

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

DIANA MARCELA CARDONA CANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
CIUDAD  
2021

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

Proyecto de Grado – Seminario especializado presentado para optar por el título de  
ESPECIALISTA EN SEGURIDAD INFORMATICA

Diana Marcela Cardona Cano

Tutor de Curso:

Jhon Freddy Quintero Tamayo

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

CIUDAD

2021

## RESUMEN

Las amenazas informáticas, riesgos de SI y metodologías, han evolucionado desde los últimos 50 años conforme a la necesidad y exigencia de cada época. A partir de la década de los 70, se vislumbró la propagación de malware entre artefactos sin mayor impacto, hasta lo que vemos hoy en día, lo cual desencadena riesgos importantes e ineludibles de tratar por su importancia a raíz de su consecuencia.

El problema planteado en el presente documento intenta mostrar la problemática actual, la cual se deriva de amenazas informáticas surgidas a partir del active ocasionado por la evolución y cambios tecnológicos asentados especialmente, en el actual siglo.

La justificación frente al argumento de establecer métodos técnicos y estratégicos para que una organización pueda controlar las amenazas que debe enfrentar su negocio, es una iniciativa que se intenta mostrar mediante el planteamiento del presente documento, por medio de la adopción de buenas prácticas entre las cuales, se considera la conformación de equipos especializados tales como aquellos denominados Red Team y Blue Team.

Esta consideración, trae consigo técnicas, procedimientos y métodos que hacen parte de las buenas prácticas empleadas por los grupos especializados en mención.

Dichas prácticas están apoyadas en metodologías para la identificación de vulnerabilidades técnicas sobre los sistemas informáticos, desde un proceso de monitoreo y habilidades por parte de los profesionales quienes lo realizan, apoyados en estrategias que involucran un rol de atacante para evidenciar anomalías y deficiencias antes que los ciber atacantes con propósitos delictivos, puedan descubrir estas brechas de seguridad las cuales deberían ser evidenciadas y controladas con antelación, por parte de una organización si considera protocolos de seguridad preventiva.

Igualmente, estas prácticas mencionadas, consideran métodos para la implementación de planes que tengan como objetivo, subsanar vulnerabilidades e igualmente, procedimientos para contrarrestar amenazas en caso de que los riesgos de seguridad se vean materializados.

**PALABRAS CLAVE:** Amenazas Informáticas, Análisis de vulnerabilidades, Blue Team, Métodos de seguridad, Procedimientos de seguridad, Red Team.

## **ABSTRACT**

Computer threats, its risks and methodologies have evolved over the last 50 years according to the need and demand of each era. Starting in the 70s, the spread of malware between artifacts was glimpsed without major impact, up to what we see today, which triggers important and unavoidable risks to treat due to their importance as a result of their consequence.

The problem posed in this document tries to show the current problem, which is derived from computer threats arising from the active caused by evolution and technological changes settled especially in the current century.

The justification against the argument of establishing technical and strategic methods so that an organization can control the threats that its business must face, is an initiative that is tried to show through the approach of this document, through the adoption of good practices among which The formation of specialized teams such as those called Red Team and Blue Team is considered.

This consideration brings with it techniques, procedures and methods that are part of the good practices used by the specialized groups in question.

These practices are supported by methodologies for the identification of technical vulnerabilities on computer systems, from a monitoring process and skills by the professionals who carry it out, supported by strategies that involve an attacker role to reveal anomalies and deficiencies before the cyber attackers with criminal purposes can discover these security breaches which should be evidenced and controlled in advance, by an organization if it considers preventive security protocols.

Likewise, these aforementioned practices consider methods for the implementation of plans that aim to correct vulnerabilities and also, procedures to counter threats in the event that security risks materialize.

**KEY WORDS:** Computer Threats, Vulnerability Analysis, Blue Team, Security Methods, Security Procedures, Red Team.

## GLOSARIO

**ACTIVOS DE INFORMACIÓN:** Dispositivos tangibles e intangibles dentro de los cuales, se almacenan o procesan información.

**ANTIVIRUS:** Conglomerado de programas que operan para desintegrar un virus informático, identificado dentro de un sistema de información (Pc, redes, servidores etc.).

**ATAQUES INFORMATICOS:** Son procedimientos ejecutados con intención de desestabilizar, suprimir, y/o de acceder de manera no autorizada, un sistema informático.

**BLUE TEAM:** Grupos de seguridad que tienen por objetivo, prevenir, corregir fallas y vulnerabilidades informáticas halladas en los sistemas informáticos. Estos grupos, trabajan en asocio con los equipos denominados Blue Red.

**DELITO INFORMÁTICO:** ES una acción o procedimiento realizado al margen de la ley, el cual tiene por propósito irrumpir en los sistemas informáticos de manera no autorizada para conseguir fines lucrativos o, sabotaje sobre dichos sistemas.

**INCIDENTES DE SEGURIDAD:** Acceso o intento de acceso sobre los sistemas informáticos mediante lo cual, trasgreden o intentan trasgredir la información desde su confidencialidad, disponibilidad o integridad.

**MALWARE:** ES un término genérico, el cual es asignado a cualquier programa informático, que tenga por finalidad destruir o secuestrar los datos para un determinado fin. Igualmente, afecta la disponibilidad de los sistemas de información desde el hardware o software.

**RED TEAM:** Equipo de seguridad, encargado de inspeccionar los sistemas de

información los cuales se encuentran bajo su responsabilidad, con el fin de identificar posibles vulnerabilidades técnicas apoyado, en herramientas de hacker, las cuales son usadas para hallar vulnerabilidades técnicas antes, de que los atacantes puedan descubrirlas.

**RIESGOS DE SEGURIDAD:** Probabilidad de ser materializada una amenaza informática, la cual trae por consecuencia, pérdida de imagen, dinero, reputación y en algunos casos, el cierre parcial de una organización.



## CONTENIDO

<b>INTRODUCCIÓN .....</b>	<b>2</b>
<b>1. DEFINICIÓN DEL PROBLEMA .....</b>	<b>3</b>
1.1 FORMULACIÓN DEL PROBLEMA .....	3
<b>2. JUSTIFICACIÓN.....</b>	<b>5</b>
<b>3. OBJETIVOS.....</b>	<b>6</b>
3.1 OBJETIVO GENERAL .....	6
3.2 OBJETIVOS ESPECÍFICOS .....	6
<b>4. MARCO REFERENCIAL.....</b>	<b>7</b>
4.1 MARCO TEÓRICO .....	7
<b>5. METODOLOGIA .....</b>	<b>14</b>
<b>6. DESARROLLO DEL INFORME .....</b>	<b>15</b>
6.1 CONFIGURACIÓN DEL BANCO DE TRABAJO.....	15
6.2 PROCESO DE PENT TESTING.....	19
6.3 CONTENCIÓN DE ATAQUES INFORMÁTICOS.....	28
6.4 MEDIDAS DE HARDENIZACIÓN.....	34
<b>7. LINK VIDEO DE SUSTENTACIÓN.....</b>	<b>36</b>
<b>8. CONCLUSIONES .....</b>	<b>37</b>
<b>9. RECOMENDACIONES .....</b>	<b>39</b>
<b>BIBLIOGRAFÍA .....</b>	<b>40</b>

## LISTA DE TABLAS

<b>Figura 1.</b>	<b>Instalación Virtual Box .....</b>	<b>15</b>
<b>Figura 2.</b>	<b>Ambiente Virtual.....</b>	<b>18</b>
<b>Figura 3.</b>	<b>Sistema Operativo Kali Linux.....</b>	<b>18</b>
<b>Figura 4.</b>	<b>Ejecución Comando Nmap.....</b>	<b>19</b>
<b>Figura 5.</b>	<b>Archivo Plano con Vulnerabilidades Técnicas.....</b>	<b>20</b>
<b>Figura 6.</b>	<b>Ejecución Herramienta LEGION.....</b>	<b>23</b>
<b>Figura 7.</b>	<b>Ejecución Herramienta Metasploit.....</b>	<b>26</b>
<b>Figura 8.</b>	<b>Visor de Eventos de Windows.....</b>	<b>29</b>
<b>Figura 9.</b>	<b>Ejecución Comando Netstat.....</b>	<b>30</b>

## INTRODUCCIÓN

La seguridad de la información en la actualidad, no ha sido una práctica dinámica ni mucho menos evolutiva, posiblemente, esto se deba a que no reconocemos aun la transformación y el valor que han ido tomando los datos en este nuevo siglo o tal vez, que la mentalidad de muchas personas especialmente la de los empresarios, sigue ceñida a las arcaicas costumbres generadas desde tiempos pasados, por lo que se sigue gestionando, actividades poco planificadas que inciden en resultados que determinan en la mayoría, hechos reactivos ante un riesgo de seguridad materializado, a causa de una ciber amenaza.

A falta de conciencia ante esta nueva realidad, se resta importancia de invertir y constituir procedimientos, que hacen parte de planes estructurados y adheridos a los riesgos de seguridad. Estos planes no considerados dentro de la estrategia de la compañía, amplia la brecha de seguridad sobre los diversos activos informáticos custodiados por las organizaciones.

El escenario problemático planteado en el presente documento intenta establecer la realidad frente a la situación de referencia, justificando el interés de argumentar metodologías, herramientas y técnicas halladas dentro del marco de gestión empleado como parte de una buena práctica adoptada, por la constitución de equipos de trabajo conformado por profesionales, que establecen procesos tanto defensivos y ofensivos, para cubrir los activos informáticos de amenazas latentes.

# 1 DEFINICIÓN DEL PROBLEMA

## 1.1 FORMULACIÓN DEL PROBLEMA

¿Qué tipo de estrategias podrían tener en cuenta los equipos Blue Team apoyados en prácticas de equipos red Team en la implementación de mejores controles preventivos dentro de las organizaciones, para mitigar los diversos riesgos a partir de las amenazas informáticas existentes?

Ante la situación problemática actual, desafiada desde la perspectiva acaecida por los cambios tecnológicos y evolutivos los cuales, han surgido de manera acelerada y emergente en estos últimos años, las organizaciones, entidades y diversos grupos sociales, no se encuentran listos para enfrentar amenazas cibernéticas a falta de procedimientos estandarizados, metodologías y prácticas eficientes, para anteponerse a escenarios complejos a los cuales se vean enfrentados sus activos informáticos. Pero, es innegable que su mayor problema es el entendimiento frente a lo inevitable de involucrar como parte de una buena práctica, las medidas preventivas que son precisas para afrontar diversas amenazas y mantener sus riesgos de seguridad, en un nivel aceptable y controlado.

Por lo anterior, la falta de conciencia ante lo expuesto exige que se conozcan las contramedidas para asegurar los activos informáticos, tales como, la constitución de grupos de seguridad dedicados a preservar la protección de estos sistemas de información (Red Team y Blue Team), estándares y buenas prácticas (Normas ISO, COBIT, ITIL), procedimientos de Pent Testing, herramientas de monitoreo y escáner, entre otros. Lo anterior prevalece, para ser constituido como parte de una opción, que garantice el mantener el riesgo de seguridad controlado, ante la operación de sus sistemas informáticos.

Una vez dicho lo anterior, las organizaciones poseen un faltante con relación a la inversión de estructuras y recursos que apoye los procesos misionales, estratégicos

y operativos, en la ejecución eficiente de sus actividades sin que a estas se antepongan, aspectos relacionados con amenazas y riesgos de seguridad informática.

## 2 JUSTIFICACIÓN

El trabajo de grado planteado bajo la modalidad de “Seminario Especializado”, se enfocará en diversos aspectos que involucran como parte de una buena práctica, la constitución de equipos de seguridad tales como los Red Team y Blue Team. Dichos aspectos, estarán enmarcados como primera medida, en la manera de proceder de cada uno de los equipos, el tipo de directrices que los rige tales como normas, legislación y estándares. Igualmente, en herramientas tecnológicas que soportan las actividades ejercidas para inspeccionar los sistemas de información para el descubrimiento de vulnerabilidades y metodologías adoptadas para el uso y aplicación de procedimientos definidos que contribuyan al resguardo y aseguramiento de los datos.

La consulta documental se realizará con el propósito de afianzar conocimientos acerca de los aspectos mencionados para emitir ante la universidad UNAD, una vez se haya concretado el seminario, las recomendaciones desde una posición personal y crítica, las cuales serán impartidas desde un escenario controlado mediante los laboratorios prácticos del curso a realizar bajo la modalidad de grado en mención.

Los beneficios otorgados mediante la puesta en práctica ante un evento simulado dentro del marco del seminario, proporcionará un documento de guía el cual podrá ser consultado con posterioridad por parte de los estudiantes de la especialización de “Seguridad Informática”, con el fin de ser empleado como parte de una fuente de conocimiento que contribuya en la investigación de temas, en referencia a la importancia de constituir equipos que fomente la seguridad sobre sistemas de información e igualmente, en recomendaciones impartidas ante eventos de amenazas y riesgos de seguridad reales.

## **3 OBJETIVOS**

### **3.1 OBJETIVO GENERAL**

Establecer mediante un informe técnico, recomendaciones acerca de estrategias de contención empleadas por equipos de Blue Team, con base a los procedimientos practicados por un equipo Red Team para, determinar la importancia de instituir dentro de una organización, buenas prácticas en relación con la constitución de grupos de seguridad.

### **3.2 OBJETIVOS ESPECÍFICOS**

3.2.1 Implementar un banco de trabajo para simular una situación real que permitirá establecer el informe técnico.

3.2.2 Establecer el proceso de Pent Testing desarrollado por grupos de Red Team.

3.2.3 Describir las fases de contención de ataques establecido por grupos de Blue Team.

3.2.4 Plantear las diferentes medidas de hardenización empleados por grupos Blue Team.

## **4 MARCO REFERENCIAL**

### **4.1 MARCO TEÓRICO**

La seguridad informática en referencia a los diversos tipos de ataques y a las contramedidas empleadas en proporción a los cambios que han surgido en los últimos años, ha demarcado significativamente los procedimientos, tipo de herramientas y metodologías diversas las cuales son empleadas, como parte de los planes para asegurar los activos de información ante amenazas y riesgos de seguridad. Las amenazas han evolucionado paralelamente a las técnicas y contramedidas empleadas para garantizar control sobre la posible pérdida de integridad, confidencialidad y disponibilidad de la información.

Los controles empleados para asegurar la información en todos sus aspectos se han transformado de acuerdo con una necesidad que, sin lugar a duda, a dependido de la evolución vertiginosa a causa de los avances de la tecnología que han surgido desde el inicio del presente siglo.

Hablar de seguridad de la información en la década de los 70, simbolizaba controles completamente diferentes a lo que en la actualidad se podrían considerar siendo estos, obsoletos para la necesidad que exige, sea contemplada sobre un activo de información en el presente siglo.

En la década de los 80, se dio a conocer los primeros malwares, estos, surgieron a partir del uso de computadoras personales. Aunque su distribución no era tan masiva por la arquitectura tecnológica empleada en ese entonces, el malware se portaba en los diferentes medios de almacenamiento los cuales podrían llevar el virus en dichos artefactos tales como disquetes y cd. La contramedida empleada a partir de aquellas amenazas absolutas que se dieron en ese entonces fue la originación de los antivirus.



En la década de los 90, se instauró una nueva amenaza con el uso del internet concediéndose de esta manera, un hecho de modalidad de hurto y la oportunidad de optar por efectuar ciberataques para tener como objetivo, el acceso no autorizado a la información y/o datos de tipo sensible.

A partir del siglo XXI, se dinamizó la explotación de vulnerabilidades técnicas halladas en los diversos sistemas de información. De allí, la exploración por parte de individuos que se especializaron en descubrir las falencias halladas en los sistemas informáticos revelando mediante las cuales, la oportunidad de hacer uso de dichas falencias para la captación inapropiado de la información.

Conforme iba evolucionando las amenazas, riesgos y contramedidas, se tecnificaba y sofisticaba los ataques informáticos.

Los ataques de SI actuales, exigen una preparación y planificación mayormente elaborada por lo que en la actualidad existen, organizaciones dedicadas a analizar y establecer procedimientos para llevar a cabo este tipo de acometimientos. (Hard2bit CyberSecurity,2019).

### **¿Están las organizaciones preparadas ante los ataques informáticos?**

Estudios realizados por entidades confiables “Ejemplo: EY -antes Ernst&Young”, demuestran que las organizaciones de este siglo no poseen entendimiento ni mucho menos, un enfoque acerca de los diferentes riesgos cibernéticos. Parte de los presupuestos diseñados por las organizaciones contemporáneas, no discurren en planes para resguardar los riesgos de seguridad como parte de una inversión más que un gasto, ignorando que, ante un evento o incidente tecnológico, este puede poseer grandes consecuencias entre las cuales, podría originarse la no continuidad de su negocio.

La fuente del estudio por parte de la entidad en mención demostró que solo un 43% de las organizaciones encuestadas contemplaban presupuesto para poner en marcha, los planes que se requirieran en caso de surgir algún tipo de incidente de seguridad. El 46% restante, no pensaron en absoluto, en acciones ni mucho menos, recurso para

ser encauzadas dichas acciones a posibles operaciones que fueran pertinentes en caso, de que se presentara algún tipo de evento que amenazara con la no continuidad del servicio.

Lo anterior es justificado por la falta de dinero para ser empleado y redireccionado a este tipo de inversiones las cuales, carecen de argumentos y credibilidad a la hora de ser justificadas frente a la implementación de metodologías, estándares, buenas prácticas, equipos tecnológicos y personal especializado que contribuyan a los procedimientos preventivos para evitar sucesos de envergadura de tipo crítica.

Estos análisis demuestran falencias frente al entendimiento, pero, sobre todo, la concientización por parte de los directivos acerca de las amenazas y riesgos complejos. Solo el 4 % de las organizaciones tomadas como muestra del análisis, acentuaron que poseían un grupo dedicado a la inteligencia de amenazas con personal dedicado, a la identificación de sucesos riesgosos.

Es importante tener en cuenta, que las amenazas informáticas son evolutivas y cada día más tecnificadas. Las directrices empleadas frente a la idealización en aspectos de seguridad sobre los activos informáticos de una organización, debe convertirse en lineamientos para la operación segura de sistemas informáticos, haciendo parte de dichas directrices, recomendaciones para combatir la ciberseguridad. Parte de las recomendaciones, podrían constar de lo siguiente:

Prevenir las amenazas informáticas mediante el monitoreo y conformación de equipos especializados (Red Team/Blue Team).

Entender el entorno de las amenazas con el propósito de establecer los diversos planes de seguridad, ajustados a la necesidad puntual de la organización para que se contrarreste de manera eficiente, los riesgos que puedan ocasionar dichas amenazas.

Reconocer el valor de los activos informáticos desde la importancia de la disponibilidad, confidencialidad e integridad de los datos resguardados en cada activo.

Estructurar procedimientos para la gestión de incidentes de seguridad mediante los cuales, permitan hacer gestión correctiva y planificación efectiva. (Ernst&Young, 2020).

## **Catalogación de delitos informáticos.**

Existe actualmente legislación aplicable, según sea catalogado el delito informático. Para esto, se emplea una clasificación de delitos la cual es considerada a la hora de establecer penalidades y faltas disciplinarias. Entre la clasificación de delitos, se encuentra aquellos denominados “Delitos contra la seguridad de los datos (confidencialidad, integridad y disponibilidad de la información), estos consisten en aquellos sucesos a lo que se le atribuyen aquellos casos en donde existe un evento de ingreso o interceptación de la información de manera ilícita. Igualmente, se encuentra dentro del marco explicativo aquellos eventos relacionados con daños provocados de manera conciente, a los sistemas informáticos. A este consolidado, se le suma aquellos delitos acerca de fraudes informáticos los cuales consisten, en fraudes que conllevan a procedimientos de falsificación que tienen como consecuencia, el borrado o alteración de aquella información accedida de manera no autorizada. Los delitos de contenido relacionado con la pornografía infantil y los delitos de propiedad intelectual, son otra clasificación a considerar. Seguidamente, tenemos aquellos delitos catalogados como robo de servicio los cuales consisten en aquellas acciones que intentan robar tiempo y acceso a aquellos servicios que no se encuentran pactados contractualmente entre un proveedor y el individuo protagonista del suceso. Finalmente, se tiene catalogado un sexto delito informático en relación a la fuga de datos y la reproducción no autorizada de paquetes de software. (Universidad Nacional Abierta y a Distancia, 2019).

## **Normativa establecida que rige actualmente la Seguridad de la Información en Colombia.**

Actualmente existen estándares y normas legales que rigen la seguridad de la información de manera controlada y normalizada. La evolución de la tecnología ha demandado igualmente, un avance a lo que se refiere las amenazas cibernéticas y, las directrices las cuales, al ser implementadas, gestionan correctamente los riesgos corporativos.

Estándares internacionales reconocidos como normas ISO (27001, 9001, 27005) COBIT, ITL, al igual que legislación en materia de protección de la información y datos,

contribuyen a que la seguridad sobre los datos formales e informales, se encuentren protegidos ante cualquier evento que amenace con alterar su integridad, confidencialidad y disponibilidad.

### **Norma ISO 27001**

La norma ISO 27001 contiene 7 requisitos certificables y un anexo que describe 114 controles los cuales, se encuentran distribuidos en 14 dominios generales. La norma está fundada en la metodología PHVA y establece un enfoque basado en procesos y riesgos por lo que, mediante su fase de planeación establece como parte de un requisito, la necesidad de identificar diversos riesgos de seguridad de la información para ser tratados de manera preventiva y así, evitar posibles incidentes de seguridad sobre los activos informáticos.

El anexo de esta norma contiene tantos controles técnicos, de recurso humano y administrativos lo que permite mediante su implementación, gestionar debidamente los activos de información por medio de su identificación y procedimientos bien estructurados que establezcan condiciones para asegurar su custodia. La debida gestión y definición de los controles de acceso digitales para resguardar aplicaciones y sistemas informáticos. Las directrices para establecer políticas criptográficas y la definición frente a la gestión de llaves, la seguridad física y del entorno e igualmente, la de los equipos.

Estos controles también contienen lineamientos para gestionar la operación del negocio mediante procedimientos que permitan efectuar y garantizar que el recurso informático tipo crítico y fundado en el CORE del negocio, es inspeccionado por medio de la gestión de la capacidad y los cambios.

Otros controles que aportan a la gestión de la operación y que son contemplados dentro de la norma, son aquellos que se encuentran enfocados a las buenas prácticas frente al respaldo de la información, las auditorías a

los sistemas de información y el análisis de vulnerabilidades técnicas para la identificación de brechas de seguridad.

Por último, se determina controles para establecer la seguridad de las comunicaciones, las reglas para determinar la seguridad dentro del ciclo de vida de desarrollo desde su análisis hasta la puesta en operación de aquellas aplicaciones que son construidas, la gestión de los proveedores tipo críticos, la gestión de incidentes de seguridad, la continuidad del negocio y el cumplimiento de normativas y/o legislación tal como el habeas data y la propiedad intelectual.

Esta norma posee un alcance muy amplio por lo que puede ser implementada en diferentes tipos de negocio no importando su tamaño y/o misión. Tanto los requisitos y controles deben ser implementados de manera obligatoria, pero, puede hallarse no aplicable algunos de estos por lo que deberá ser muy bien argumentada la exoneración de alguna de estas cláusulas. (ISO27001, 2020).

### **Ley 1581 de 2012**

La ley 1581 de 2012 es una norma colombiana que rige políticas para el cumplimiento en materia de resguardo de información tipo personal. Estas políticas son acordes al derecho constitucional denominado “Habeas Data”, el cual poseen todos los ciudadanos y les reconoce actividades tales como el conocer, actualizar, rectificar información tipo personal que haya sido recolectada y administrada por terceros. (Ley1581de2012, 2020).

### **Ley 1273 2009**

Esta ley nacional establece el alcance frente a los posibles delitos que podrían acaecer bajo el marco de gestión de la información tipo formal (Tecnológica). Establece así mismo, las penalidades y sanciones las Cuales son representadas en penas de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa, de 100 a 1000 salarios mínimos legales mensuales vigentes.

Algunos de estos delitos podrían ser representados, por ejemplo, en:

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación
- Violación de datos personales, entre otros. (MINTIC,2020).

## 5 METODOLOGIA

La metodología a desarrollar frente a la elaboración del informe técnico se realizará en referencia a las siguientes fases:

- Montaje del laboratorio practico.
- Actuación ética y legal.
- Ejecución pruebas de intrusión.
- Contención de ataques informáticos.

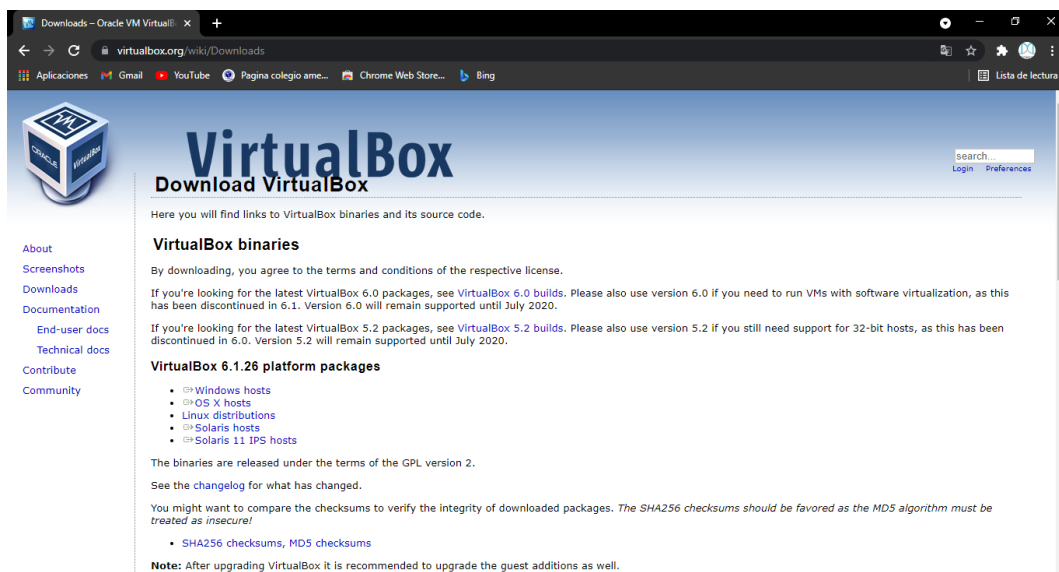
## 6 DESARROLLO DEL INFORME

### 6.1 CONFIGURACIÓN DEL BANCO DE TRABAJO PARA DESARROLLAR PRÁCTICA.

Para la presente actividad, se dará a conocer la implementación y posterior configuración del banco de trabajo el cual será usado para el desarrollo técnico del seminario especializado:

*Se procedió a descargar desde la página oficial de VirtualBox, el software correspondiente para ser instalado en el host donde operará la máquina virtual.*

**Figura 1. Instalación Virtual Box**

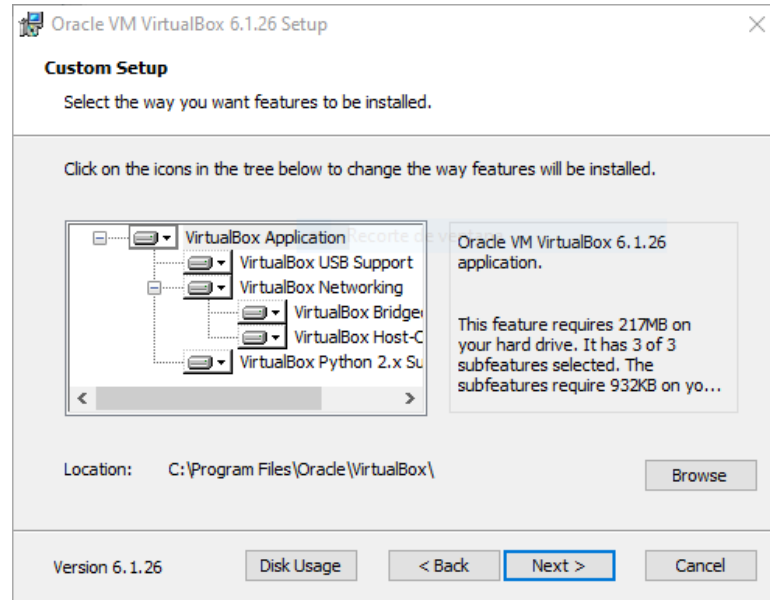


**Fuente: Propia**



Se estableció la ruta de instalación de la máquina virtual.

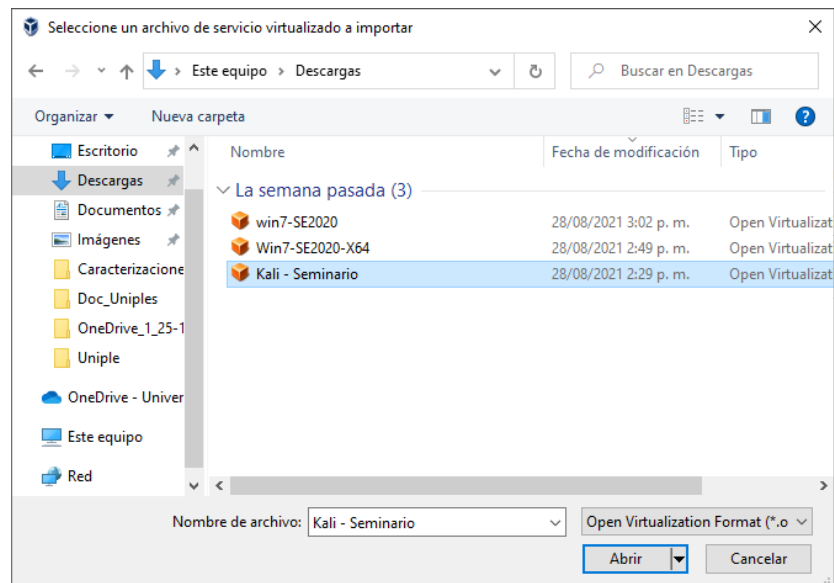
**Figura 1. Instalación Virtual Box**



**Fuente: Propia**

Se procedió a importar las imágenes correspondientes para proceder con la instalación de los sistemas operativos sobre la máquina virtual VB (Windows 7 y Kali Linux).

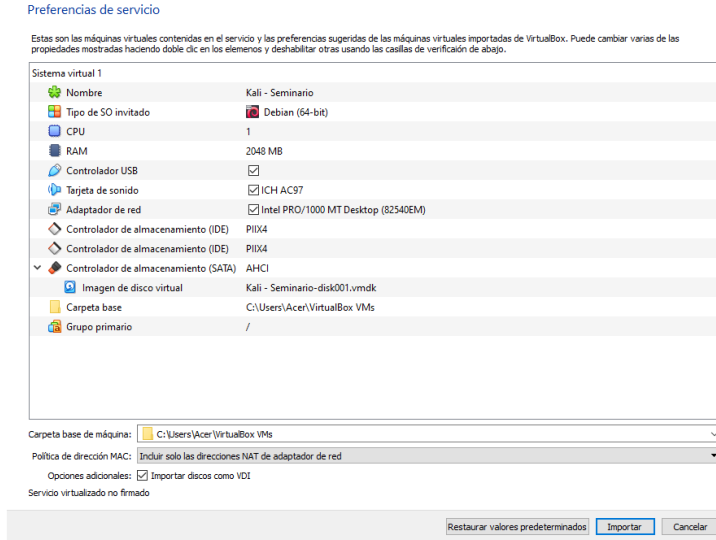
**Figura 1. Instalación Virtual Box**



**Fuente: Propia**

Características preconfiguradas dentro del sistema operativo Kali Linux.

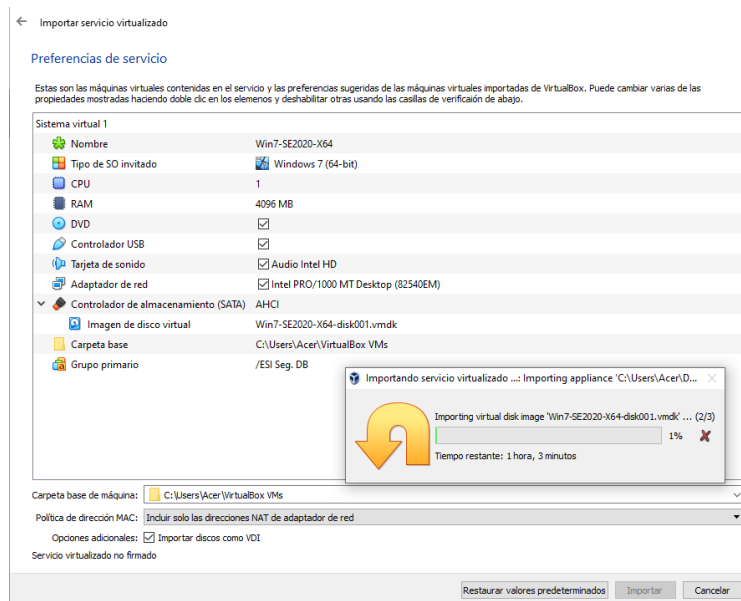
**Figura 1. Instalación Virtual Box**



**Fuente: Propia**

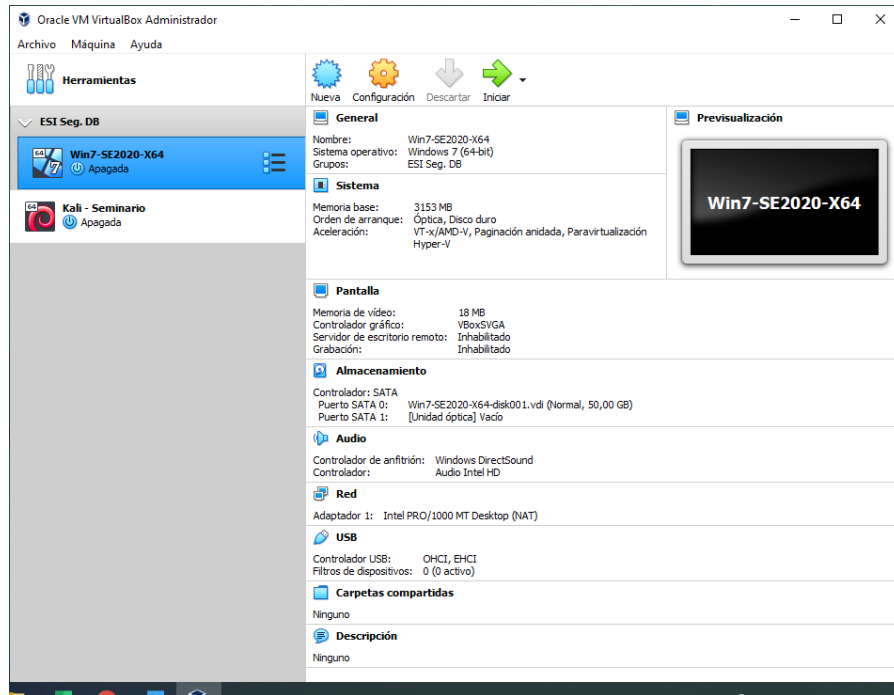
Características preconfiguradas dentro del sistema operativo Windows 7.

**Figura 1. Instalación Virtual Box**



**Fuente: Propia**

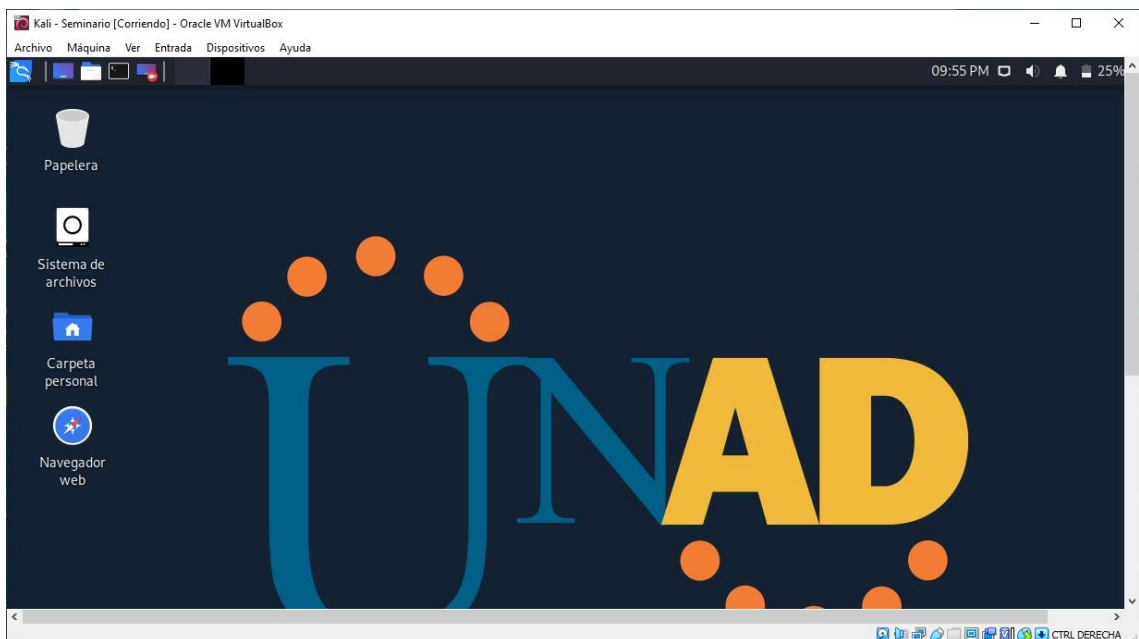
**Figura 2. Ambiente Virtual**



**Fuente: Propia**

*Se procede a ingresar a cada uno de los S.O. mediante el usuario y credencial (estudiante – unad2020)*

**Figura 3. Sistema Operativo Kali Linux**



**Fuente: Propia**

## 6.2 PROCESO DE PENT TESTING.

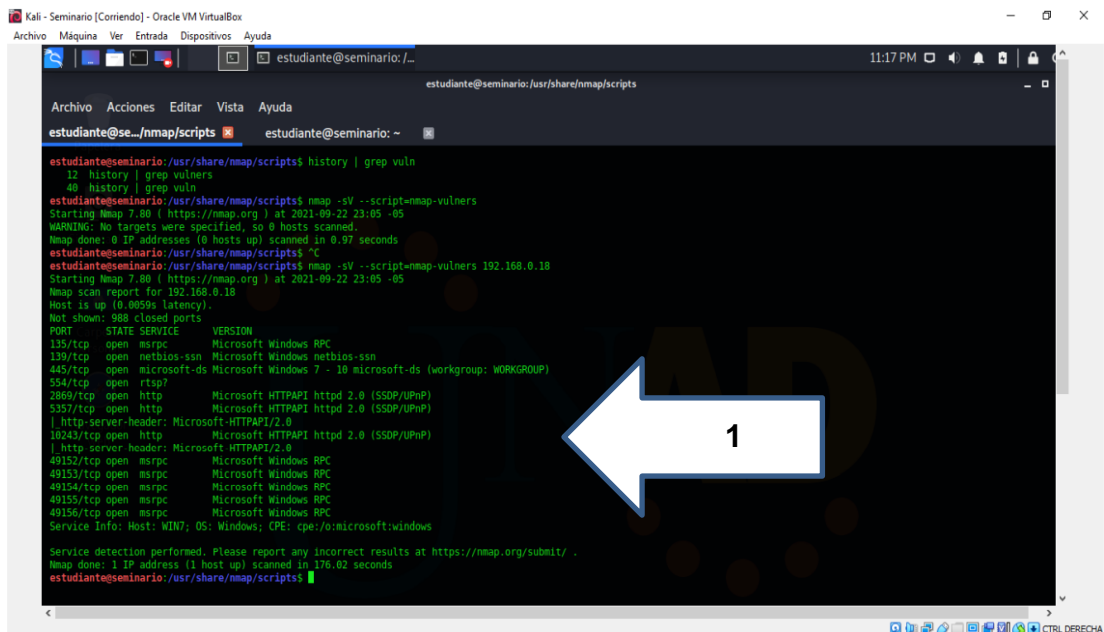
### 6.2.1 Fase de Recolección

#### Detalle de las pruebas desarrolladas:

Considerando la fase de “Recolección de información” para identificar las vulnerabilidades técnicas, se ilustra a continuación mediante imágenes representativas:

IP maquina afectada: **192.168.0.18**

**Figura 4. Ejecución comando Nmap**



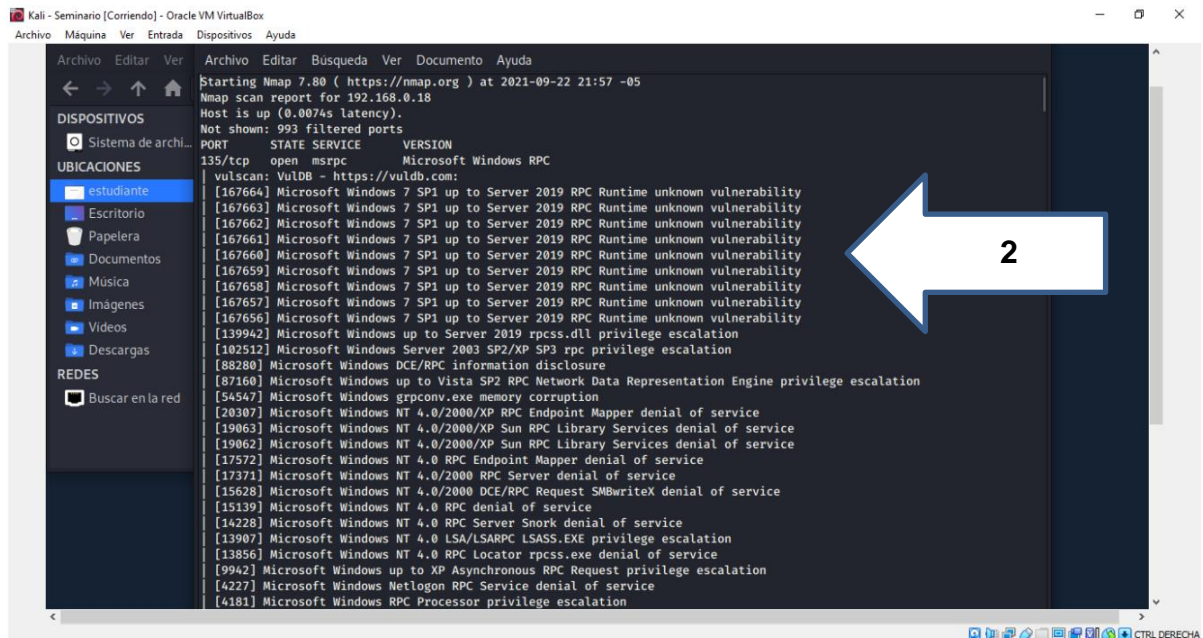
```
estudiante@seminario: /usr/share/nmap/scripts$ history | grep vuln
12 history | grep vulners
40 history | grep vuln
estudiante@seminario: /usr/share/nmap/scripts$ nmap -sV --script=nmap-vulners
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-22 23:05 -05
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.97 seconds
estudiante@seminario: /usr/share/nmap/scripts$ ^C
estudiante@seminario: /usr/share/nmap/scripts$ nmap -sV --script=nmap-vulners 192.168.0.18
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-22 23:05 -05
Nmap scan report for 192.168.0.18
Host is up (0.0099s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtp?             Microsoft RTP
2869/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/I/PHP)
5357/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/I/PHP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/I/PHP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49156/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 176.02 seconds
estudiante@seminario: /usr/share/nmap/scripts$
```

**Fuente Propia**

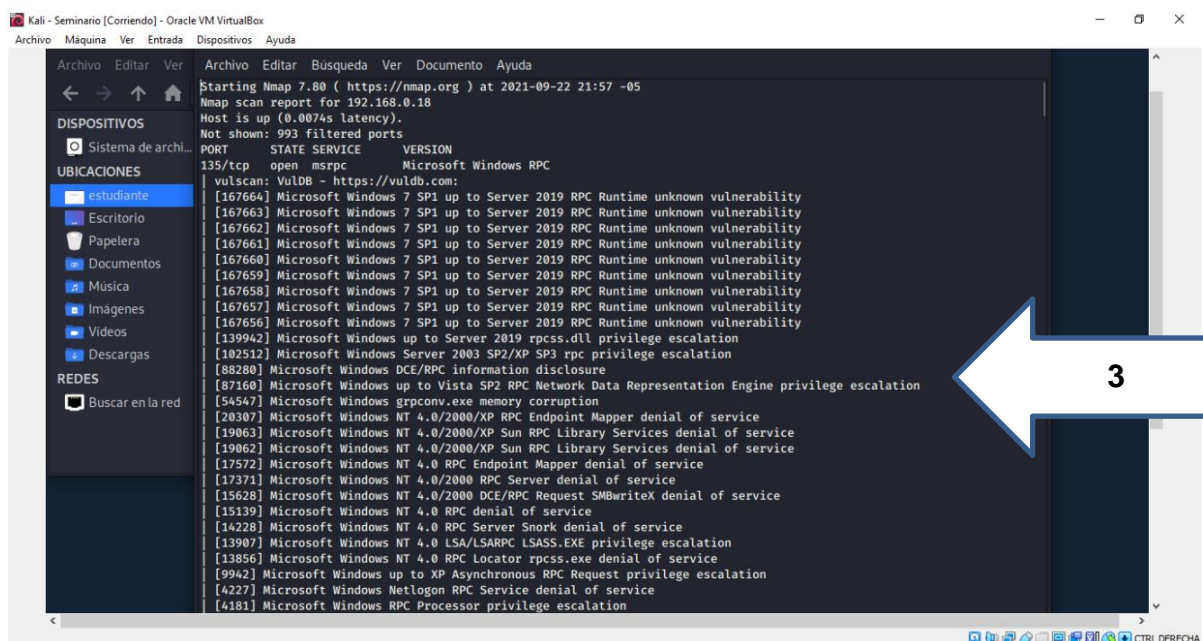
Se exporta información a un archivo plano, y se denota varios aspectos a considerar por parte del analista.

**Figura 5. Archivo plano con vulnerabilidades técnicas**



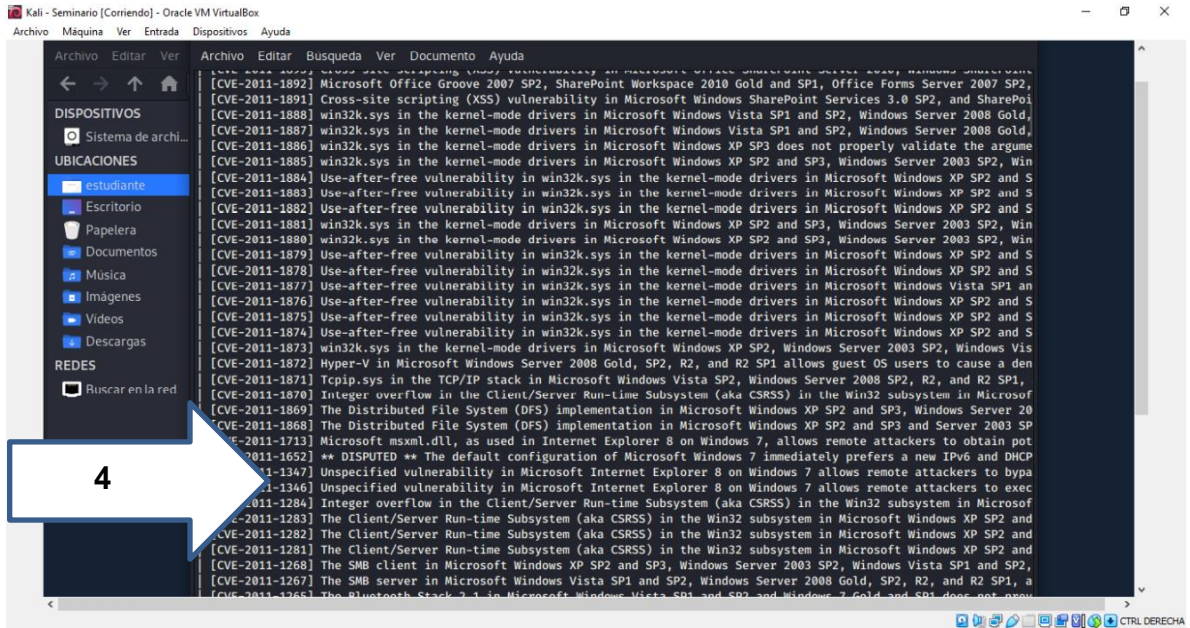
**Fuente Propia**

**Figura 5. Archivo plano con vulnerabilidades técnicas**



**Fuente Propia**

**Figura 5. Archivo plano con vulnerabilidades técnicas**



**Fuente Propia**



A partir de la recolección de información efectuada, se identificó de manera general los siguientes aspectos:

1. Puertos abiertos en referencia al SMB, HTTP, Msrpc, entre otros.
2. Desactualización del Microsoft Windows 7 (SP 1).
3. Escalamiento de privilegios.
4. Notificación por parte de la CVE (Vulnerabilidades y exposiciones comunes).

A partir de la notificación encontrada por la CVE, ese procedió a investigar el tipo de vulnerabilidad técnica al detalle (Se ilustrará mediante el detalle de dos incidencias):

#### **CVE-2011-1883 (Escalamiento de privilegios)**

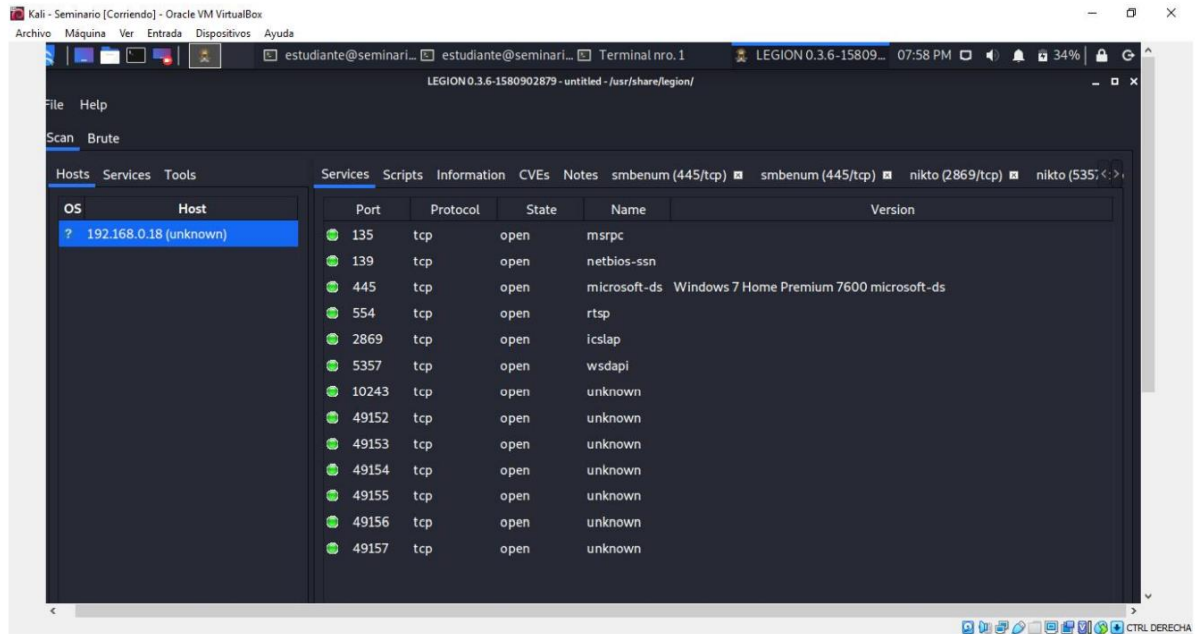
*Vulnerabilidad de uso después de liberarse en win32k.sys en los controladores de modo kernel en Microsoft Windows XP SP2 y SP3, Windows Server 2003 SP2, Windows Vista SP1 y SP2, Windows Server 2008 Gold, SP2, R2 y R2 SP1 y Windows 7 Gold y SP1 permiten a los usuarios locales obtener privilegios a través de una aplicación diseñada que aprovecha la gestión incorrecta de los objetos del controlador, una vulnerabilidad diferente a otras CVE enumeradas en MS11-054, también conocida como "Win32k Use After Free Vulnerability". (CVE, 2021).*

#### **CVE-2011-1881 (Escalamiento de privilegios)**

*win32k.sys en los controladores de modo kernel en Microsoft Windows XP SP2 y SP3, Windows Server 2003 SP2, Windows Vista SP1 y SP2, Windows Server 2008 Gold, SP2, R2 y R2 SP1, y Windows 7 Gold y SP1 permite a los usuarios locales para obtener privilegios a través de una aplicación diseñada que activa una eliminación de referencia de puntero NULO, una vulnerabilidad diferente a otras CVE enumeradas en MS11-054, también conocida como "Vulnerabilidad de eliminación de referencia de puntero nulo de Win32k".*

Se completó la prueba de análisis mediante la ejecución de la herramienta "Legion" la cual contiene a su vez, otras herramientas de escaneo de vulnerabilidades:

**Figura 6. Ejecución herramienta LEGION**

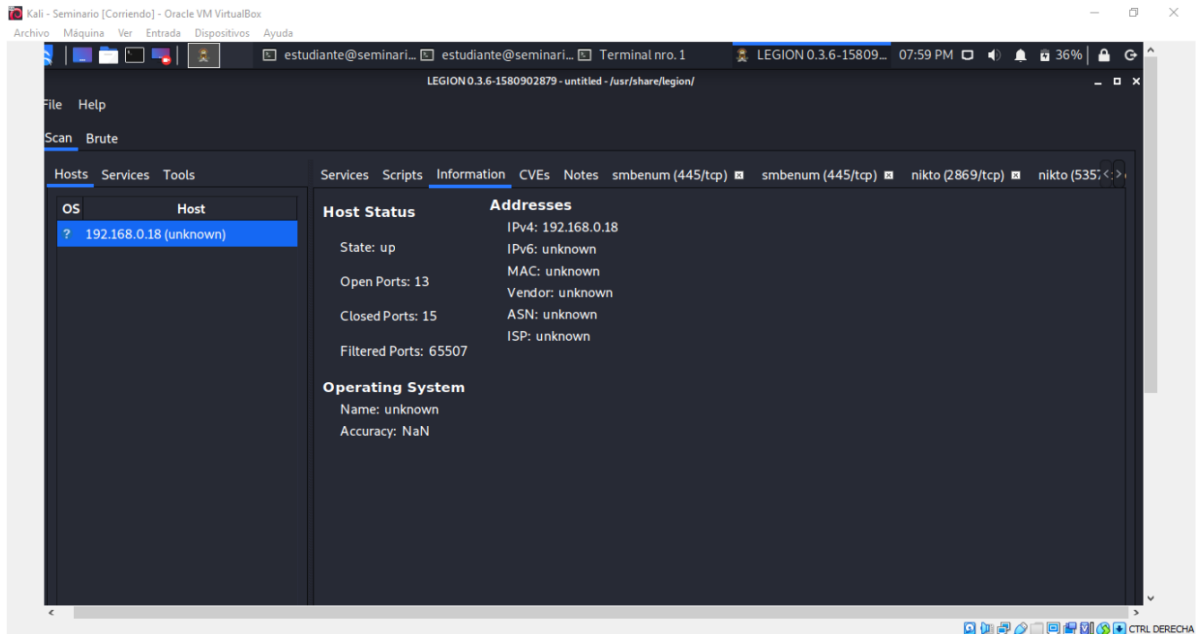


**Fuente Propia**

Se evidencia escaneo con Nmap, y se denota 13 puertos abiertos TCP. Se evidencia el nombre de los puertos y la versión del S.O. Windows 7 home Premium.



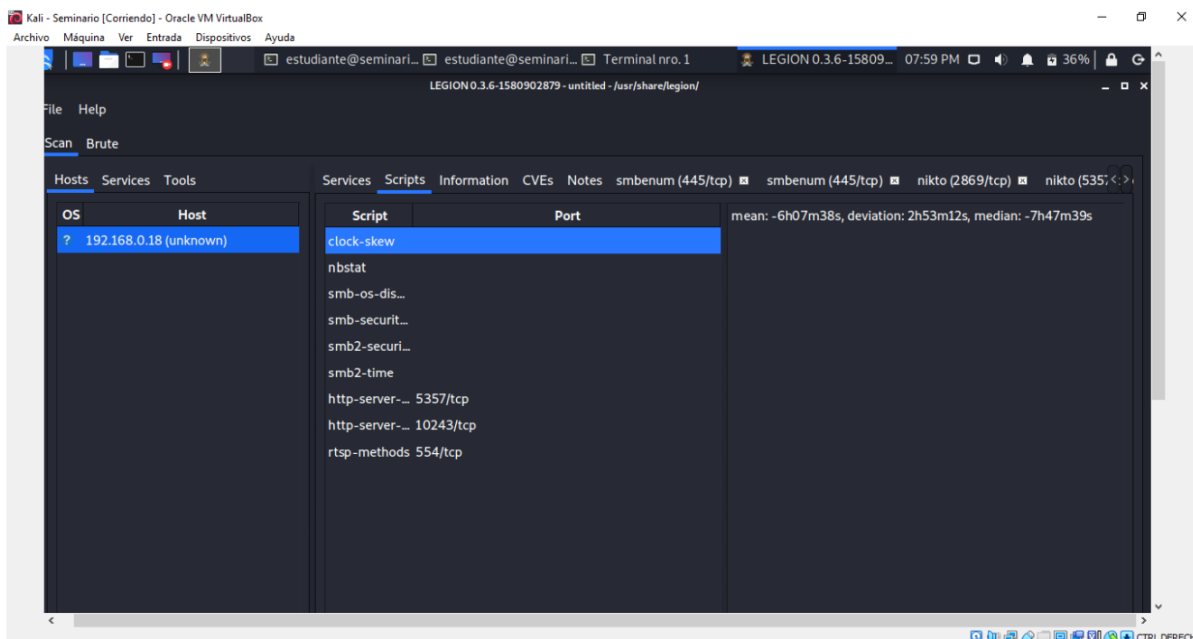
**Figura 6. Ejecución herramienta LEGION**



**Fuente Propia**

*En la imagen se detalla información frente al host el host el cual se encuentra arriba en el momento de efectuar el escaneo. En la siguiente fila, muestra que hay 13 puertos abiertos y hay aproximadamente, 65507 puertos cerrados. No se identifica el sistema operativo "Unknwn". Se detalla la dirección IP de la maquina afectada. No se identifica la IPV6 ni la dirección MAC.*

**Figura 6. Ejecución herramienta LEGION**



**Fuente Propia**

## 6.2.2 Fase de Explotación

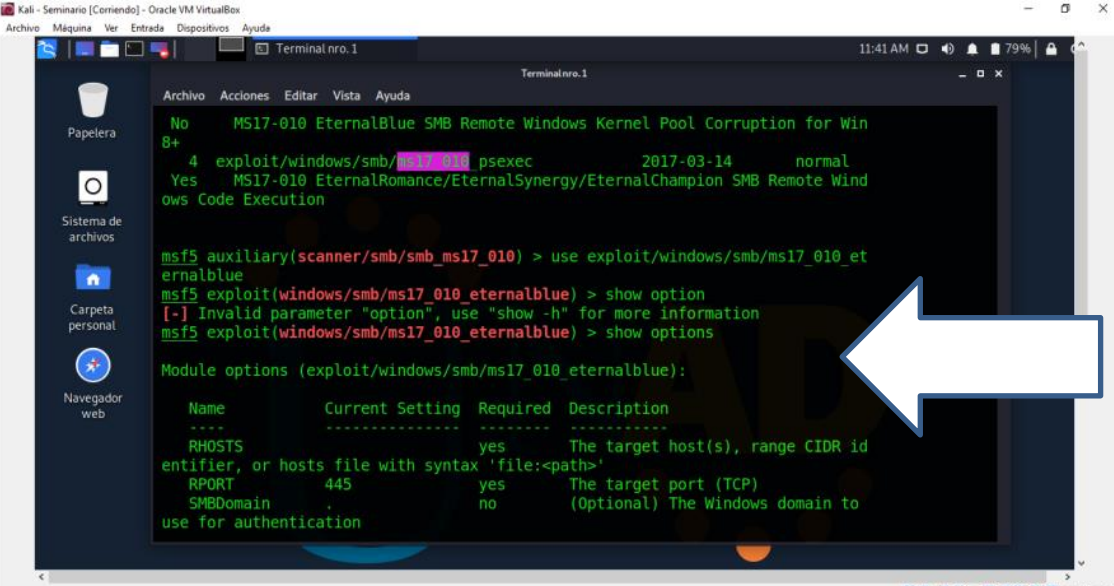
Para efectuar explotación de las vulnerabilidades previamente identificadas, se empleó la herramienta Metasploit.

Para este fin, se ejecutó los siguientes comandos:

`Windows/http/rejetto_hfs_exec`

`Windows/smb/ms17_010_eternalblue`

**Figura 7. Ejecución herramienta Metasploit**



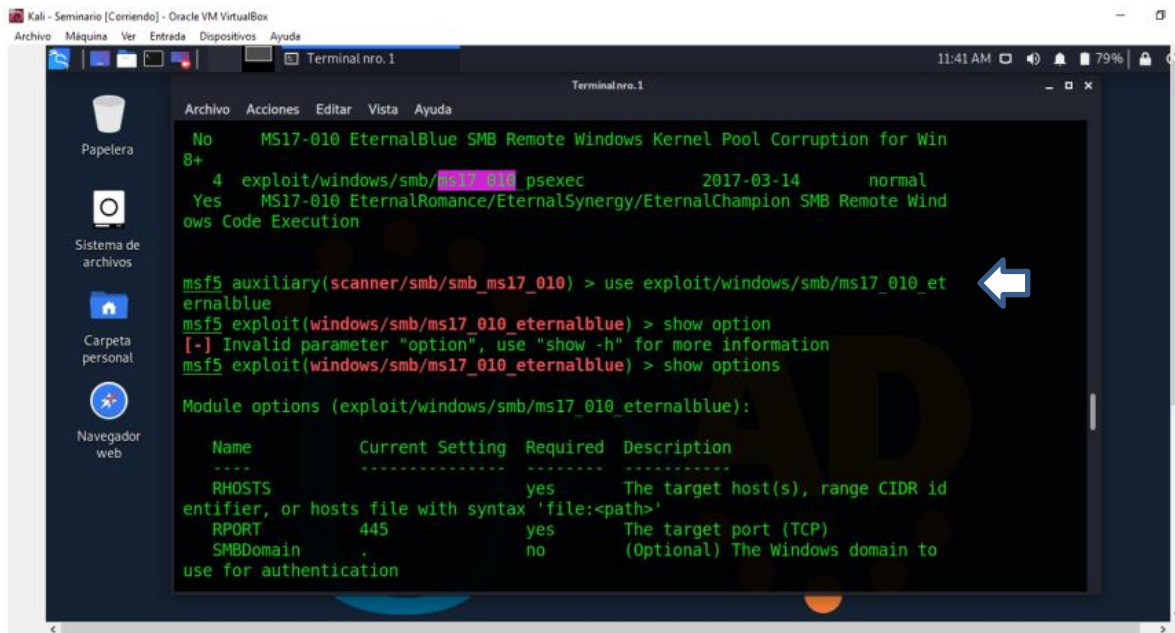
```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    .                yes       The target host(s), range CIDR id
entifier, or hosts file with syntax 'file:<path>'
  RPORT     445              yes       The target port (TCP)
  SMBDomain .                no        (Optional) The Windows domain to
use for authentication
```

**Fuente Propia**

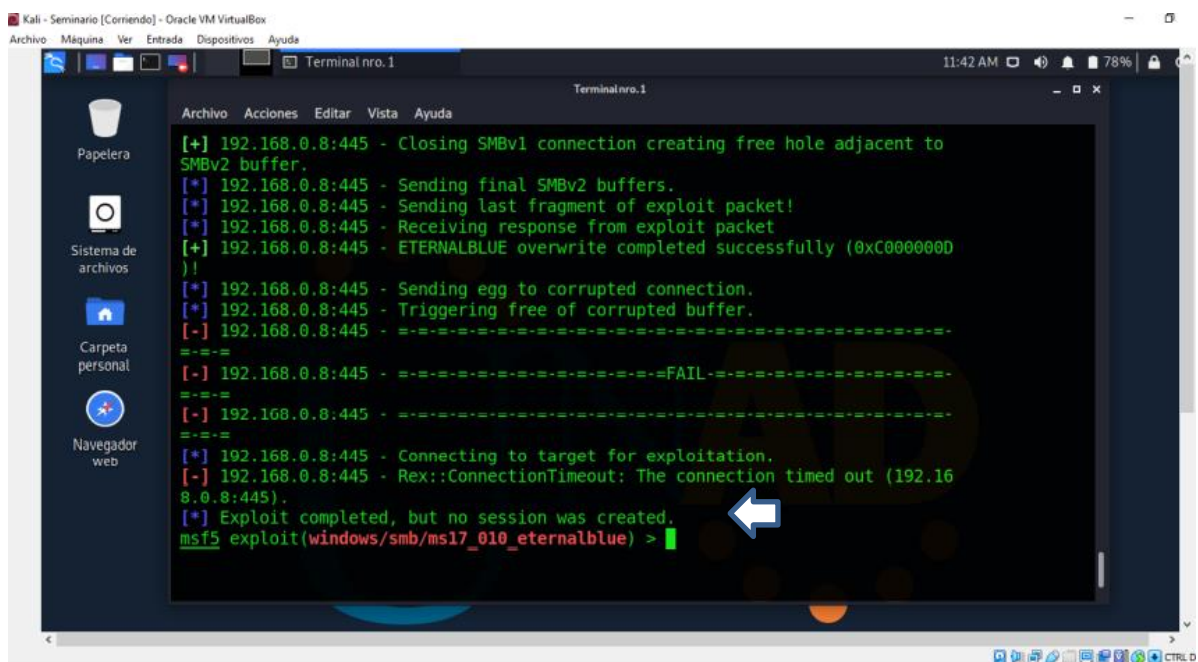
**Figura 7. Ejecución herramienta Metasploit**



**Fuente Propia**

Se procedió a explotar la vulnerabilidad arrojando, la siguiente información.

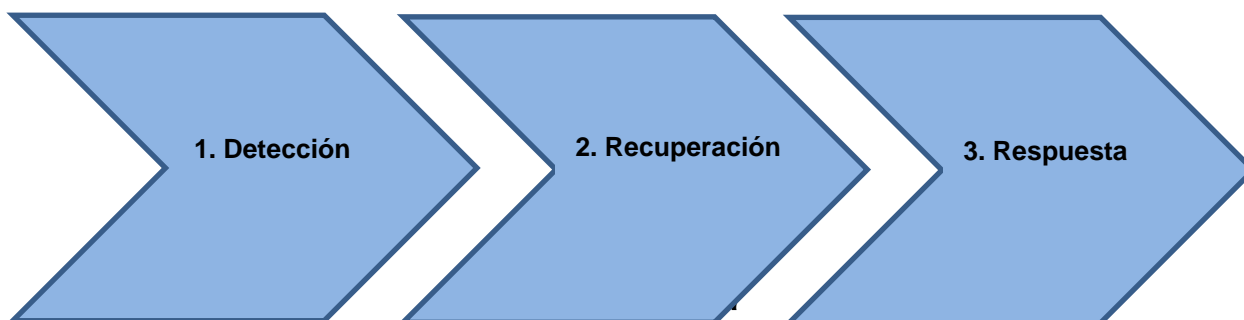
**Figura 7. Ejecución herramienta Metasploit**



**Fuente Propia**

## 6.3 CONTENCIÓN DE ATAQUES INFORMÁTICOS

Ante el ataque sufrido dentro de la maquina virtualizada “Windows 7 X 64”, se procederá a seguir un plan de acción que considerará el siguiente esquema:



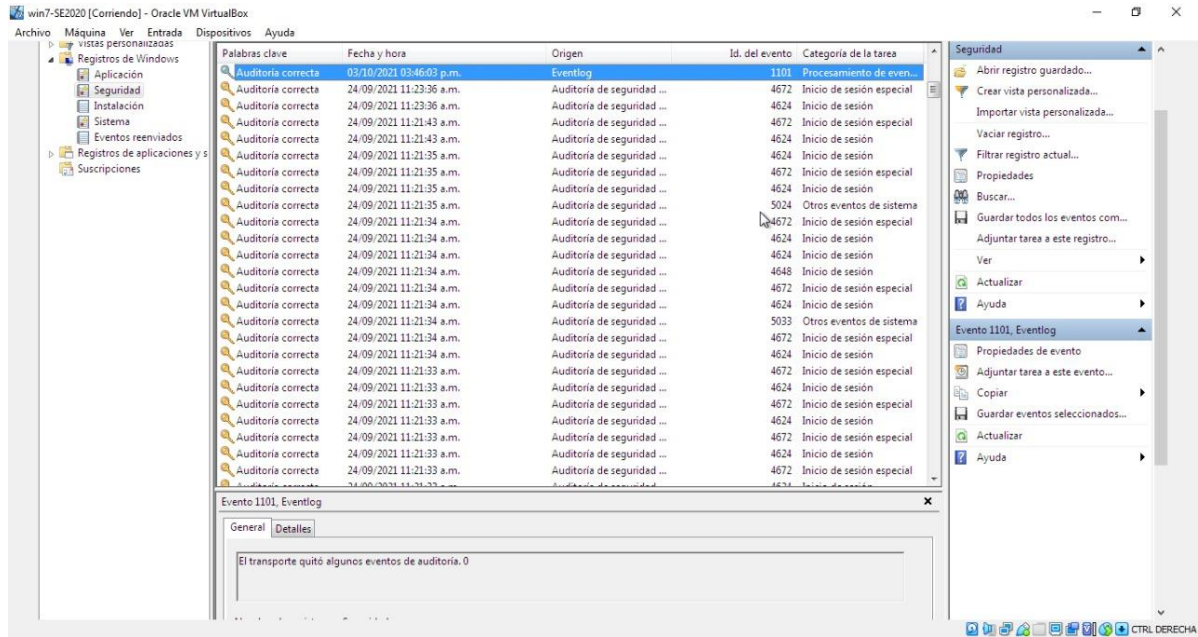
### 6.3.1 Detección:

Dentro de esta sección se puede efectuar la detección como primera instancia, mediante herramientas técnicas que ayuden a identificar los eventos ocurridos e igualmente, la fuente del ataque.

A partir de lo anterior, se hace aprovechamiento de la herramienta “Visor de Windows” la cual se encuentra dentro de la maquina afectada. Se ingresa a la máquina virtual y se examina a partir de dicha herramienta, los eventos registrados el 24 de septiembre de 2021, fecha en la cual se realizó el procedimiento.

Se ingresa a registros de Windows, seguridad y allí se denota diversos eventos registrados.

**Figura 8. Visor de eventos de Windows**



**Fuente: Propia**

El sistema operativo Windows permite registrar igualmente, eventos que puedan originarse desde máquinas externas. Es así, que la herramienta "Netstat" podría ejecutarse desde la máquina afectada para deducir posiblemente, accesos no autorizados desde máquinas atacantes. Se ilustra a continuación el siguiente evento, el cual se originó desde la máquina 192.168.0.6:

Figura 9. Ejecución comando netstat

```
Adaptador de Ethernet Conexión de área local:
  Sufijo DNS específico para la conexión. . . :
  Dirección IPv6 . . . . . : ::95eb:ebc6:4e79:bd21
  Dirección IPv6 temporal. . . . . : ::1a0:f654:2551:9939
  Vínculo: dirección IPv6 local. . . . . : fe80::95eb:ebc6:4e79:bd21%11
  Dirección IPv4. . . . . : 192.168.0.9
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : 192.168.0.1

Adaptador de túnel isatap.{A658CFDA-2CEF-4786-9B5A-536C989076D5}:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . :

C:\Users\usuario>netstat -an

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:554 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2869 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:10243 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING
TCP 192.168.0.9:139 0.0.0.0:0 LISTENING
TCP 192.168.0.9:49178 192.168.0.6:139 TIME_WAIT
TCP 192.168.0.9:49179 192.168.0.6:139 TIME_WAIT
TCP 192.168.0.9:49180 192.168.0.6:139 TIME_WAIT
TCP [::1:80 [::1:0 LISTENING
TCP [::1:135 [::1:0 LISTENING
TCP [::1:445 [::1:0 LISTENING
TCP [::1:554 [::1:0 LISTENING
TCP [::1:2869 [::1:0 LISTENING
TCP [::1:5357 [::1:0 LISTENING
TCP [::1:10243 [::1:0 LISTENING
TCP [::1:49152 [::1:0 LISTENING
TCP [::1:49153 [::1:0 LISTENING
TCP [::1:49154 [::1:0 LISTENING
TCP [::1:49155 [::1:0 LISTENING
TCP [::1:49156 [::1:0 LISTENING
TCP [::1:49157 [::1:0 LISTENING
UDP 0.0.0.0:5000 *: *
UDP 0.0.0.0:3702 *: *
```

Fuente: Propia



Las anteriores actividades se podrían considerar como acciones correctivas en el momento de efectuarse el ataque. Igualmente, deberán discurrir planes correctivos para ejecutarse, estas acciones podrían consistir en las siguientes descripciones:

- **Medias de detección organizativas:**

Establecer un reglamento para gestionar incidentes de seguridad al interior de la compañía. Este reglamento podría estar acompañado de un comité de crisis que sea compuesto por personal con competencias en seguridad informática. Las personas asociadas al comité podrán ejecutar tareas coordinadas y eficientes para tratar de manera asertiva, el incidente de seguridad que se presente.

- **Medidas de detección legales:**

Estas medidas podrán ser consideradas en el momento de efectuar recolección de evidencias, bien sea por personal competente que labore al interior de la compañía o, personal externo que tenga la competencia suficiente para tratar los registros probatorios en caso de iniciar una investigación ante el hecho fraudulento.

Para este escenario la compañía deberá registrar el evento mediante descripción del hecho, el tipo de evento dado, el registro en términos de tiempo en que se haya dado el hecho, el detalle de las personas quienes realizan la notificación, las consecuencias impartidas de la incidencia y por último, la descripción acerca de las medidas y/o correcciones que se efectuaron.



### **6.3.2 Recuperación:**

Dentro de este apartado se deberá restaurar el sistema informático antes de que el evento se haya dado. Aquí se podrá aplicar o restaurar la información mediante las copias de seguridad que hayan sido generadas por la compañía afectada.

Se podrán cerrar las brechas de seguridad identificadas tales como puertos accesos habilitados para evitar nuevos ingresos indebidos.

Se podrá igualmente poner en marcha el plan de continuidad del negocio el cual deberá tener mediante su estructura, las diversas acciones que deberán ponerse en ejecución ante un posible evento que amenace con la indisponibilidad de los activos informáticos custodiados por la compañía.

### **6.3.3 Respuesta:**

Dentro de esta instancia, se deberá poner en marcha los planes de comunicación estructurados por la compañía. Deberán ser dirigidos a todas sus partes interesadas, tal como se muestra a continuación:

- **Respuestas a clientes:**

Es muy importante poner en conocimiento el incidente de seguridad surgido al interior de la compañía, el cual deberá conocer los clientes de la empresa. Para el caso expuesto dentro del ejercicio, este será parte del protocolo implantado en la empresa. En otros países, este tendrá que ser una actividad obligatoria en lo que respecta al marco de gestión de datos personales, por lo que, si se viera afectada la información de los titulares, la compañía está en la obligación de reportar a estos el evento surgido.

- **Respuestas dentro de la organización:**

Este tipo de respuesta deberá ser dada a los colaboradores de la compañía para que tengan el conocimiento del caso y, puedan referirse ante el incidente con completo conocimiento del caso, de explicar a los clientes de la compañía el suceso presentado.

Por otro lado, será necesario que se comunique para crear conciencia a cada uno con el propósito de que aporten a una gestión importante en aspectos de seguridad y una muy buena custodia a los activos informáticos que tengan bajo su cargo.

- **Respuestas a terceros:**

Dentro de este apartado, se refiere a todos los medios de comunicación que podrían incidir el tipo de negocio que se gestiona. Aquí podría considerarse aquellos medios de comunicación tales como periodísticos y diversas plataformas digitales.

#### **6.1.4 Denuncias:**

Ante los eventos de seguridad presentados dentro de la compañía, es importante entablar denuncias judiciales para que esto se ponga en conocimiento de las diferentes autoridades y estas, puedan aportar a las investigaciones que permitan esclarecer los hechos delictivos presentados.

## 6.4 MEDIDAS DE HARDENIZACIÓN

- Instalar las últimas versiones del sistema operativo o software liberado por el fabricante, siempre y cuando esta sea una versión estable y soportada por la función a instalar.
- Instalar los últimos parches del sistema operativo o versión del software, siempre y cuando no vaya a crear conflictos con los otros sistemas o servicios con los que interactuará.
- Deshabilitar los servicios del sistema operativo o software que no van a ser usados por el servicio, la operación o la administración.
- Deshabilitar las aplicaciones, servicios o protocolos que sean inseguros o cuenten con vulnerabilidades conocidas.
- Bloqueo de puertos que no van a hacer usados por el servicio, la operación o la administración.
- Bloquear la transferencia de archivos.
- Evitar el uso del usuario administrador o root del sistema para la ejecución de los servicios, para los que aplica.
- Establecer permisos y diferentes niveles de privilegios para usuarios que por operación o administración puedan requerir.
- Eliminar los usuarios del sistema operativo o software que vienen por defecto y que no van a ser usados en el servicio, operación o administración.
- Tomar como base, en los puntos que pueda aplicar, o implementar las guías de hardening propuestas por organismos internacionales de buenas prácticas de seguridad como CIS (Computer for Internet Security) u otros reconocidos
- Habilitar los logs de auditoría para dejar trazabilidad de las acciones realizadas en el sistema operativo o software.

Adicional a lo anterior, se podría considerar controles compensatorios de red, operativas o a través de elementos tecnológicos, que fortalezcan las seguridades del sistema y servicios para así minimizar el riesgo asociado a:

- Acceso no autorizado.
- Escalamiento de privilegios.
- Interceptación de comunicaciones.
- Comunicaciones con equipos de la red no necesarios por el servicio.
- Comunicaciones con protocolos inseguros.
- Explotación de vulnerabilidades.
- Infecciones por archivos o tráfico de red malicioso.
- Escaneo de puertos.
- Entre otros.

## 7 LINK VIDEO DE SUSTENTACIÓN

[https://youtu.be/RfEpFqfs\\_8s](https://youtu.be/RfEpFqfs_8s)

## 8 CONCLUSIONES

En este trabajo se estableció el diseño frente a la estructura de un informe técnico dentro del cual, se contempló las recomendaciones acerca de estrategias de contención empleadas por equipos de Blue Team con base, a los procedimientos practicados por equipos de Red Team, demostrando mediante esto, la importancia de instituir dentro de una organización buenas prácticas en relación con la constitución de grupos especializados en seguridad informática.

El desarrollo ejercido dentro del presente documento permitió explorar mediante el enfoque ofrecido por medio del seminario especializado y el despliegue de diversas fuentes de información, el procedimiento en toda su extensión respecto a la misión, directrices y objetivos que enmarcan las funciones desarrolladas por parte de grupos de seguridad denominados Red Team y Blue Team. A partir de lo anterior, se identificó la preeminencia de constituir estos equipos de seguridad los cuales, aportan por medio de una metodología bien definida, controles que asisten a que las amenazas de seguridad sean contenidas e intervenidas.

Es así, que la generación en cuanto a la colocación de los formatos diseñados con base a informes reales que generalmente son ofrecidos por medio de los equipos de seguridad de referencia destacó mediante su contenido, procedimientos que al ser aplicados generan un nivel de seguridad arduo para cualquier tipo de compañía que desee adoptar buenas prácticas y estándares de seguridad comprobados.

Dentro del marco del seminario especializado ofrecido por la universidad UNAD, se determinó para el desarrollo del presente documento, los lineamientos que permitieron definir, diseñar y argumentar información suficiente para establecer los informes de gestión con base a la ejecución práctica de pruebas de Pent Testing y Análisis de Vulnerabilidades Técnicas. A partir de lo anterior, se argumenta la

importancia de lo desarrollado ya que esto logró evidenciar que las prácticas de seguridad deben ser tareas dinámicas y no estáticas, por lo que las amenazas informáticas incrementan exponencialmente y su nivel de riesgo es importante ante la posibilidad de materializarse, desligando un posible incidente de seguridad tipo grave.

Una de las cosas que más contribuyó al desarrollo del trabajo fue justamente el revelar por medio de la identificación de cada una de las actividades que asumen los grupos de seguridad blue team y red team los cuales, establecen una serie de tareas que aportan de manera preventiva, a que se realice gestión para la contención de amenazas tales como ataques cibernéticos cambiantes y latentes a los cuales se ven expuestos de manera recurrente y concurrida, los diversos sistemas informáticos en general. La actividad frente al desarrollo del documento permitió reconocer la problemática a la cual se expone actualmente muchas organizaciones ya que, en su mayoría, las empresas apoyan su CORE del negocio sobre sistemas de información los cuales, si fallan, podrían representar impactos determinantes tales como el cierre definitivo o total de una organización.

## 9 RECOMENDACIONES

A partir del tema desarrollado dentro del marco de gestión del seminario especializado el cual ayudó a construir e identificar las trascendentales funciones que determinan los grupos de seguridad Blue Team y Red Team, acompañado de esto, la identificación de los tipos de ataques impulsados actualmente y de manera recurrente por grupos no éticos de hacking, la identificación de herramientas técnicas para apoyar en esta labor notable de dichos equipos de seguridad y, las diversas vulnerabilidades halladas en sistemas de información, se establece los siguientes preceptos como parte de las recomendaciones derivadas de la experiencia practicada :

- Ahondar dentro de la práctica profesional para determinar con mayor detalle, las metodologías y herramientas técnicas las cuales aportan en la calidad de los procesos ejercidos por parte de los equipos de Red Team.
- Conocer a mayor escalabilidad y a partir de las experiencias practicadas por parte de los equipos de seguridad Blue Team, los procesos considerados para endurecer la seguridad de la información los cuales son desarrollados a partir de los tipos de vulnerabilidades técnicas descubiertas en diversos sistemas de información.
- Poner en práctica y de manera recurrente, la actividad efectuada para confirmar sus procedimientos y el detalle frente a la eficacia de sus resultados.

Lo anteriormente descrito, aportará mayor eficiencia a la actividad por lo que contribuirá sin lugar a duda, a la calidad de la formación del programa de Especialistas en seguridad informática.



## BIBLIOGRAFÍA

ACTUALÍCESE. Ataques informáticos ¿Están las organizaciones preparadas paraenfrentarlos?.[Sitio Web]. Colombia.Ernst&Young.[Consulta: el 22 de septiembre de 2021]. Disponible en: <https://actualicese.com/ataques-informaticos-estan-las-organizaciones-preparadas-para-enfrentarlos/>

AUDITECH. Seguridad Ofensiva.[Sitio Web]. España.Tech Solutions for your business.[Consulta: el 29 de septiembre de 2021]. Disponible en: <https://auditech.es/seguridad-ofensiva/>

BLOG - LATEST NEWS. Como ha evolucionado la ciberseguridad en los último 25 años y como ha sido la evolución de la seguridad de las empresas. [Sitio Web]. Colombia. Hard2bit CyberSecurity.[Consulta: el 22 de septiembre de 2021]. Disponible en: <https://hard2bit.com/blog/como-ha-evolucionado-la-ciberseguridad-en-los-ultimos-25-anos-y-como-ha-sido-la-evolucion-de-seguridad-en-las-mpresas/>

CAMPUSCIBERSEGURIDAD. Phishing, una de las principales amenazas de Nuestra era. [Sitio Web]. España. Campus de Ciberseguridad. [Consulta: el 29 de septiembre de 2021]. Disponible en: <https://www.campusciberseguridad.com/blog/item/128-phishing-principal-menaza-de-nuestra-era>

CVE. Common Vulnerabilities and Exposures.[Sitio Web]. USA. [Consulta: el 1 de octubre de 2021]. Disponible en: <https://cve.mitre.org/>

CSAT. Controls Evaluation [Sitio Web]. EEUU [Consultado : el 05 de octubre de 2021]. Disponible en : <https://csat.cisecurity.org/critical-controls/control/061b05ea-ed66-4d39-9c16-6208647a51bb/>

FIREEYE. Operación del equipo de emergencias Red Team.[Sitio Web]. España.Ficha tecnica - Fireeye.[Consulta: el 29 de septiembre de 2021]. Disponible en: [https://www.fireeye.com/content/dam/fireeye-www/regional/mx\\_ES/services/pdfs/ds-red-team-operations.pdf](https://www.fireeye.com/content/dam/fireeye-www/regional/mx_ES/services/pdfs/ds-red-team-operations.pdf)

GEEKSFORGEEKS. [Sitio Web] EEUU. [Consulta: el 06 de octubre de 2021]. Disponible en: <https://www.geeksforgeeks.org/what-is-information-security/>

HEMEROTECA UNAD. Seguridad informática en el siglo XXI. Una perspectiva jurídica tecnológica enfocada hacia las organizaciones y mundiales. [Sitio Web]. Colombia. Juan José Candelario Samper & Moises de Jesus Rodriguez Bolaño.Universidad Nacional Abierta y a Distancia.[Consulta: el 22 de septiembre de 2021]. Disponible en: <https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1441/1880>

INCIBE. Tendencias en el mercado de la ciberseguridad.[Sitio Web]. Madrid. Ministerio de Industria, Energía y Turismo.[Consulta: el 1 de octubre de 2021]. Disponible en: [https://www.incibe.es/sites/default/files/estudios/tendencias\\_en\\_el\\_mercado\\_de\\_la\\_ciberseguridad.pdf](https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf)

ISO 27001. Sistema de Gestión de Seguridad de la Información. [Sitio Web]. España. ISO27001.ES. [Consulta: el 29 de septiembre de 2021]. Disponible en: [https://www.iso27000.es/sgsi.html#:~:text=Un%20SGSI%20desde%20la%20visi%C3%B3n,%20de%20servicio%20\(p](https://www.iso27000.es/sgsi.html#:~:text=Un%20SGSI%20desde%20la%20visi%C3%B3n,%20de%20servicio%20(p)

ISO. [Sitio Web] EEUU [Consultado: el 06 de octubre de 2021]Disponible en: <https://www.iso.org/home.htmllog/que-es-un-siem>

LEY 1581 DE 2012. Ley de tratamiento de datos personales. [Sitio Web]. Colombia. Consulta de la norma. [Consulta: el 29 de septiembre 2021]. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

PURPLESEC. Red team vs blue team: what's the difference? [Sitio Web] EEUU.[Consulta: el 06 de octubre de 2021]. Disponible en: <https://purplesec.us/red-team-vs-blue-team-cyber-security/>

WELIVESECURITY. [Sitio Web] EEUU. [Consulta: el 06 de octubre de 2021]. Disponible en: <https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/>