000876ee0008000110000000
00ffffffff0000000000000000000000540000054000200230000001100005c00500049005000
45005c0000000000

Received:
ff534d4225050200c09803c8000000000000000000000000000876ee00080001000000
```

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

http://www.nessus.org/u?52ade1e9

http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090
MSKB	3147461
MSKB	3147458
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information

Published: 2016/04/13, Modified: 2019/07/23

Plugin Output

tcp/49157/dce-rpc

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2022/09/19

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```