# CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOHN EDIER RIAÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2022

# CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOHN EDIER RIAÑO

M.Sc. JOHN FREDDY QUINTERO
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2022

## RESUMEN

El documento sintetiza un informe técnico realizado con las temáticas tratadas en el Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team de la Universidad Nacional Abierta y a Distancia UNAD.

Este informe técnico busca describir las características que existen entre los equipos interdisciplinarios Red Team y Blue Team y, a su vez mostrar las actividades que desempeñan, los logros que obtienen al desplegar sus capacidades técnicas en el ámbito empresarial.

El informe muestra la importancia que tienen los equipos Red Team y Blue Team en las compañías, muestra desde los fundamentos jurídicos hasta la descripción de las actividades técnicas que estos equipos realizan. Para este informe se ha tenido en cuenta un caso puntual relacionado en los anexos de cada una de las fases propuestas por el seminario y, de manera simulada se hizo el respectivo análisis con herramientas de intrusión y testing, brindando de esta forma un contexto general hasta llegar a unas conclusiones que muy seguramente tienen una relevancia a la hora de documentarse y tener una guía que permita elaborar un plan para contener y, prevenir un ataque informático en determinada organización.

El informe contiene 5 fases que inicia con la apropiación de conceptos relacionados con la seguridad informática, pasa por la actuación ética y legal, después muestra herramientas de mitigación de ataques junto a procedimientos técnicos propios de los equipos Red Team y Blue Team, hasta llegar a la socialización de cada una de las actividades.

## CONTENIDO

pág.

## TABLA DE ILUSTRACIONES

## GLOSARIO

**ATAQUE INFORMÁTICO:** Son los diferentes intentos que los ciberdelincuentes realizan con el objetivo de vulnerar una red informática por medio de técnicas empleando software malintencionado como virus, troyanos, malware. Etc.

**COPNIA:** Es la entidad gubernamental de Colombia que tiene la labor de vigilar, inspeccionar y controlar el ejercicio de la ingeniería en todo el territorio nacional.

**EXPLOIT:** Es una parte de software o datos con la que se aprovecha una vulnerabilidad informática para lograr un comportamiento inesperado del mismo. Generalmente al identificar una vulnerabilidad en los sistemas, los intrusos toman posesión con privilegios de administrador para generar denegación de servicio en las organizaciones.

**INFORMACIÓN:** Es el conjunto de elementos en especial datos que están ordenados de manera lógica y que busca transmitir una idea a quien los interpreta, se emplea para transmitir un mensaje en específico o a su vez generalizado.

**SEGURIDAD INFORMÁTICA:** son las medidas que adoptan las organizaciones y los particulares con el objetivo de proteger sus activos digitales para que no sean vulnerados por ciberdelincuentes.

**SISTEMAS INFORMÁTICOS:** Es el conjunto de activos conformados tanto por Software y Hardware, son los que se encargan de recibir instrucciones, procesar datos y realizar diferentes tareas ordenadas por un usuario.

**TIC:** Sus siglas significan **TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES,** son los diferentes elementos de la informática empleados para realizar procesos y poder recibir y transmitir información.

**VIRUS INFORMÁTICO:** Son software o códigos que buscan infectar un sistema informático con el fin de alterar su funcionamiento y realizar una tarea específica que generalmente es malintencionada.

**VULNERABILIDAD:** Son las debilidades con las que cuenta un sistema informático o una infraestructura de red las cuales pueden ser aprovechadas por ciberdelincuentes para hurtar o alterar la información.

## INTRODUCCIÓN

El informe técnico comprende una contextualización de conceptos de los equipos de ciberseguridad desde el punto de vista jurídico de la normatividad colombiana y, a su vez de la definición técnica de las diferentes herramientas empleadas en la ciberseguridad. También este informe muestra la implementación de un banco de trabajo implementado de manera simulada en un ambiente virtual con el sistema operativo Linux y Windows.

También comprende una serie de preguntas enfocadas en las leyes de la seguridad de la información de Colombia, más específicamente de la ley 1273 de 2009; con la que hace una comparación de las implicaciones de esta ley frente a un caso de ejemplo dado como anexo y, se realiza un análisis de las vulnerabilidades cometidas y las consecuencias que estas conllevan al cometer delitos informáticos.

A su vez se hace un análisis personal de si se aceptaría una oferta laboral en la compañía WhiteHouse Security, teniendo presente la firma de una cláusula de confidencialidad, que entre sus ítems se generan dudas con respecto a las funciones asignadas y también se hace un análisis del caso muy mencionado en Colombia llamado Operación Andrómeda Buggly que se refiere a un caso de espionaje por el ejército colombiano.

Este documento comprende la solución a varias actividades que inicialmente son en términos teóricos y que posteriormente se lleva a términos prácticos, los temas desarrollados en dichas actividades son con base al tema de ejecución de pruebas de intrusión. Se parte desde el análisis de una situación problema planteado en el escenario y en el que se busca realizar pruebas de intrusión desde el sistema operativo Kali Linux para encontrar las vulnerabilidades en el sistema operativo Windows 7 x64.

El informe técnico describe cada una de las herramientas empleadas para realizar las pruebas de intrusión, también la información suministrada directamente en los anexos de cada actividad y finalmente se describe paso a paso todo el procedimiento que se ejecutó para encontrar las mencionadas vulnerabilidades.

En resumen, el desarrollo de toda la actividad se centra en interactuar de manera práctica y concisa con el banco de datos instalado y, configurado en una máquina virtual previamente configurada en el sistema operativo Kali Linux y Windows 7 x64, con los que se buscó hacer procesos prácticos de manera simulada.

Las temáticas abordadas en este informe técnico son contextualizaciones de conceptos que en su mayoría ya han sido vistos durante la carrea y, también

algunos que son nuevos, pero a que a su vez se complementan conceptualmente.

Es así como se ha realizado una serie de preguntas que van desde la definición de temas específicos hasta la descripción de sus características y, diferencias en cuanto a la contención de ataques cibernéticos.

# OBJETIVOS

## 1.1 OBJETIVO GENERAL

Que el informe técnico sirva como guía para la identificación de un problema específico en temas técnicos que se presentan en equipos Blue Team y Red Team y, a su vez les sirva como insumo para atender ataques cibernéticos con mayor agilidad y eficacia.

## 1.2 OBJETIVOS ESPECÍFICOS

- Conocer los decretos, leyes y normas que actualmente existe con el fin de identificar sus características de cada una de ellas.
- Configurar un banco de trabajo en la herramienta de virtualización VirtualBox
- Definir cada una de las etapas de pentesting y dar un ejemplo de una herramienta de cada definición.
- Reconocer la importancia que tiene los equipos de ciberseguridad dentro de las compañías para contener ataques cibernéticos.
- Documentar los procedimientos paso a paso realizados para encontrar las vulnerabilidades del sistema operativo Windows 7 x64.

# 2 CONCEPTOS EQUIPOS DE SEGURIDAD

## 2.1 Normatividad en Colombia sobre delitos informáticos.

En Colombia las leyes que se encargan de tipificar la protección de la información y los delitos informáticos están centradas en la ley 1581 de 2012 y la ley 1273 de 2009. La primera ley se encarga de velar por la protección de datos y la información, al mismo tiempo es una ley reglamentada de manera parcial por el decreto de ley reglamentario 1377 de 2013, la segunda ley se encarga de los delitos informáticos.

**Ley 1581 de 2012:** Esta ley tiene como objetivo velar por el derecho que tienen todas las personas en Colombia a conocer, actualizar y corregir sus datos personales que se guarden en bases de datos y/o archivos , también a proteger los derechos, garantías y libertades estipulados en la Constitución Política en su artículo 15; así como también lo estipula el artículo 20 de la Constitución el cual establece el derecho a la información.

En efecto esta ley fundamenta las respectivas disposiciones legales para la protección de la información personal almacenada en archivos, sistemas o bases de datos que pueden ser utilizados por compañías privadas o públicas. Dicha ley establece los parámetros que clasifican los datos sensibles y el tratamiento que se le debe dar y caracterizándolos al afirmar que los datos sensibles son los que atentan contra la intimidad de las personas y que pueden dar espacio a algún tipo de discriminación si la información es mal utilizada. También busca proteger los derechos de los adolescentes, niñas y niños en el ámbito del tratamiento de sus datos personales.

En esta ley se establecen los deberes y derechos de los dueños de la información y de quienes la administran, también establece los sistemas de vigilancia y control por medio de la SIC (Superintendencia de Industria y Comercio) entidad encargada de establecer las sanciones a que dé lugar aplicar[1].

**Ley 1273 de 2009:** Esta ley se encarga de la protección de datos y la protección de la información. También se encarga de tipificar los delitos que vulneran la integridad, confidencialidad y disponibilidad de la información, es así como en el capítulo primero de la misma se relacionan los delitos de interceptación de datos informáticos, el acceso abusivo a un sistema informático , violación de datos personales, utilización de software malicioso, suplantación de sitios web , etc. En el capítulo segundo se relaciona los delitos de hurto a través de medios informáticos

[1] FUNCIÓN PÚBLICA. Ley 1581 de 2012. [En línea]. [Consultado : 10 de febrero de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

y la manipulación de información, transferencia de información sin autorización, así como otros delitos estipulados en esta ley 1273 de 2009[2].

**Documento CONPES 3701 de 2011:** Este documento tiene como objetivo darle herramientas al Estado colombiano para enfrentar las amenazas que atentan contra la seguridad y defensa nacional en cuanto a la ciberseguridad lo que le permite al estado crear normatividades para garantizar y proteger el ciberespacio y, de esta manera contribuir al crecimiento y fortalecimiento de la economía digital[3].

**Documento CONPES 3854 de 2016:** Este documento busca preparar y concientizar a todos los actores del entorno digital para que conozcan los riesgos informáticos a los que están expuestos en la era digital y con el objetivo de aportar al crecimiento vertiginoso de la economía digital y al mismo tiempo generar prosperidad[4].

## 2.2 Pentesting

El pentesting son las pruebas que se realizan en un sistema informático con el objetivo de encontrar las vulnerabilidades[5] que tiene con respecto a la seguridad informática, busca identificar las fallas que hay en la disponibilidad, confidencialidad e integridad de la información del sistema informático. Cuando en las compañías realizan actividades de pentesting buscan identificar las fallas y vulnerabilidades a las que están expuestas y cuál es la capacidad o el nivel que tienen actualmente para defenderse y contrarrestar los ataques informáticos.

Hay varios tipos de pentestig como lo es del de **Caja blanca**, en este el profesional que realiza el proceso conoce bien los datos del sistema como son las contraseñas, las IPs, y toda su infraestructura de software y hardware; lo que le permite tener una gran facilidad para identificar qué puede ser vulnerado o mejorado dentro del sistema[6].

---

[2] CONGRESO DE COLOMBIA. Ley 1273 de 2009. [En línea]. [Consultado: 10 de febrero de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[3] ALCALDÍA DE BOGOTÁ D.C. CONPES 3701 DE 2011. [En línea]. [Consultado : 10 de febrero de 2022]. Disponible en: https://tic.bogota.gov.co/transparencia/marco-legal/normatividad/conpes-3701-2011

[4] CÁMARA DE COMERCIO BOGOTÁ. Documento Conpes 3854, Política nacional de seguridad digital. [En línea]. [Consultado : 10 de febrero de 2022]. Disponible en: https://bibliotecadigital.ccb.org.co/handle/11520/14856

[5] S. Rahimi, M. Zargham (2013). "Vulnerability detection with deep learning," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2013, pp. 395 - 407, doi: 10.1109/CompComm.2017.8322752. Consultado el 02 de octubre de 2021.Disponible en:https://ieeexplore.ieee.org/document/6502762

[6] CAMPUSCIBERSEGURIDAD. ¿Qué es el pentesting? [En línea]. [Consultado: 10 de febrero de 2022]. Disponible en: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

También existe pentesting de **Caja negra**, en esta actividad es mucho más real, porque el pentester no tiene la suficiente información del sistema y actúa simplemente como un atacante y debe realizar las pruebas a oscuras, debe identificar las amenazas y vulnerabilidades a las que está expuesta la compañía.

Por último, se tiene el pentestig de **Caja gris,** es una combinación de los dos anteriores ya que el pentester o auditor cuenta con toda la información en el momento de realizar la prueba, este tipo de pentester es el más empleado y solo se requiere de tiempo para realizar la prueba en toda su totalidad.

Por otra parte, las actividades que realiza un pentester se fundamenta en llevar la secuencia de varios procesos que garanticen un buen resultado y pueda encontrar todas las vulnerabilidades y amenazas posibles.

**Etapas de pentestig**

- **Etapa de reconocimiento**: En esta etapa se busca información sobre la compañía en todos los medios digitales como internet, en sitios web que permitan identificar el dominio para identificar la información de contacto y los DNS, se revisan bases de datos con el objetivo de hallar información de los equipos, herramientas y tecnología que emplea la compañía.

Existen varias herramientas empleadas para ejecutar la etapa de reconocimiento:

- **BuiltWith:** Es un generador de perfiles que le suministra a los pentester información en tiempo real por medio de una API de dominios lo que le permite tener información técnica y el análisis de la información del sistema de la compañía[7].

- **Etapa de escaneo:** En esta etapa se efectúa el escaneo de servicios, puertos, sistemas operativos y se debe tener en cuenta los dispositivos activos con un escaneo del protocolo ICMP y luego efectuar el escaneo en el protocolo TCP con el objetivo de encontrar puertos abiertos en los dispositivos y de esta manera encontrar las vulnerabilidades.

**Herramienta utilizada para la etapa de escaneo:** En esta etapa se emplea la herramienta Nmap que es un software de código libre para rastrear puertos, como por ejemplo realizar un escaneo de la siguiente manera **Nmap -sS 192.168.1.27,** lo

[7] GEEKFLARE. Herramientas en línea de pentest de reconcimiento. [En línea]. [Consultado: 11 de febrero de 2022]. Disponible en: https://geekflare.com/es/reconnaissance-exploit-search-tools/

que significa que **–sS** el tipo de escaneo que se hace con Nmap que en este caso es el escaneo SYN lo que permite analizar el puerto configurado en la dirección IP **192.168.1.27**

- **Etapa de identificación:** Esta es la etapa de análisis de vulnerabilidades y seguridad de las aplicaciones y en ella se emplea la herramienta Openvas, también puede emplearse la Bort Suite.

Con la **herramienta Openvas** se hace el análisis a determinado host por medio de la dirección IP y se puede configurar en la herramienta la labor que debe realizar para encontrar el análisis y las vulnerabilidades para finalmente generar un informe con el resultado mostrando todas las vulnerabilidades con las que cuenta el sistema.

- **Etapa de explotación:** En esta etapa es donde se logra tener acceso al sistema de la compañía para efectuar los exploits contra las vulnerabilidades anteriormente identificadas.

En esta etapa se puede emplear la **herramienta** Metaexploit que contiene una gran cantidad de exploit[8] para realizar el ataque dentro de un dispositivo y explotar las vulnerabilidades que tiene, lo que le permite ingresar de manera remota al host atacado y aprovechar las vulnerabilidades.

- **Etapa de informes:** En esta etapa lo que se realiza es un informe técnico con todos los resultados hallados en las pruebas de pentesting**,** el informe técnico comprende detalladamente todo el proceso realizado como las técnicas empleadas, herramientas que se utilizaron, vulnerabilidades y fortalezas que se encontraron en el ejercicio.

### 2.3 Herramientas de pentestig

- **Metasploit:** Esta herramienta es empleada para efectuar exploit con la que se identifica la seguridad de los dispositivos por medio de códigos y aprovechar las vulnerabilidades del sistema. Con esta herramienta se logra conseguir las credenciales de acceso al sistema, la exportación de información y escaneo de puertos de acceso.

- **Nmap:** Con esta herramienta se hacen auditorías en la seguridad de las compañías a su vez identificar redes y vigilar el tiempo de la actividad del

[8] EXPLOIT DATABASE. Exploit. Consulted: March 18, 2022. Available in: https://www.exploit-db.com/exploits/42031

dispositivo por medio de paquetes de direcciones IP, tiene la utilidad de transferencia de datos, una herramienta del análisis de respuesta y permite comparar los resultados de todo el escaneo. El tipo de sondeo que realiza puede ser en los protocolos UDP, TCP y SYN, también sondeo del protocolo IP, con esta herramienta se logra identificar los puertos cerrados o abiertos y realizar escaneo a puertos en el protocolo TCP.

- **OpenVas:** Es una herramienta que permite instalación en el PC y se configura con el puerto 9392 y se le ingresa la IP a explorar y con la tarea específica a realizar con el objetivo de mostrar un informe con las vulnerabilidades que tiene el objetivo a atacar.

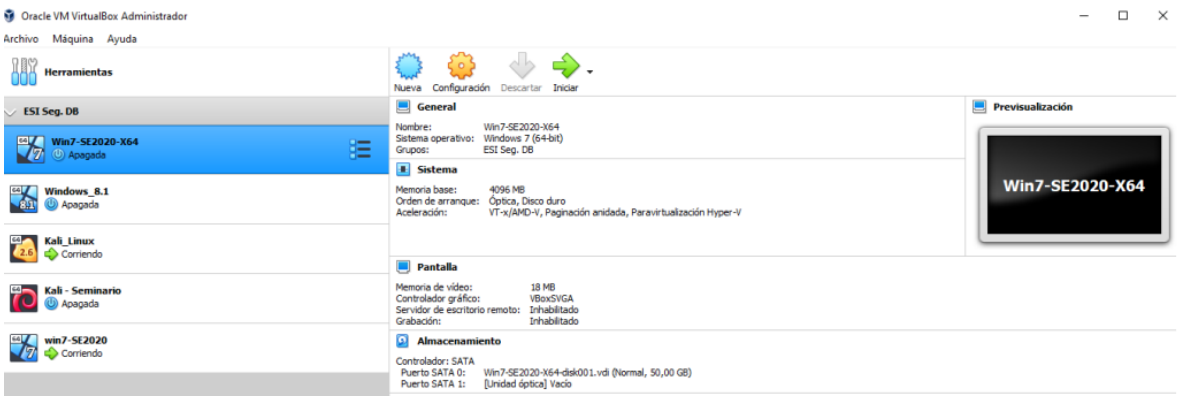
**Servicios en línea:**

- **ExploitDB:** La compañía Offensive Security creo la herramienta llamada ExploitDB que consiste en una base de datos que contiene Exploit públicos con el objeto de investigación, los Exploit almacenados en esta base de datos están listos para ser ejecutados y realizar pruebas de penetración, se puede encontrar en la siguiente url: https://www.exploit-db.com/

- **CVE:** sus siglas significan, Vulnerabilidades y Exposiciones Comunes. Consiste en una lista de vulnerabilidades informáticas registradas y cada una es identificada con un código CVE - ID con las características y propiedades lo que se traduce en el software afectad y también de las probables configuraciones y soluciones. El código CVE- ID es CVE-YYYY-NNNN. El número de vulnerabilidades es NNNN, el año de la vulnerabilidad es YYYY y CVE el formato de entrada.

## 2.4 Configuración banco de trabajo

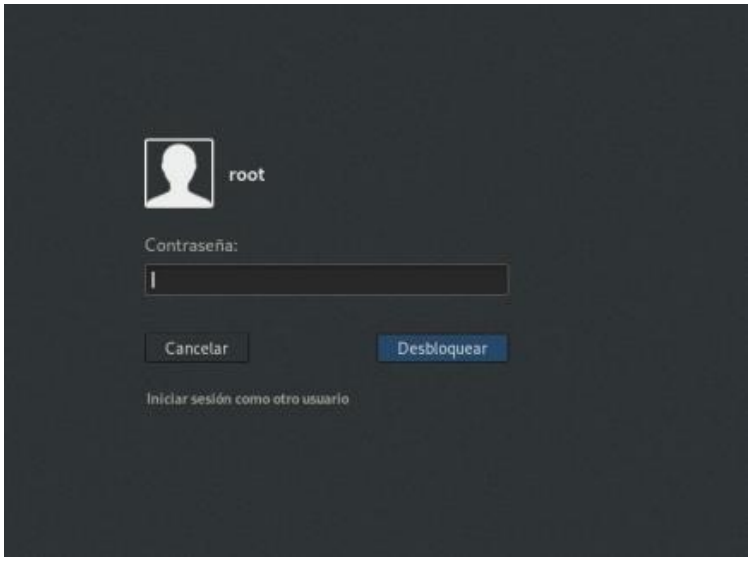
**Ilustración 1. Instalación Virtual Box**




**Fuente 1. Creación propia**

- Se hace instalación del sistema operativo Kali Linux-2019.3-amd64. Se procede a realizar la comunicación con el sistema operativo Windows 7, como se muestra en la ilustración 2.

**Ilustración 2. Ingreso al S.O Kali Linux**




**Fuente 2. Creación propia**

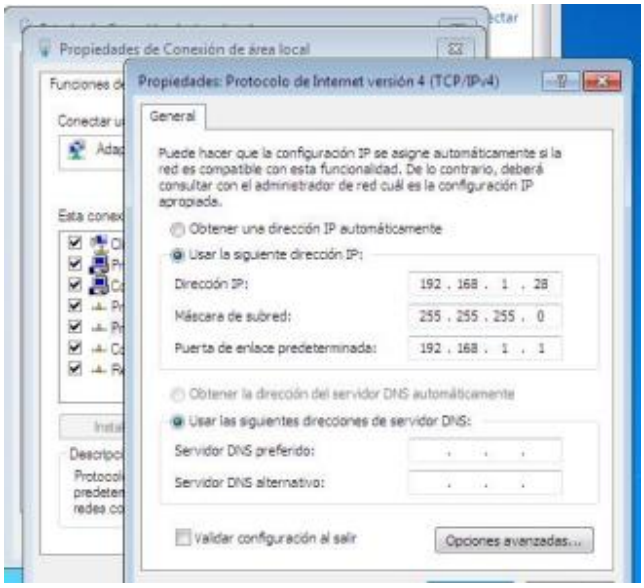
- Se procede a acceder a la configuración de Kali Linux y se configura la IP 192.168.1.27 . A continuación, se muestra en la ilustración 3.

**Ilustración 3. Configuración de IP 192.168.1.27 en tarjeta de red**


**Fuente 3. Creación propia**

- Se procede a encender el sistema operativo Windows 7 wind7-SE2020 y se configura dirección IP fija 192.168.1.28, como se muestra en la ilustración 4.

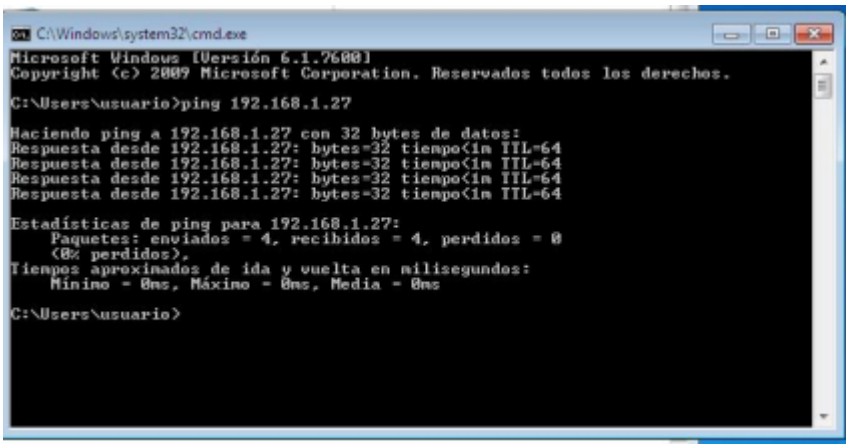
**Ilustración 4. Configuración IP 198.168.1.28 en S.O Win7**




**Fuente 4. Creación propia**

En la ilustración 5 se muestra cómo se procede a realizar ping para conocer la comunicación, inicialmente se hace desde Windows 7 y posteriormente desde Kali Linux.

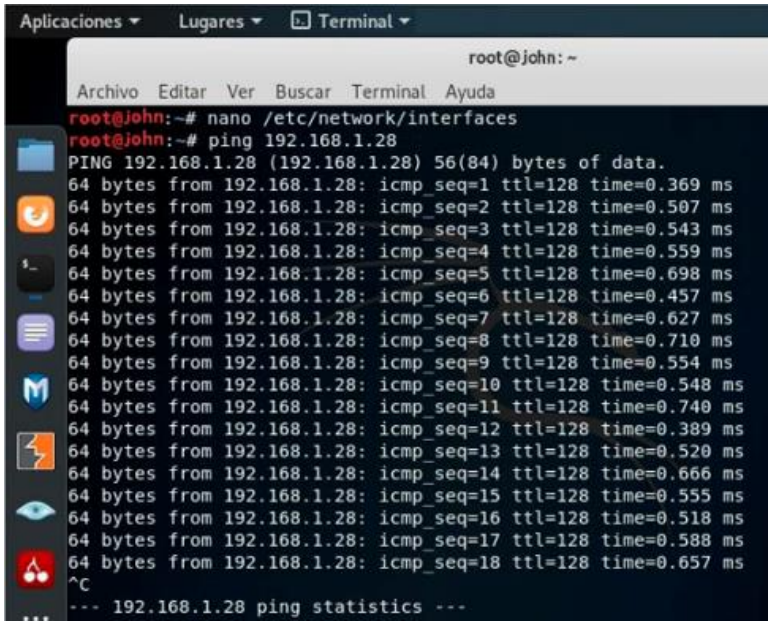
**Ilustración 5. Ping entre Win7 y Kali Linux**




**Fuente 5. Creación propia**

- Ahora se procede a realizar ping desde Kali Linux a Windows 7, se muestra en la ilustración 6.

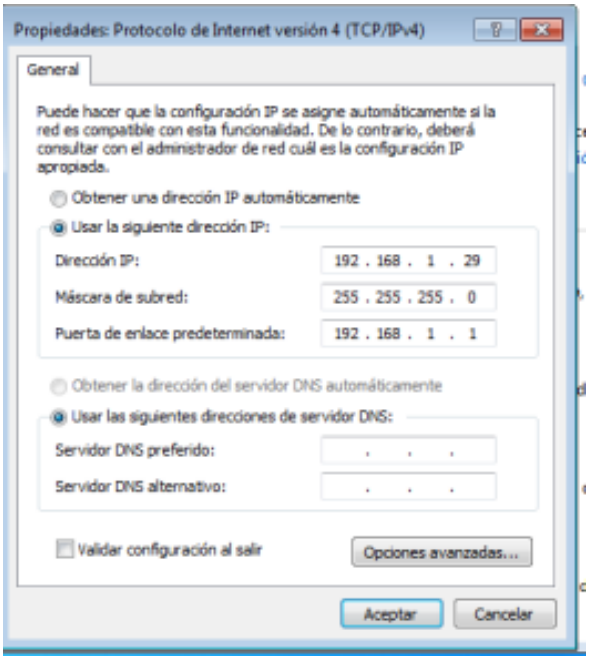
**Ilustración 6. Ping entre Linux y Win7**




**Fuente 6. Creación propia**

- Se enciende el segundo sistema operativo Win7-SE2020-X64 y se le configura la IP 192.168.1.29 , como se refleja en la ilustración 7.

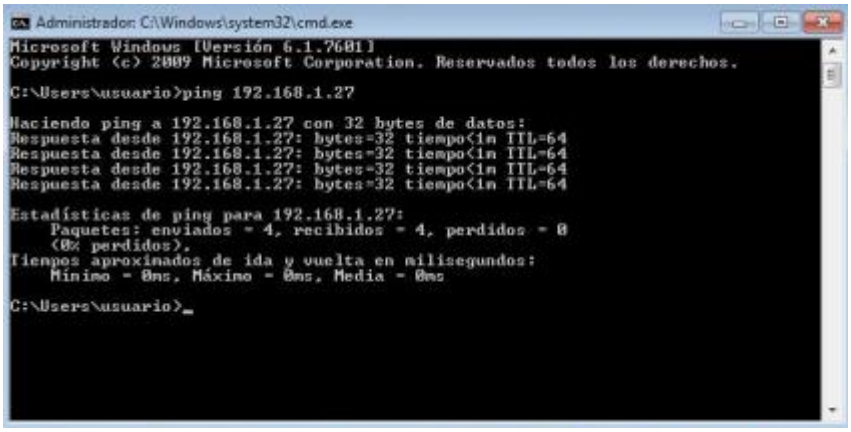
**Ilustración 7. Configuración IP 198.168.1.29 en S.O Win7**




**Fuente 7. Creación propia**

- Ahora se realiza la comprobación de comunicación entre Win7-SE2020-X64 y Kali Linux con ping y se muestra dicha comprobación en la ilustración 8.

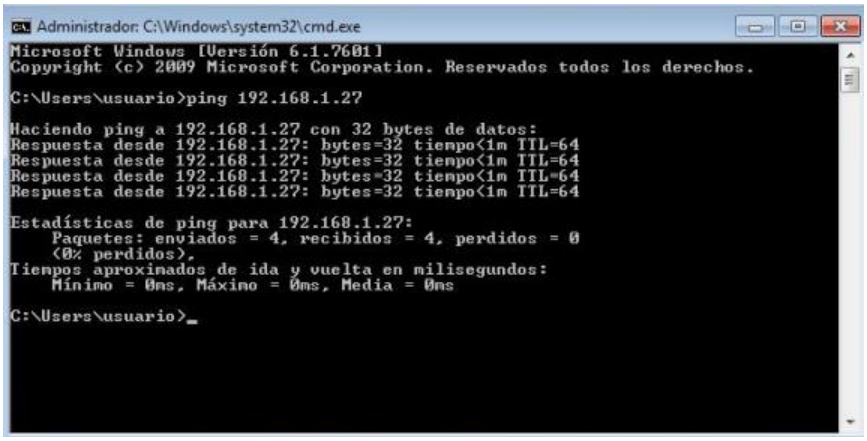
**Ilustración 8. Ping entre Win7 y Kali Linux**




**Fuente 8. Creación propia**

- Se comprueba que sí se establece conexión entre ambos sistemas operativos, no hay pérdida de paquetes en el ping, como se muestra en la ilustración 9.

**Ilustración 9. Ping entre Win7-SE2020-X64 y Kali Linux**




**Fuente 9. Creación propia**

- Se realizado ping entre los tres sistemas operativos dentro de la máquina virtual comprobando que el banco de trabajo ya se encuentra listo, como se visualiza en la siguiente ilustración 10.

## Características técnicas de hardware

**Ilustración 10. Características del hardware instalado**


**Fuente 10. Creación propia**

# 3 ACTUACIÓN ÉTICA Y LEGAL

## 3.1 Análisis de los del acuerdo anexo 3 – acuerdo y anexo 2 - escenario 2

Una vez leído y analizado ambos anexos se ha podido evidenciar procesos ilegales y no éticos que en virtud como profesional de la ingeniería y amparado por las leyes éticas colombianas de la entidad COPNIA[9] se procede a continuación, señalar los fragmentos en los cuales se considera hay ilegalidad:

- **Cláusula Primera. Objeto:** en virtud del presente **acuerdo de confidencialidad**, la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima o remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la **información confidencial** o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.

  **Argumento:** evidentemente la compañía Whitehouse Security al emitir este acuerdo de confidencialidad, busca evitar que el empleado que firme denuncie ante las autoridades competentes los procesos ilegales que la compañía realice; lo que levanta sospecha, porque la compañía es cómplice y oculta procesos, y esto puede desencadenar consecuencias legales para los empleados ante la justicia colombiana.

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

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

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

[9] COPNIA. República de Colombia. Código de Ética. [En línea]. Consultado: 20 de febrero de 2022. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

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

**Argumento:** en esta cláusula es claro cómo la compañía pretende que el profesional de ingeniería guarde silencio en y de cierto modo sea cómplice de las actividades delictivas de la compañía como es la violación a información confidencial y también como actos tan sensibles como lo son las chuzadas e interceptaciones ilegales, toda esta cláusula deja una mala percepción tanto para la compañía como para los empleados que firmen el acuerdo. En el literal 2 de la cláusula se nota una mala estructura del documento lo que genera inquietud que puede ser modificada o alterada al encontrarse un espacio considerable en el que se puede anexar información de manera posterior al ser firmada.

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

  **Argumento:** la cláusula es muy explícita en cuanto a que no importa el origen de la información y esto hace que se genere riesgos, porque no se sabe la procedencia de la misma, no se conoce qué tan vulnerable sea y es indispensable conocer tanto el origen de la información como el destino y uso que se le va a dar. Lo anterior genera un alto riesgo para el profesional involucrado en el proyecto.

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

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

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

**Argumento:** en el **ítem 3** la compañía Whitehouse Security busca que el empleado sea cómplice absoluto de los actos delictivos al no permitirle denunciar ante las autoridades las irregularidades que se hacen en la empresa.

En el **ítem 8** la compañía quiere involucrar directamente al empleado ante la autoridad competente, quiere que el empleado se eche todo los cargos y la compañía librarse de responsabilidades.

- **Cláusula Quinta. Obligaciones de la parte reveladora:** Son obligaciones de la parte reveladora:

  1. Mantener la reserva de la información confidencial hasta tanto adquiera el carácter de pública.

  **Argumento:** en esta cláusula también se encuentra una inconsistencia en la redacción y estructura de la misma, lo que genera suspicacia, porque no se sabe una vez firmado el documento qué otros textos le pueden agregar que involucre de manera negativa al empleado.

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

  **Argumento:** la compañía Whitehouse Security, busca en esta cláusula librarse de toda responsabilidad y dejar al empleado solo en su defensa en caso de ser detectados por la autoridad, se evidencia mucha falta de ética y nulo apoyo para el empleado que al firmar este acuerdo con esta cláusula no tendría ninguna garantía.

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

  **Argumento:** si el profesional firma es porque está de acuerdo de todos los delitos anteriores y consciente de las consecuencias a la que puede llegar, muy seguramente con esta cláusula la compañía pretende librarse de responsabilidades e involucrar directamente al empleado poniéndolo en alto riesgo de ir a prisión, tener multas considerables y con seguridad perder la licencia profesional.

### 3.2 Artículos de la ley 1273 que se podrían vulnerar en dicho acuerdo y especificación de porqué vulnera artículos de la ley 1273.

A continuación, se mencionan las cláusulas en las cuales se vulnera los artículos de la ley 1273 de 2009:

- **Cláusula Primera. Objeto:** en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima o remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.

**Los artículos vulnerados son el 269F y el 269H**

El artículo **269F de la ley 1273 de 2009,** es vulnerado por la compañía ampliamente y con esta cláusula está obligando al empelado a no denunciar y ser cómplice de todos los actos delictivos acarreándole al empleado graves consecuencias como lo dicta la ley: incurrirá en pena 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. [10]

El artículo **269H de la ley 1273 de 2009,** este artículo es vulnerado por la compañía, porque en calidad de tercero está manipulando información confidencial y privada sin autorización expresa del dueño de la misma, lo que incurre en un delito que como lo dice la misma ley acarrea prisión hasta por tres años e inhabilidad para ejercer la profesión. El empleado al firmar este acuerdo la compañía lo está obligando a guardar silencio y a no divulgar los delitos que se están cometiendo dentro de la compañía.

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

**Los artículos vulnerados son el 269C y el 269H**

En esta cláusula la compañía deja claro que se va a apropiar de información, va acceder sin autorización a sistemas de información, a realizar interceptación de datos sin ninguna autorización y la ley es clara al afirmar que incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. También el empleado quedará inhabilitado para ejercer su profesión hasta por tres años.

[10] CONGRESO DE COLOMBIA. Ley 1273 de 2009. [En línea]. [Consultado: 16 de febrero de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- **Cláusula Tercera. Origen de la información confidencial**

**Los artículos vulnerados son el 269I y el 269H**

La compañía en esta cláusula vulnera los artículos anteriormente mencionados, porque realiza manipulación de la información de un tercero sin su consentimiento por medio de herramientas informáticas hurtando también su información personal al receptar sus datos personales en los procesos de selección.

- **Cláusula Cuarta. Obligaciones de la parte receptora**

**Los artículos vulnerados son. 269A, 269C, 269F y 269H**

Se vulnera el artículo 269A porque en la cláusula se hace referencia a la receptación de información y espionaje

Se vulnera el artículo 269C, porque en la cláusula se menciona la interceptación de información.

Se vulnera el artículo 269F, porque la cláusula hace alusión la violación de información tanto personal como empresarial.

Se vulnera el artículo 269H, porque la compañía trabaja con herramientas informáticas, capta información sin autorización y saca provecho ampliamente de ella.

En el empleado se ve directamente implicado en la vulneración de estos artículos los cuales siempre hacen el llamado a abstenerse de manipular información y hurtar la misma y a su vez al firmar este tipo de acuerdos con esta cláusula está siendo cómplice al no poder denunciar.

### 3.3 ¿Aplicaría a este trabajo en The Whitehouse?

A pesar de que la oferta laboral es muy atractiva en cuanto al salario y el tipo de contrato vitalicio, es muy evidente que se va a realizar una labor delictiva lo que a la final se tendría graves consecuencias como ir a prisión y, perder la licencia profesional. En efecto, no se justifica de ninguna manera aceptar este tipo de empleo que solo generará consecuencias nefastas, no tiene justificación ganar mucho dinero hoy y tener que pasar necesidades mañana y, además atentar contra la vulnerabilidad y privacidad de las personas, es algo que no está dentro la ética personal ni profesional y más aun conociendo las leyes que existen y las consecuencias a las hay que atenerse si se vulneran. Hay que ser consecuentes con el código de ética de la entidad COPNIA.

**Argumento:**

El acuerdo de confidencialidad interpuesto por la compañía Whitehouse Security, vulnera ampliamente varios artículos del código de ética de COPNIA quien es la entidad que regula los actos de los profesionales de las ingenierías TICs.

El código de ética de COPNIA es muy claro en varios de sus artículos, entre ellos se tiene los siguientes:

- **Artículo 31 en el literal f:** habla de utilizar y ocultar información de manera incorrecta y a su vez no denunciar las faltas que se comentan contra el mismo código.

- **Artículo 32 en el literal b**: en el código se prohíbe aceptar prebendas a cambio de actos delictivos que van en contra del miso código de ética de COPNIA.

- **Artículo 34 en el literal a:** en este ítem el código es muy claro al prohibir aceptar u ofrecer empleo que van en contra de las disposiciones legales o aceptar labores que excede la competencia que le otorga el título.

- **Artículo 35 en el literal b:** el artículo hace referencia a respetar las disposiciones legales y reglamentarias e incidan en la profesión y al mismo tiempo a denunciarlas.

- **Artículo 38 en el literal a**: el código en este artículo prohíbe material propio un tercero sin autorización.

- **Artículo 53 en el literal e:** en este literal el código COPNIA hace referencia a las faltas gravísimas como incurrir en algún delito que atente contra los clientes o las autoridades.

## 3.4 Noticia del caso Operación Andrómeda Buggly

Con total claridad la operación que pretendía realizar el ejército fue un gran fracaso, porque no tuvo autorización y mucho menos planeación, la operación vino a tener supervisión una vez fue descubierta y claramente se violaron todos los códigos de ética tanto de la informática como del ejército colombiano mismo. El ejército de esto no sacó ninguna ganancia y fue una batalla silenciosa que perdió, tal vez por inexperiencia, tal vez por ingenuos o porque quizá el ejército está altamente entrenado para un campo de batalla y no para una guerra cibernética.

La operación Andrómeda es un claro ejemplo que un país como Colombia no está preparado como debería para el mundo cibernético y hay muchos baches como leyes y personal altamente calificado para manera este tipo de operaciones, es así

como desde los entes académicos y gubernamentales se debe hacer mayor énfasis y apoyo a el crecimiento del entorno digital, que se puedan apropiar del tema y le den un impulso importante, porque la tecnología cada día crece más y sin lugar a dudas es una forma de defensa y a su vez una forma de crecimiento económico.

En la operación Andrómeda se violó el código de ética de CONPIA de 2015 de la ley 842 de 2013 y la ley 1581 de 2012,[11] porque se hizo todo lo contrario a lo que ordena y prohíbe el código. El código es muy claro al prohibir **el espionaje**, al prohibir la **manipulación y alteración de la información**, pero sobretodo el código hace gran énfasis en **actuar con responsabilidad, honestidad y basados siempre en la ley.**

# 4 EJECUCIÓN PRUEBAS DE INTRUSIÓN

## 4.1 Descripción específica de las herramientas y software empleado para llevar a cabo el caso del anexo 4 – escenario 3 enfocado a Redteam.

Las herramientas empleadas para llevar a cabo el caso del anexo 4 - escenario 3 fueron las siguientes:

- **Kali Linux:** en este sistema operativo instalado en la máquina Virtual Box fuer donde hizo el efectuó el ataque a la máquina instalada de Windows 7 X64

- **Metasploit:** esta herramienta fue empleada para realizar el ataque a la máquina Win7 X64 y con la que se pudo encontrar las vulnerabilidades de dicho sistema operativo.

- **Nmap:** con esta herramienta se hizo el escaneo de puertos en el sistema operativo Windows 7 y se pudo encontrar la vulnerabilidad para poderla atacar específicamente por el puerto TPC 80, es decir se identificó que para poderlo atacar se puede hacer vía web.

- **Rejetto v.2.3:** programa que se identificó que es el que producía la pérdida de información.

[11] MINTIC. Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

## 4.2 Lista y descripción de los datos e información del anexo 4 – escenario 3 que fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 7 x64

- **Fuga de información:** la primicia que informe el caso que al interior de la compañía se presenta una fuga de información en una de sus máquinas.

- **Aplicación rejetto v.2.3:** esta aplicación según informa el ejercicio se encuentra instalada en el sistema operativo Windows 7 X64 justamente donde se presenta la fuga de información. La aplicación rejetto v.2.3. es una aplicación de tipo servidor web conocida como un HTTP y es empleada para compartir archivos masivos, pero para este caso presenta una vulnerabilidad que al realizar el ejercicio es identificada.

- **Exploit:** la actividad menciona que la aplicación presuntamente tiene adherido un exploit que puede finalizar en una Shell[12] reversa y a su vez tiene abierta una sesión meterpreter.

- **Escalamiento de privilegios:** la actividad conlleva a que la investigación indague sobre la creación de un usuario administrador del sistema que conlleve a un escalamiento de privilegios.

## 4.3 ¿Qué herramientas se utilizó para poder identificar los fallos de seguridad de la máquina Windows 7 ? * ¿qué puerto abre la aplicación específica en el anexo?

- Con la herramienta **ipconfig** se identifica la ip de la máquina victima que para este caso es la IP: 192.168.1.23

- Con la herramienta **netstad** se identifica los puertos que están abiertos y que se encuentran en estado **LISTENING.**

- Al emplear la herramienta Nmap se identifica los servicios que la máquina tiene corriendo y a su vez el puerto por donde se puede atacar.

- La aplicación **rejetto v.2.3** tiene abierto el puerto **80**

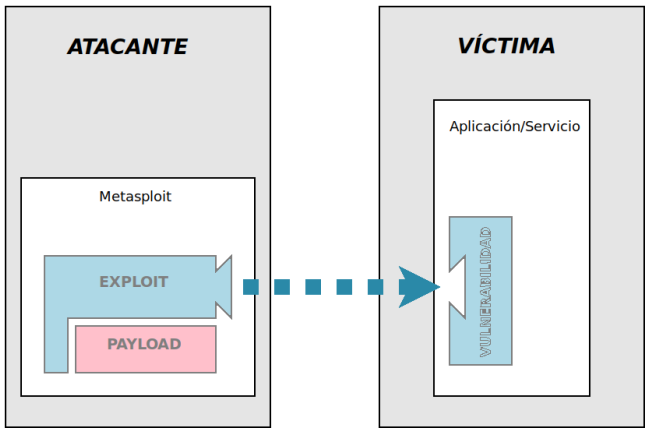
[12] DESDE LINUX.NET. ¿Qué es un Shell? [En línea]. Consultado: 2 de marzo de 2022. Disponible en: https://blog.desdelinux.net/que-es-un-shell/

## 4.4 Explicación con mis propias palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 x64) Se emplea gráficos para explicar el ataque.

La máquina Windows 7 x64 ha sido explotada por medio de herramientas de pentesting[13] lo que ha dejado al descubierto la vulnerabilidad que presenta y por ende se ha identificado la fuga de información de la que se habla en el ejercicio. En efecto ha sido fácil atacar a la máquina víctima, porque el firewall está desactualizado y no pudo identificar el ataque para detenerlo, muy seguramente por lo que el sistema operativo Windows 7 x64 ya no cuenta con parches de seguridad actualizados, es un software que ha dejado de ser actualizado y por parte de su fabricante, desde el 14 de enero de 2020 como lo anunció Microsoft[14].

Por otro lado, al tener la máquina víctima instalada la aplicación **rejetto v.2.3** con el puerto 80 abierto hace que sea muy vulnerable y permita hacer un exploit[15] de manera remota desde el sistema operativo Kali Linux y como lo muestra de manera gráfica la siguiente ilustración 11.

**Ilustración 11. Explotación de vulnerabilidades con Metasploit**




**Fuente 11. https://ccia.esei.uvigo.es/docencia/SSI/1819/practicas/ejercicio-metasploit/**

[13] CAMPUSCIBERSEGURIDAD. ¿Qué es el Pentesting? [En línea]. Consultado: 2 de marzo de 2022. Disponible: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

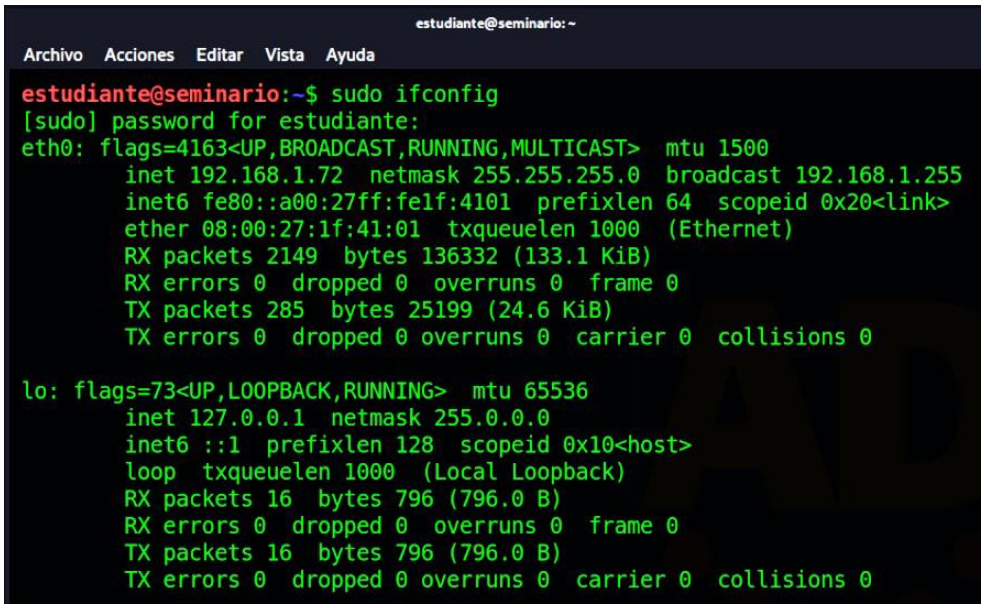
[14] MICROSOFT. Soporte técnico de Windows. [En línea]. Consultado: 4 de marzo de 202. Disponible en: https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finaliz%C3%B3-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962

[15] PANDA. ¿Qué es un Exploit? [En línea]. Consultado: 2 de marzo de 2022. Disponible en:https://www.pandasecurity.com/es/security-info/exploit/

## 4.5 Documentación de cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

- Se realiza la consulta de la dirección IP que tiene instalada la máquina Kali Linux que está alojada en el banco de datos y se identifica la IP: 192.168.1.72 como se muestra en la siguiente ilustración, como se ve en la ilustración 12.

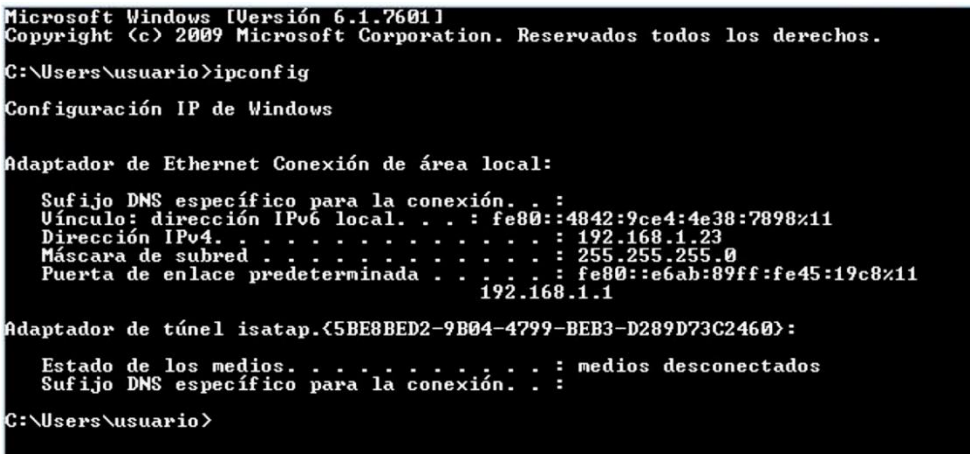
**Ilustración 12. Consulta de IP en Kali Linux**




**Fuente 12. Creación propia**

- Se consulta la dirección IP del sistema operativo Windows 7 x64 y de identifica la IP: 192.168.1.23

**Ilustración 13. Consulta de IP en Windows 7 x64**




**Fuente 13. Creación propia**

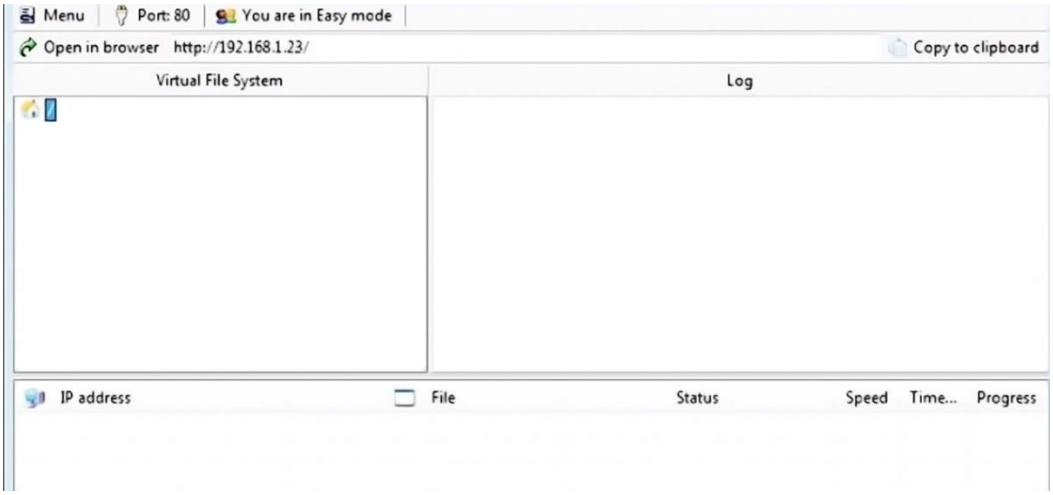
- Una vez instalado Kali Linux y Window 7 x64 y establecida la comunicación entre las dos máquinas, se procede a realizar la instalación de la aplicación rejetto v.2.3 con el objetivo de experimentar lo que dice la actividad y encontrar el punto de fuga de información, como se muestra en la ilustración 14.

**Ilustración 14. Descarga de aplicación rejetto v.2.3**


**Fuente 14. https://www.download3k.es/Red/Intercambio-de-Archivos/Download-HFS-HTTP-File-Server.html**

- Se realiza instalación de aplicación rejetto v.2.3

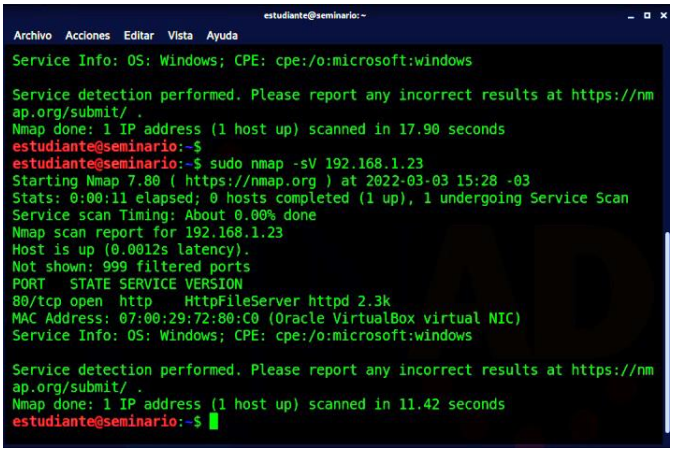
Ilustración 15. Aplicación rejetto v.2.3 en Window 7 x64




**Fuente 15. Creación propia**

- A través de la herramienta Nmap[16] de Kali Linux se hace el escaneo de puertos hacia la máquina víctima Windows 7 x64 por medio de la dirección IP: 192.168.1.23 como se ve en la ilustración 16.

**Ilustración 16. Escaneo de puertos con Nmap desde Kali Linux a Wn x64**



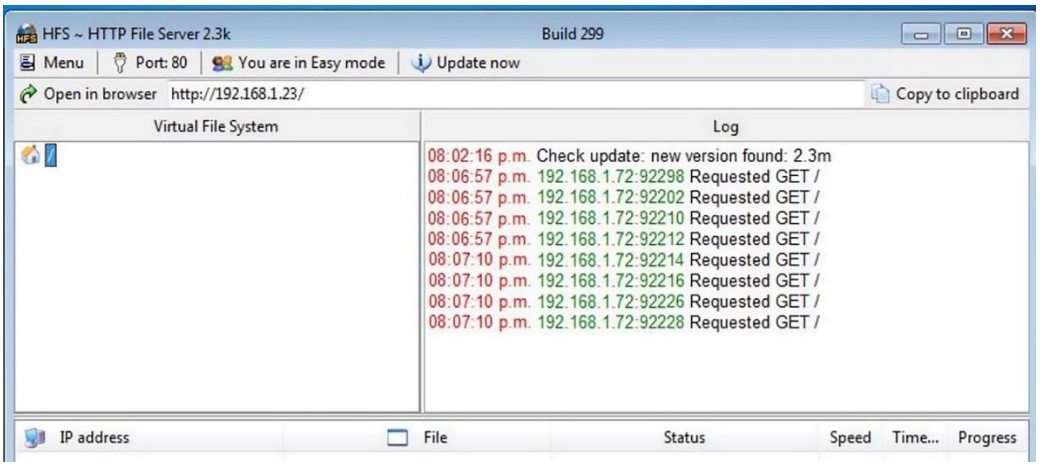

**Fuente 16. Creación propia**

[16] MARIN DE LA FUENTE. ¿ Qué es Nmap? Por qué necesitas este mapeador de red . Consultado: 3 de marzo de 2022. Disponible en: https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/

- Al realizar el escaneo con la herramienta Nmap en Windows se identifica una vulnerabilidad con HttpFileServer 2.3K lo que permite tener abierto el puerto 80 TCP.

- Se efectúa la aplicación rejetto v.2.3 ya instalada en Kali Linux y se hace el análisis de Windows 7 x64 con la dirección IP: 192.168.1.23 como se ve reflejado en la ilustración 17.

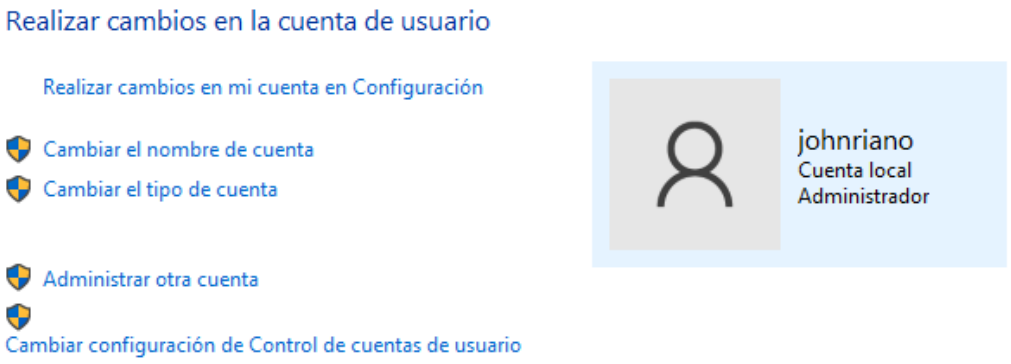
**Ilustración 17. Ejecución de la aplicación rejetto v. 2.3 con la IP 192.168.1.23 en Win 7 x64**




**Fuente 17. Creación propia**

- Se crea un usuario administrador en Windows 7 x64 con el propósito de comprobar la vulnerabilidad y hacer el exploit. También se crea una cuenta distinta a la mía en Kali Linux con mi primer nombre y mi primer apellido: johnriano, como se muestra en la ilustración 18.

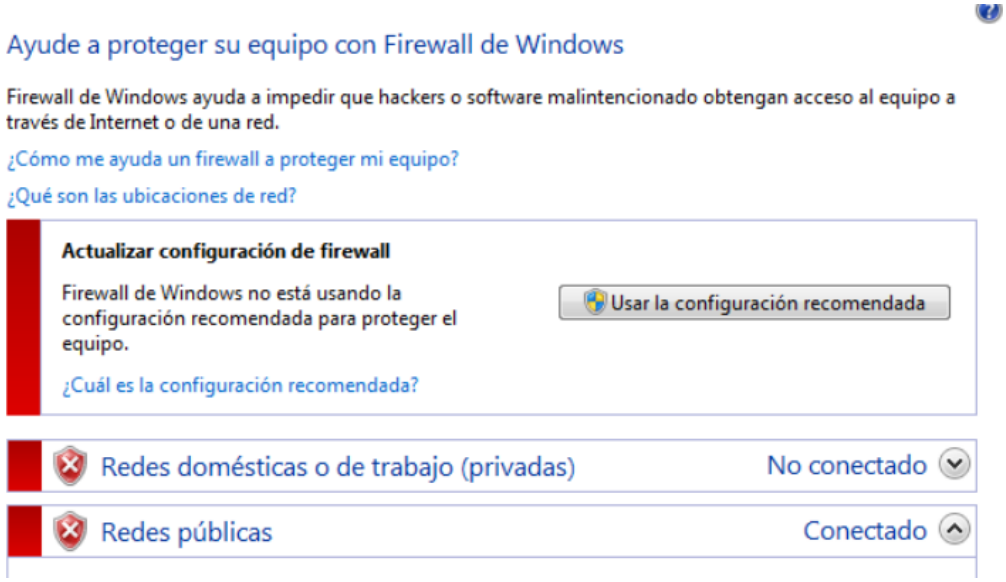
**Ilustración 18. Creación de usuario admin en Win 7 x64**




**Fuente 18. Creación propia**

- Se procede a desactiva el firewall de Windows 7 x64, como se ve en la ilustración 19.

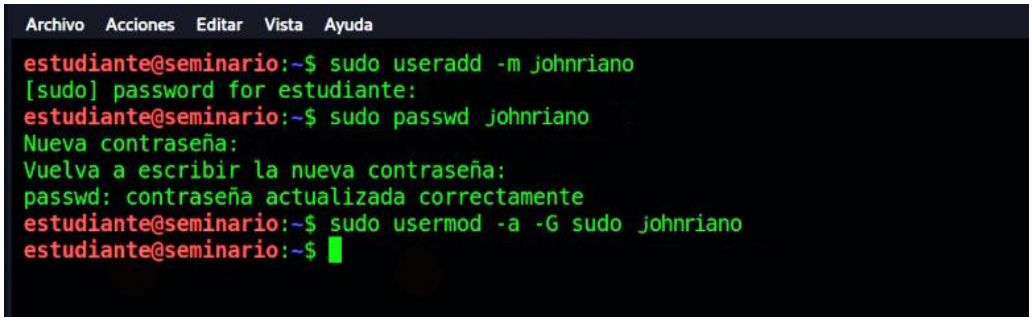
  Ilustración 19. Desactivación de firewall en Win 7 x64




**Fuente 19. Creación propia**

- Ahora en Kali Linux también se crea una cuenta con primer nombre y apellido: johnriano y se ve reflejado en la ilustración 20.

**Ilustración 20. Creación de cuenta johnriano en Kali Linux**




**Fuente 20. Creación propia**

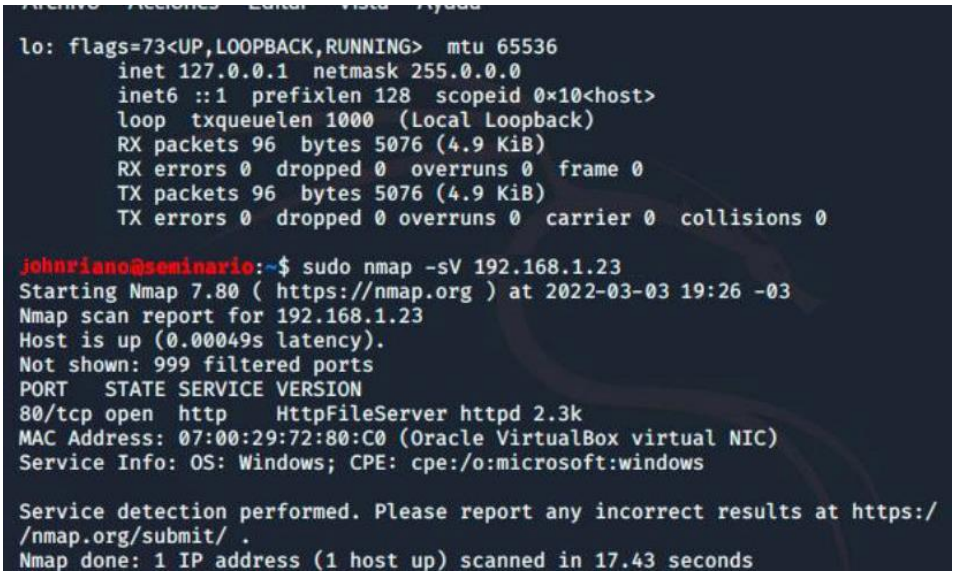
- Se crea el usuario en Kali Linux con privilegios de administrador con el comando sudo o usermod -a -G sudo johnriano. A su vez el usuario johnriano es agregado a la Shell para que sea visible en la terminal con el siguiente comando de Kali Linux: chsh -s /bin/bash johnriano, como se muestra en la ilustración 21.

**Ilustración 21. Asignación de privilegios de admin al usuario johnriano en Kali Linux**


**Fuente 21. Creación propia**

- Desde el usuario johnriano, se realiza escaneo de la máquina víctima con Nmap con el objetivo de encontrar la vulnerabilidad del programa HttpFileServer 2.3K, como se muestra a continuación en la ilustración 22.

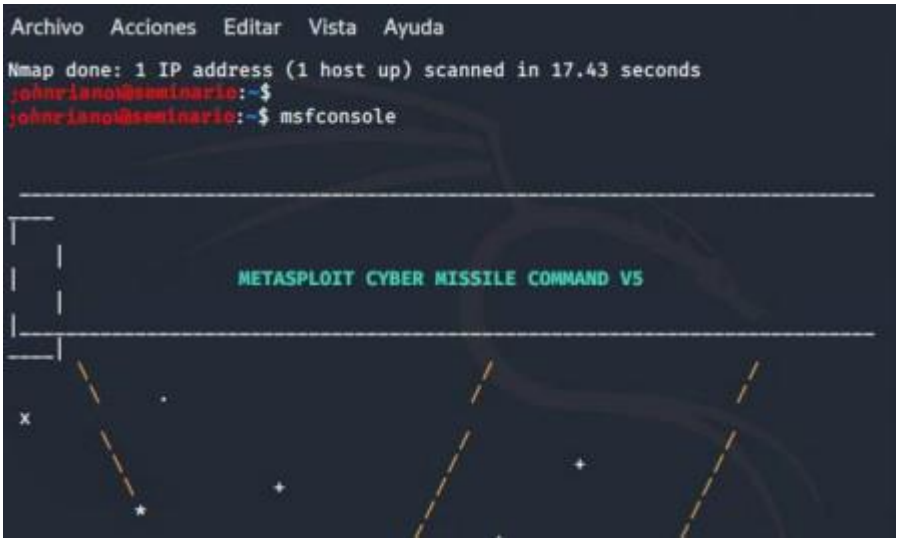
**Ilustración 22. Escaneo de puertos con Nmap desde el usuario johnriano**




**Fuente 22. Creación propia**

- Ahora con Metasploit se ingresa a la consola y se hace la explotación de la vulnerabilidad por medio del comando msfconsole, como se muestra en la ilustración 23

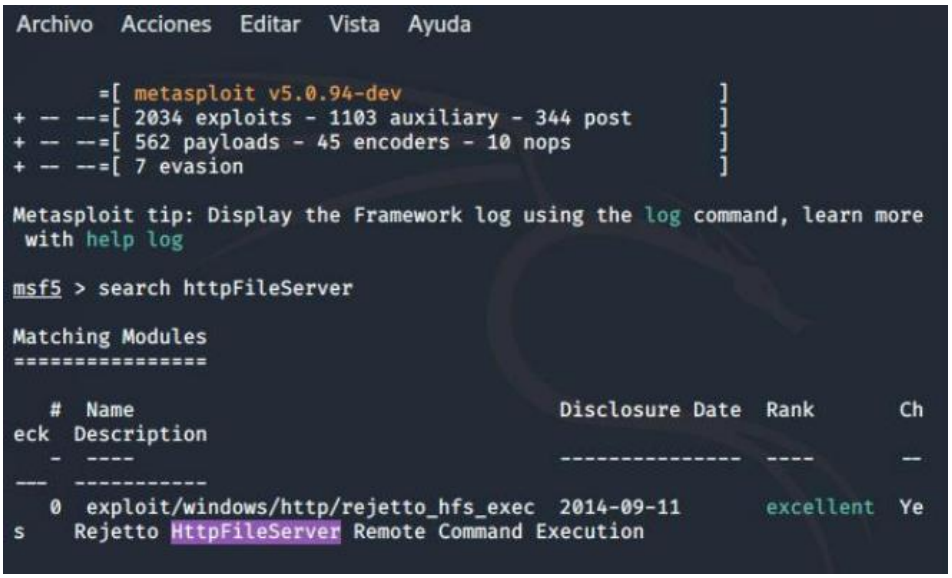
**Ilustración 23. Ingreso a la consola con el comando msfconsole**




**Fuente 23. Creación propia**

- En el Metasploit se realiza la búsqueda de la vulnerabilidad con el siguiente comando: search httpFileServer, como se visualiza en la siguiente ilustración 24.

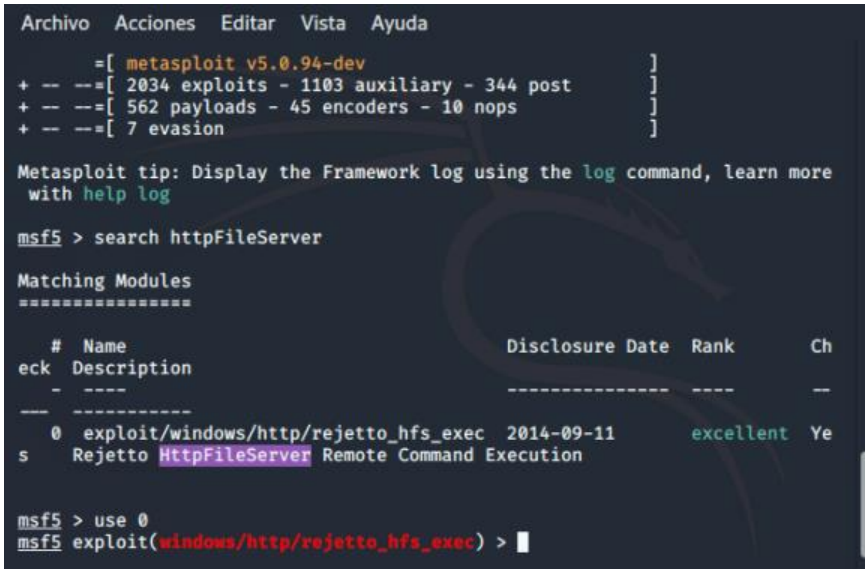
**Ilustración 24. Búsqueda de vulnerabilidad con Metasploit**




**Fuente 24. Creación propia**

- El módulo donde se debe hacer el exploit es el 0 entonces se procede a ejecutar el comando use 0 para ingresar a él, como se muestra en la ilustración 25.

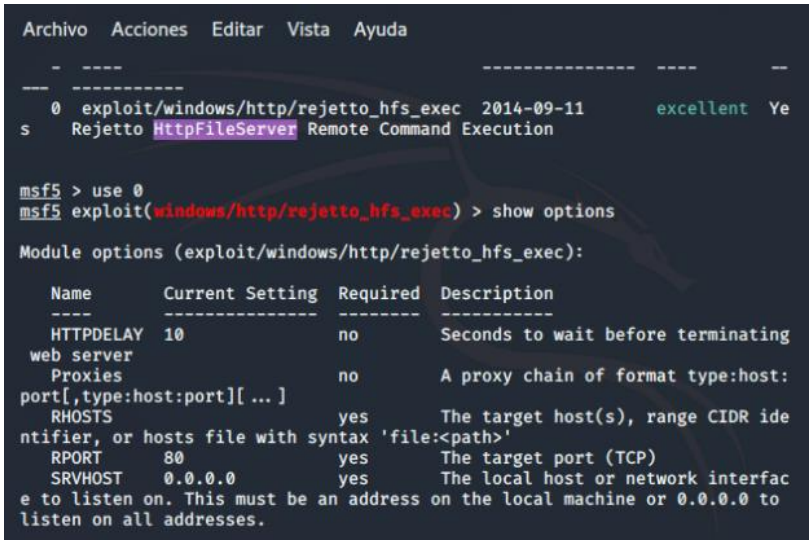
**Ilustración 25. Detección de la herramienta rejetto v. 2.3**




**Fuente 25. Creación propia**

- Con el comando show options se escoge la variable dentro del Metasploit, como se observa en la ilustración 26.

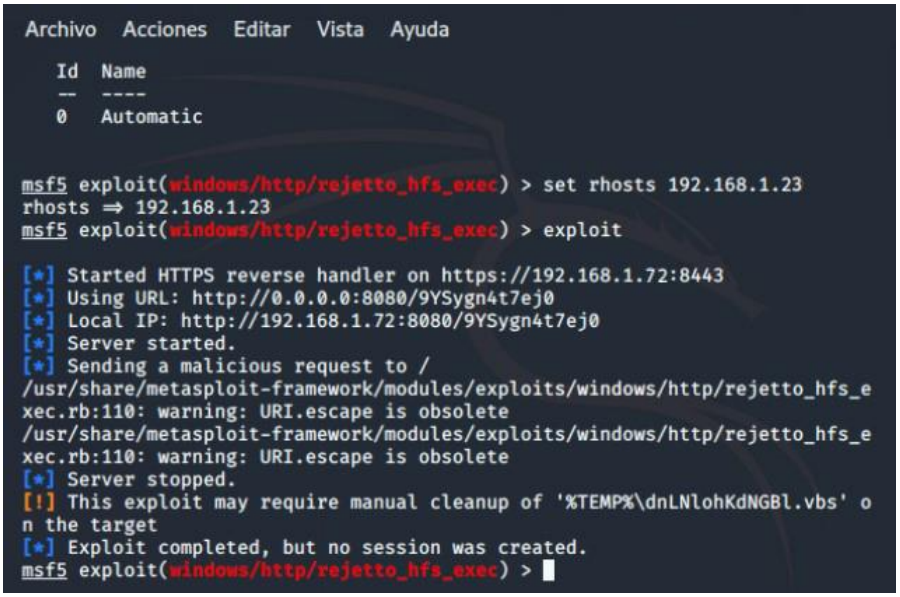
**Ilustración 26. Variables en Metasploit**




**Fuente 26. Creación propia**

- Con el comando **set rhosts** se realiza el ataque apuntando a la dirección IP del Window x64, la IP 192.168.1.23 entonces se ejecuta así: set rhosts **192.168.1.23**, como se muestra en la ilustración 27.

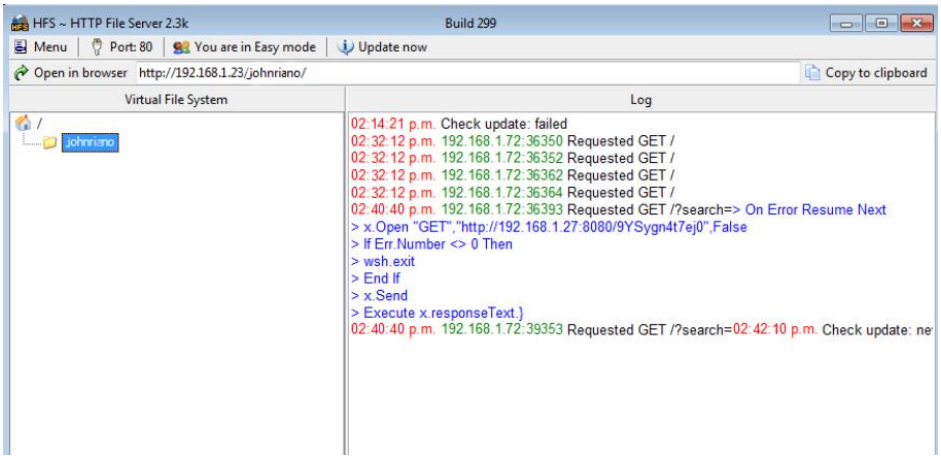
**Ilustración 27. Explotando la vulnerabilidad**




**Fuente 27. Creación propia**

- Ahora en la máquina víctima Windows 7 x64 donde está alojado el programa HttpFileServer se visualiza el ataque efectuado desde la máquina Kali Linux, como se visualiza a continuación en la ilustración 28.

**Ilustración 28. Explotación de vulnerabilidad en Win7 x64 desde Kali Linux**




**Fuente 28. Creación propia**

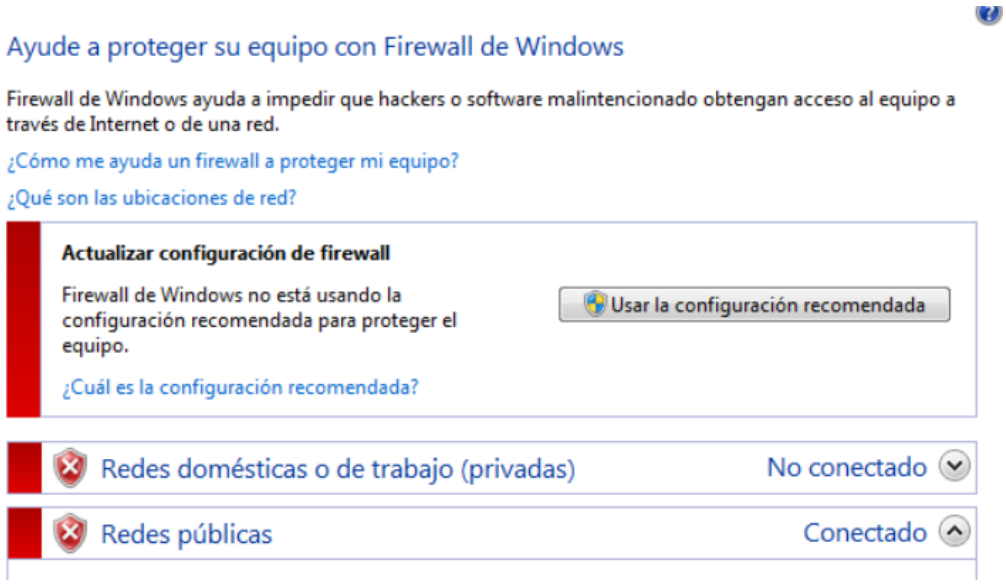
- Con este último proceso se comprobó que se logró ingresar de manera remota desde Kali Linux a Win 7 x64 por medio del sploit y se conoció la vulnerabilidad que hay en el puerto 80.

# 5 CONTENCIÓN DE ATAQUES INFORMÁTICOS

## 5.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

- Como primera medida es realizar la contextualización de qué tipo de ataque se está presentando y qué activos digitales está impactando, de manera inmediata por prevención verificar que el antivirus y el firewall estén activados en la máquina Windows 7 x64 teniendo en cuenta que en la etapa anterior se había desactivado, como se muestra en la ilustración 29.

**Ilustración 29. Firewall desactivado en Win 7 x64**



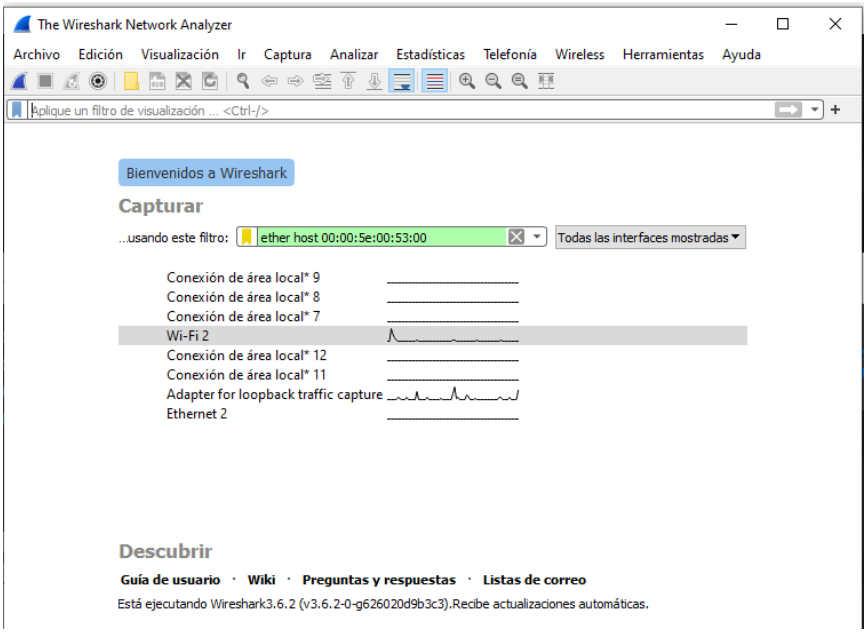

**Fuente 29. Creación propia**

- Como segunda opción generar la alerta con el equipo Red Team[17] y recoger información de las vulnerabilidades que tiene la red.

[17] CORE SECURITY. Red Team. [Online]. Consulted: March 19, 2022. Available in: https://www.coresecurity.com/penetration-testing/red-team

- Como tercer paso empleo la herramienta Wireshark la cual me va permitir realizar un escaneo completo de la red y me mostrará por dónde se está presentando fuga de información y la actividad específica que esté realizando cada computador.[18]

**Ilustración 30. Herramienta Wireshark realizando sniffer**




**Fuente 30. Creación propia**

- Al tener el escaneo completo de las máquinas se tiene un panorama completo de lo que está pasando y se puede identificar el tipo de ataque que se está presentando.

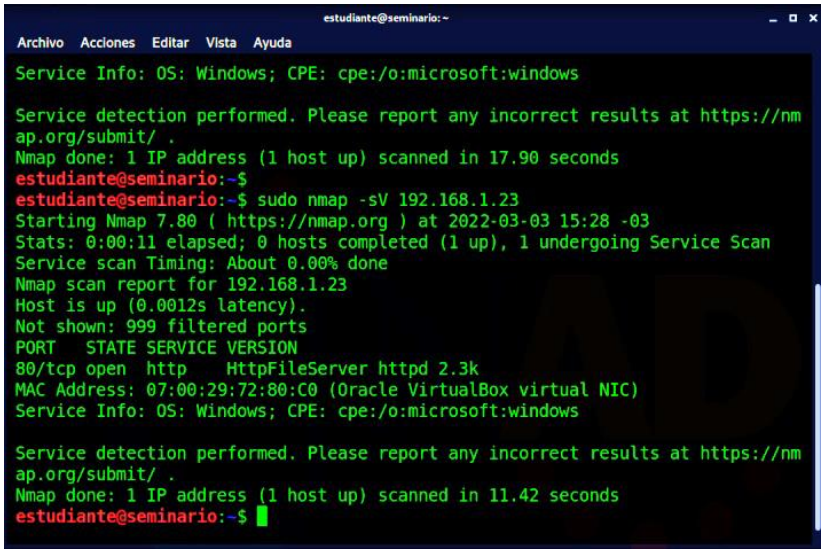
- También con la herramienta Nmap se realiza una revisión de los puertos que se encuentren abiertos y procede a cerrarlos en caso de encontrarlos.

- Se activa el Firewall y antivirus y, se realiza un escaneo completo.

- Por último, se procede a actualizar los últimos parches de seguridad del sistema operativo Windows 7 x64 bits, como se muestra a continuación en la ilustración 31.

[18] REYDES. Herramientas para Esnifar la Red y Analizar Paquetes. [En línea]. Consultado: 13 de marzo de 2022. Disponible en: http://www.reydes.com/d/?q=Herramientas_para_Esnifar_la_Red_y_Analizar_Paquetes

**Ilustración 31. Escaneo de puertos con Nmap desde Kali Linux a Wn x64**




**Fuente 31. Creación propia**

## 5.2 ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de red team qué medidas de hardenización propondría para que el ataque no se repita?

- Instalación más segura del sistema operativo: al momento de realizar la instalación realizar particiones del disco duro, en una partición dejar el sistema operativo y programas, en la otra partición para almacenar información.

- Configuración de todas las actualizaciones automáticas del sistema operativo para que reciba de manera permanente las últimas versiones de los parches de seguridad enviado por el proveedor del sistema operativo que para este caso es Microsoft.

- Instalación de software de alta protección como lo son los Antispyware, filtros Antispam y Antivirus

- Establecer medidas robustas de seguridad como al crear los usuarios de acceso que tengan contraseñas más encriptadas y con fecha de vencimiento de manera más frecuente.

- Emplear un sistema para cifrado de archivos y carpetas propias del sistema operativo y del almacenamiento de datos.

## 5.3 Diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos.

El equipo Blue Team[19] es un grupo de personas expertas en Ciberseguridad encargadas de analizar el comportamiento de una red informática y a su vez el uso que los usuarios le dan a los sistemas informáticos dentro de una empresa y de esta forma encontrar vulnerabilidades en los sistemas. El equipo Blueteam desempeñan su labor desde adentro de la compañía y están pendientes todo el tiempo de los ataques que puedan ocurrir desde la parte externa de la organización.

Los equipos de respuesta a incidentes informáticos son los encargados de recibir los informes de las vulnerabilidades de la seguridad de la red informática y hace la respuesta a las amenazas que surgen en la red, también está compuesto por un grupo de personas especializadas en seguridad informática.

## 5.4 ¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS Center For Internet Security usted lo utilizaría para qué fin?

Teniendo en cuenta que el Center for Internet Security ( CIS ), es una organización que tiene como fin hacer del mundo un lugar conectado de manera más segura y, en donde dan recomendaciones y establecen protocolos como mejores prácticas de protección de la seguridad informática; sin lugar a dudas se debe emplear, porque genera garantías y buen soporte; además se tiene muy buena documentación y está respaldado por una organización seria que lleva más de 20 años funcionando[20].

## 5.5 Funciones y características principales de lo que es un SIEM.

Los sistemas llamados SIEM son una herramienta fundamental para brindarle a las compañías una respuesta inmediata en caso de presentarse un ciberataque. Esto sistemas les permite a las empresas tener todo el control para detectar de manera temprana cualquier comportamiento sospechoso y poder actuar de forma más efectiva. Como principal venta de un sistema SIEM es poder minimizar o en su defecto evitar las consecuencias de un ataque, ya que con esta herramienta se realiza un análisis completo de toda la red informática de la compañía, revisando las vulnerabilidades, las licencias y en general todos los activos digitales de la

[19] INVICTI. Red Team Vs Blue Team Testing for Cybersecurity. Consulted: March 18, 2022. Available in: https://www.invicti.com/blog/websecurity/red-team-vs-blue-team/

[20] MANAGEENGINE. ¿Qué son los controles de CIS? [En línea]. Consultado: 13 de marzo de 2022. Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

organización y de esta manera poder tener un amplio margen de respuesta para evitar incidentes informáticos.[21]

**Características principales de un sistema SIEM:**

- **Genera capacidad de respuesta inmediata en tiempo real:** el SIEM[22] busca la respuesta más rápida efectuando un seguimiento en tiempo real de todos los comportamientos sospechosos dentro de la red informática.

- **Crea una base de conocimiento:** la herramienta realiza la documentación y el registro de todos los incidentes y comportamientos dentro de la red, de esta manera se logra construir una base de conocimientos para tener suficiente documentación en futuros incidentes.

- **Reduce al máximo los costos:** La herramienta permite hacer automatización de procesos con lo que se logra la optimización de los recursos tanto técnicos como humanos.

- **Mejora la gestión de los recursos:** Con la herramienta se logra mejor aprovechamiento de los recursos y activos digitales para la compañía, lo que representa garantía a la hora de atender incidentes informáticos.

**Herramientas más empleadas por un SIEM:**

- **IBM Security QRadar:** Este programa es uno de los más completos que hay en el mercado, ya que cuenta con más de 400 módulos capaces de soportar grandes cargas.

- **McAfee Enterprise Security Manager:** Con software la compañía logra monitorizar, analizar y recopilar incidentes de seguridad creando una data histórica para poder detectar y contrarrestar indecentes de una manera mucho más eficaz e inteligente.[23]

[21] AMBIT-BST. ¿Qué significa SIEM y cómo funciona? [En línea]. Consultado: 13 de marzo de 2022. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

[22] LOGRHYTHM.SIAM. Consulted: March 20, 2022. Available in: https://logrhythm.com/solutions/security/siem/

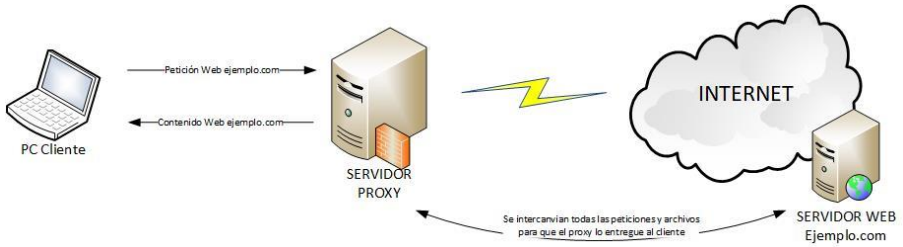
[23] AMBIT-BST. Cuáles son las herramientas SIEM más utilizadas [En línea]. Consultado: 13 de marzo de 2022. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

- **LogRhythm:** Esta herramienta es para compañías que no tienen la capacidad económica para contratar herramientas más robustas y avanzadas.

## 5.6 Herramientas de contención de ataques informáticos hardware o software

- **Servidor proxy:** Este dispositivo actúa como intermediario entre la red informática y la internet, lo que permite hacer un filtro de los paquetes de datos que llegan desde la parte externa de la compañía y también de los que salen, con esta herramienta se puede bloquear sitios web peligrosos o prohibidos en el ámbito laboral, como se describe en la siguiente ilustración 32.

**Ilustración 32. Servidor proxy**




**Fuente 32. Creación propia**

- **Cifrado de punto final:** Lo que se hace es un proceso de codificación de la información para quienes no tengan la contraseña asignada a cada archivo no tenga acceso a ella y también permite que el sistema operativo esté protegido de instalación de software malicioso y bloquee los archivos almacenados en otros computadores o servidores de punto final.

- **Firewall perimetral de red:** esta herramienta se encarga de hacer constante escaneo a la información que llega en paquetes a la red y genera un bloqueo de acuerdo a las reglas que se le ha configurado previamente, a continuación, se describe en la ilustración 33.

**Ilustración 33. Firewall**

**Fuente 33.** https://conceptoabc.com/firewall/

- **Antivirus:** los antivirus son elementales en todos los equipos de cómputo, porque aportan protección ante amenazas, hace escaneos al sistema operativo y monitorea el comportamiento de archivos que entren a los computadores, también facilita la forma de bloquear virus y eliminarlos.[24]

[24] CAPTIO.NET. Software antivirus. utilizadas [En línea]. Consultado: 14 de marzo de 2022. Disponible en: https://www.captio.net/blog/herramientas-seguridad-informatica

# 6 CONCLUSIONES

- Todas las compañías deben de tener un plan riguroso de pruebas de penetración y además constante, lo que les permitiría encontrar baches para corregirlos a tiempo.

- Dentro del plan de ciberseguridad de toda organización, siempre se debe contemplar las pruebas de penetración con herramientas de alta tecnología que le garantice un informe estructurado con las respectivas recomendaciones y, acciones para corregir en el sistema informático de la compañía.

- Es importante conocer las características de las herramientas que detectan las vulnerabilidades y fortalezas informáticas en las compañías, para tenerlas en cuenta al momento de implementar planes de seguridad y realizar tareas propias de la seguridad informática.

- La profesión de ingeniería sí está regulada y cuenta con un código de ética emitido por la entidad del gobierno llamada COPNIA.

- La ética es más importante que el dinero, porque la ética habla de la integridad del empleado mientras que lo antiético siempre da mala imagen y termina con consecuencias desfavorables.

- Es muy importante conocer las leyes que rigen la profesión de ingeniería en Colombia para entender y, tener presente las consecuencias a las que se somete quien las incumpla.

- Todas las compañías están expuestas a ataques informáticas y, los equipos interdisciplinarios de ciberseguridad son fundamentales para garantizar la estabilidad y funcionamiento de los sistemas de red en las organizaciones.

- La mejor forma de contener un ataque cibernético es realizar actividades, procesos y contar con herramientas actualizadas para evitarlo o en consecuencia tener las suficientes fortalezas para atacarlo cuando se presente.

- Es importante tener claro conceptos, conocer herramientas robustas de contención cibernética para desempeñar la labor como especialista de una manera altamente eficaz y reconocida.

- Las pruebas de intrusión son muy necesarias realizarlas en una red de datos o teleinformática, porque permite hacer el análisis de las vulnerabilidades y poderlas corregir a tiempo.

- Para evitar vulnerabilidades en los sistemas operativos es indispensable mantenerlos actualizados con sus últimas actualizaciones dadas por el fabricante, porque un sistema operativo desactualizado es altamente vulnerable a ataques informáticos.

- Las herramientas para identificar vulnerabilidades son elementales para un equipo Red Team & Blue Team, casi que sin este tipo de elementos sería imposible detectar fugas de información y ataques cibernéticos.

# 7 RECOMENDACIONES

**Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización**

Cabe anotar que las siguientes recomendaciones se plantean de manera general y puede que para algunos usuarios y/o compañías sean obvias y no representen relevancia; pero se estiman teniendo presente el crecimiento vertiginoso de los ataques cibernéticos y, la heterogeneidad de los niveles de escalabilidad y entendimiento con respecto a la seguridad informática en el entorno digital y, en especial en el sector empresarial.

La seguridad informática toma especial relevancia cuando se trata de hacer uso de los servicios financieros de manera online. Tener precauciones en el momento de utilizar herramientas bancarias como aplicaciones, sitios web, cajeros automáticos, minimiza el riesgo informático y ayuda a tener la información personal protegida de los ciberdelincuentes que siempre están disponibles para denegar servicios, hurtar contraseñas, suplantar identidades y, en fin, afectar tanto la infraestructura de las entidades bancarias como la economía de los usuarios.

En efecto, se hace necesario tener presente las siguientes recomendaciones a la hora de hacer transacciones bancarias de manera virtual:

- No se debe compartir contraseñas de los servicios financieros con nadie, ni patrón de acceso a los dispositivos móviles, computadores, tabletas, en sí de ningún aparato con el que se utilice el servicio bancario.

- En los dispositivos móviles es recomendable configurar el bloque automático y en la medida de lo posible tener un PIN numérico, configurar la huella digital y en el mejor de los casos el reconocimiento facial.

- No utilizar los servicios bancarios en wifi públicas, porque estos espacios son muy propensos a ser espiados de manera constante por los ciberdelincuentes y les facilita capturar contraseña, login y toda la información personal.

- No es recomendable guardar contraseñas en computadoras y equipos móviles y no se debe almacenar números de cuentas bancarias o tarjetas crédito y débito ya que es información personal y confidencial.

- No suministrar información personal y financiera por medio de correos electrónicos, llamadas telefónicas, mensajes de texto ni de ninguna manera a fuentes desconocidas, solamente a la entidad bancaria de manera presencial.

- Reportar a la entidad financiera cualquier actividad sospechosa que visualice en la sucursal virtual o en la cuenta bancaria y tener el servicio activo de notificaciones en el banco para que cuando se realice algún movimiento le llegue un mensaje de alerta al celular.

- Absténgase de consultar sitios web donde hay enlaces sospechosos como las URL recortadas, la publicidad con ventanas emergentes y spam.

- Se recomienda la instalación de aplicaciones que aumenten la seguridad de los equipos móviles y fijos como los antivirus, anti spam y aplicaciones altamente confiables que realicen copias de seguridad.

- Cuando realice transacciones en el sitio web de la entidad financiera debe revisar que la barra de direcciones empiece por https y que muestre el candado. Esto le permitirá que está ingresando a un sitio web seguro antes de digitar cualquier información personal.

- Absténgase de tener la misma contraseña para todos los dispositivos, cuenta de correo, redes sociales y aplicaciones. Quizá no tenga importancia si le hackean una cuenta de un correo electrónico, pero sí tiene mucha importancia si el ciberdelincuente obtiene la contraseña de la sucursal virtual.

- Estar alerta de las comunicaciones emitidas por la entidad bancaria, en caso de recibir un correo electrónico dudoso, no hacer click, porque puede ser un phishing. Esta es una forma muy empleada para que la víctima entregue sus contraseña y datos bancarios, envían e-mail que al darle clic direccionan al usuario a una página web falsa donde le piden información sensible.

- Ingresar a la sucursal virtual del banco desde el inicio del sitio web del mismo banco o digite de forma directa la dirección web en el navegador. De esta forma estará seguro que el sitio web es auténtico[25].

[25] CARDOZO, Rossana. BBVA. Doce consejos de seguridad para usar la banca digital. [En Línea]. [Consultado: 24 de noviembre de 2021]. Disponible en: www.bbva.com/es/doce-consejos-de-seguridad-para-usar-la-banca-digital.

# 8 VIDEO DE SUSTENTACIÓN

- https://www.youtube.com/watch?v=LeAksnU8Q8Y

## BIBLIOGRAFÍA


ALCALDÍA DE BOGOTÁ D.C. CONPES 3701 DE 2011. [En línea]. [Consultado : 10 de febrero de 2022]. Disponible en: https://tic.bogota.gov.co/transparencia/marco-legal/normatividad/conpes-3701-2011

AMBIT-BST. ¿Qué significa SIEM y cómo funciona? [En línea]. Consultado: 13 de marzo de 2022. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

AMBIT-BST. Cuáles son las herramientas SIEM más utilizadas [En línea]. Consultado: 13 de marzo de 2022. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

CÁMARA DE COMERCIO BOGOTÁ. Documento Conpes 3854, Política nacional de seguridad digital. [En línea]. [Consultado : 10 de febrero de 2022]. Disponible en: https://bibliotecadigital.ccb.org.co/handle/11520/14856

CAMPUSCIBERSEGURIDAD. ¿Qué es el pentesting? [En línea]. [Consultado: 10 de febrero de 2022]. Disponible en: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

CAMPUSCIBERSEGURIDAD. ¿Qué es el Pentesting? [En línea]. Consultado: 2 de marzo de 2022. Disponible: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

CAPTIO.NET. Software antivirus. utilizadas [En línea]. Consultado: 14 de marzo de 2022. Disponible en: https://www.captio.net/blog/herramientas-seguridad-informatica

CONGRESO DE COLOMBIA. Ley 1273 de 2009. [En línea]. [Consultado: 10 de febrero de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CONGRESO DE COLOMBIA. Ley 1273 de 2009. [En línea]. [Consultado: 16 de febrero de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COPNIA. República de Colombia. Código de Ética. [En línea]. Consultado: 20 de febrero de 2022. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CORE SECURITY. Red Team. [Online]. Consulted: March 19, 2022. Available in: https://www.coresecurity.com/penetration-testing/red-team

DESDE LINUX.NET. ¿Qué es un Shell? [En línea]. Consultado: 2 de marzo de 2022. Disponible en: https://blog.desdelinux.net/que-es-un-shell/

EXPLOIT DATABASE. Exploit. Consulted: March 18, 2022. Available in: https://www.exploit-db.com/exploits/42031

FUNCIÓN PÚBLICA. Ley 1581 de 2012. [En línea]. [Consultado : 10 de febrero de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

GEEKFLARE. Herramientas en línea de pentest de reconcimiento. [En línea]. [Consultado: 11 de febrero de 2022]. Disponible en: https://geekflare.com/es/reconnaissance-exploit-search-tools/

LOGRHYTHM.SIAM. Consulted: March 20, 2022. Available in: https://logrhythm.com/solutions/security/siem/

MARIN DE LA FUENTE. ¿ Qué es Nmap? Por qué necesitas este mapeador de red . Consultado: 3 de marzo de 2022. Disponible en: https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/

MICROSOFT. Soporte técnico de Windows. [En línea]. Consultado: 4 de marzo de 202. Disponible en: https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finaliz%C3%B3-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962

MINTIC. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

PANDA. ¿Qué es un Exploit? [En línea]. Consultado: 2 de marzo de 2022. Disponible en:https://www.pandasecurity.com/es/security-info/exploit/

REYDES. Herramientas para Esnifar la Red y Analizar Paquetes. [En línea]. Consultado: 13 de marzo de 2022. Disponible en: http://www.reydes.com/d/?q=Herramientas_para_Esnifar_la_Red_y_Analizar_Paquetes

S. Rahimi, M. Zargham (2013). Vulnerability detection with deep learning, 2013 3rd IEEE International Conference on Computer and Communications (ICCC), 2013, pp. 395 - 407, doi: 10.1109/CompComm.2017.8322752. Consulted: March 18, 2022. Availabre in:https://ieeexplore.ieee.org/document/6502762