Capacidades Técnicas, Legales y De GestiónPara Equipos Blue Team y Red Team

Diana Patricia Galviz Galviz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECTBI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM
CEAD PALMIRA
2023-1

Capacidades Técnicas, Legales y De GestiónPara Equipos Blue Team y Red Team

Diana Patricia Galviz Galviz

Tutor: M.Sc. John Freddy. Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECTBI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: CAPACIDADES TÉCNICAS, LEGALES Y DE ESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM
CEAD PALMIRA

2023-1

Contenido

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

GLOSARIO

BLUE TEAM: este equipo que representa la defensa en un proceso de simulación para determinar el alcance de seguridad cibernética que se tiene al momento de que se presenten ataques.[1]

CIBERATAQUE: se le llama ciber ataque al acontecimiento sucedido en una infraestructura TI, que tiene como fin generar un afectaciones de seguridad de forma que los puntos ocultos que se encuentran establecidos para los temas de la seguridad de la estructura tecnológica se visualicen de esta forma se puedan generar afectaciones critica en un sistema donde se comprometen los activos de información.[2]

CIBERSEGURIDAD: son las capacidades y herramientas que se utilizan en una organización, lo cual que permite que riesgo sean mínimos, teniendo en cuenta ella inseguridad que se generar con el simple hecho de estar conectados a una red de internet. [3]

CONTROL: culturas, práctica, procedimientos, y políticas que se implementa en una empresa con el fin establecer seguridad para los riesgos y vulnerabilidades que se generan en una infraestructura tecnológica.[4]

CONFIDENCIALIDAD: políticas que permiten la restricción y acceso no autorizado a la información de una empresa.

---

[1] AMÉZQUITA DURAN, Jorge Alonso, et al. Capacidades técnicas, legales y de gestión para equipos blue team & red team. 2021.recuperado de: https://repository.unad.edu.co/handle/10596/43170

[2] CANO, Jeimy J. Ciberataques. *Revista Sistemas*, 2020, no 157, p. 67-74 disponible en https://sistemas.acis.org.co/index.php/sistemas/article/view/129/101

[3] MAROTO, Juan Puime. El ciberespionaje y la ciberseguridad. En *La violencia del siglo XXI. Nuevas dimensiones de la guerra*. Instituto Español de Estudios Estratégicos, 2009. p. 45-76. Recuperado de: file:///C:/Users/diana/Downloads/Dialnet-ElCiberespionajeYLaCiberseguridad-4549946%20(2).pdf

[4] POSSO RODELO, Johana; BARRIOS BARRIOS, Mauricio. *Diseño de un modelo de control interno en la empresa prestadora de servicios hoteleros eco turísticos nativos activos eco hotel la cocotera, que permitirá el mejoramiento de la información financiera*. 2014. Tesis Doctoral. Universidad de Cartagena. Recuperado de: https://repositorio.unicartagena.edu.co/handle/11227/2130

EXPLOIT: ataque que aprovecha una vulnerabilidad para realizar acciones dañinas afectando una infraestructura por medio de instalación de un programa maligno.[5]

FIREWALL: herramienta que funciona como cortafuegos, filtrando el tráfico de una red a otra, lo cual bloque los accesos de a la información cuando se presentan eventos maliciosos. [6]

[5] *AVG. ¿Qué es un exploit en seguridad informática? [consultado el 30 de noviembre de 2022]. Recuperado de: https://www.avg.com/es/signal/computer-security-exploits*

[6] CUENCA, Jackson. Firewall o cortafuegos. *Universidad Nacional de Loja*, 2016.Recuperado de: https://www.researchgate.net/profile/Jackson-Cuenca/publication/295256426_FIREWALL_O_CORTAFUEGOS/links/56c8a7ed08ae96cdd06baf7c/FIREWALL-O-CORTAFUEGOS.pdf

RESUMEN

En el siguiente trabajo se evidenciará el desarrollo del trabajo realizado en tiempo que se desarrolló el seminario de profundización en Capacidades técnicas, legales y de gestión para equipos blue team y red team. El cual se compuso de 4 etapas que se distribuyeron de la siguiente forma:

Etapa 1: conceptos de equipos de seguridad, donde se requería realizar la evaluación de las acciones que realizan los equipos Red Team y Blue Team para las organizaciones.

Etapa 2: con base al caso de estudiose indago sobre los procesos ilegales y no éticos a los cuales se puede incurrir al momento de realizar la firma de un acuerdo dentro de una organización y porqué se debe tener cuidado al momento de firmar estos documentos.

Etapa 3: se realiza la demostración de las vulnerabilidades de un sistema informático a través del uso de metodologías y herramientas de intrusión, con base en un caso de estudio.

Etapa 4: se identificaron y formularon estrategias que permitan la detención por medio de los análisis de riesgos que se pueden generar en una infraestructura TI.

1. INTRODUCCION

El trabajo que se realiza en esta etapa cuenta con la recopilación de las actividades que se realizaron durante el desarrollo del seminario de profundización, donde se desarrollaron diferentes actividades que ayudan a fortalecer la comprensión de los temas que se establecieron dentro de la guía de actividades con respecto a la seguridad informática dentro de las 4 etapas que se desarrollaron.

Identificación de leyes

Ámbito ético y legal

Descripción de ataques a un sistema informático

Medidas de contención

El documento final se genera como informe técnico, en el cual se hace la integración de las actividades del seminario, sobre los aspectos que fueron investigados y que se consideraron de mayor relevancia para la culminación del proceso.

2. OBJETIVOS

OBJETIVO GENERAL

Estructurar el informe técnico sobre los resultados de las acciones que se realizan los equipos Red Team & Blue Team dentro de la empresa.

OBJETIVOS ESPECIFICOS

- Analizar la leyes y decretos que existen para la protección de la información
- Conocer las acciones éticas y legales de los equipos Red Team & Blue Team.
- Realizar pruebas de intrusión
- Elaborar estrategias de contención orientadas a los ataques en tiempo real.

3. DESARROLLO DE LA ACTIVIDAD

Etapa 1: leyes y decretos sobre delitos informáticos en Colombia
Ley 1273 de 2009

En la actualidad se ha incrementado el teletrabajo y con ello el uso tecnologías, lo que ha generado un alto índice en los delitos informáticos, es por eso la importancia de que se cuente con medidas de seguridad y la protección de los datos personales.

Por medio de la LEY 1273 DE 2009, se respalda la protección integral de la información, además de la prevención de sanciones cometidas en contra de los datos o cualquier sistema de información, también la prevención de delitos que se puedan cometer a través de cualquier sistema o tecnología donde se realice algún procesamiento para la obtención, creación, modificación, intercambio de información de forma inadecuada.[7]

La LEY 1273 DE 2009, cuenta con 7 artículos profundizan en cada uno de los delitos que se pueden cometer en contra o por los sistemas informáticos.

Artículo 269A

Cuando un sistema se encuentra protegido y el ciber delincuente ingresa a un sistema de información sin ser autorizado además de mantener en el sistema sin que la persona que genera las credenciales de acceso se las haya asignado.

Artículo 269B

Este delito se comete cuando se impide el funcionamiento o el acceso de personas que no están autorizadas para realizar dichas actualizaciones de credenciales de acceso.

[7] SÁNCHEZ CASTILLO, Zulay Nayiv, et al. Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. 2017. Recuperado de: https://repository.unad.edu.co/handle/10596/11943

Artículo 269C: Interceptación de datos informáticos.

Este acto se comete cuando no existe una autorización u orden judicial que autorice la intercepción de datos informáticos bien sea en su origen, destino o internamente en un sistema de información.

Artículo 269D

Delito que ocurre al momento de que ingresan a un sistema de tener la facultad para ello y que por medio del ingreso destruya, borre, trastorne o cambie datos informáticos, o en el sistema de información cambien o dañen fragmentos de los componentes.

Artículo 269E:

La instalación de software o programas maliciosos que se introduzca en un sistema de información con el propósito de generar efectos dañinos en los datos y sistemas.

Artículo 269F: Violación de datos personales.

Este delito se basa en la violación de datos personales sensibles, con el fin de sacar un provecho propio o de un tercero donde se obtenga la información para, ser vendida, divulgada o modificada a través de bases de datos.

Artículo 269G

Sin autorización previa se realicen hechos como el diseño, desarrollo, tráfico de páginas electrónicas, envió de enlaces. También la modificación de nombres de dominio, con el propósito de llevar al que el usuario pueda ingresar a una IP diferente al de confianza que se requiera.

Artículo 269H

Para el artículo 269H los delitos penales tienen una agravación punitiva que se describe anteriormente generando un aumento hasta las tres cuartas partes.

Este caso aplica para los delitos realizados en un sistemas informáticos o redes de comunicaciones estatales u oficiales o del sector financiero, también si son cometidas por un servidor público, en aprovechamiento de la confianza de la

persona que posee la información, dando a conocer información que perjudique a otros, obteniendo provecho propio o para una tercera persona, además que se utilice con fines terroristas o utilizando a otra persona en su buena fe.

Por estos delitos también se inhabilitará por 3 años para la realización de dichas actividades de su profesión relacionadas con sistemas de información.

Artículo 269I

Este delito re refiere a la conducta señalada en el artículo 239, donde se apodere de un bien ajeno, en este caso haciendo uso de un sistema informático u otro medio semejante, realizando la suplantación de un usuario autorizado y autenticado.

Artículo 269J: Transferencia no consentida de activos.

La validación y manipulación informática o instalación de algún software para realizar transferencias no autorizadas generando perjuicio a un tercero, este articulo busca proteger el patrimonio económico del ciberdelito. [8]

Ley estatutaria 1581 de 2012

Por medio de esta ley se dictan las disposiciones que se relacionan con la protección de datos.[9]

objeto, ámbito de aplicación y definiciones

Las personas tienen el derecho de verificar, modificar o pedir la exclusión de los datos personales que se manejan en bases de datos, ya que como se refiere en el artículo 15 de la constitución política, las personas tienen el derecho a la privacidad personal. Es estado se encarga de respetar y hacer respetar estos derechos.

La base de datos que se pretenden compartir a terceros debe informar y contar con el previo permiso del titular, en este caso los archivos y bases de datos son sujetas a la reglamentación de la presente ley.

[8] BECHARA PALACIOS, Yenifer Yirlesa, et al. Análisis jurídico de la ley 1273 del 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informáticos. 2020.
9 BUITRAGO, Felipe Márquez. Aplicación de la ley estatutaria 1581 de 2012 a la red social facebook en colombia. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 2016, no 15, p. 1.

Definiciones:

Autorizaciones: Se requiere de una autorización previa para compartir bases de datos

Bases de datos. Datos personales que se les da un tratamiento

Dato personal: Información asociada con una o varias personas naturales.

Responsable del tratamiento: persona o entidad que maneja bases de datos con información personal y que a su vez es la encargada de dar tratamiento a los datos.

Titular: quien suministra los datos personales o familiares a una persona o identidad para que esta realice el tratamiento de la información.

Tratamiento: cualquier acción que se genere con los datos como, recolección, uso o circulación de estos.

Principios rectores

Los datos personales de una persona o empresa no pueden ser adquiridos sin la autorización del titular o del representante legal, ni tampoco la divulgación, para la veracidad y calidad de datos, estos no pueden ser parciales o incompletos o que contengan error y su tratamiento solo debe realizarse por la persona que se encuentre autorizada o directamente por el titular y no podrán estar disponibles en internet salvo que el acceso sea controlado para dar acceso informativo solamente a los titulares o terceros autorizados.

Categorías especiales de datos

Los datos sensibles corresponden aquellos con los cuales se afecta la intimidad del titular del dato cullo uso puede generar afectación en la intimidad, por lo tanto, se prohíbe la divulgación de datos sensibles excepto cuando se tenga la autorización o que le tratamiento del dato sirva para salvaguardar.[10]

[10] GARZÓN GARCÍA, Janier Rolando. *Protección de datos personales Ley 1581 octubre 2012*. 2015. Tesis de Licenciatura. Universidad Piloto de Colombia.

Convenio sobre la Ciberdelincuencia

Busca que las partes obtén por medidas legislativas que alteren la confidencialidad integridad y disponibilidad de los sistemas de información por medio del acceso ilícito.

Terminología: Se entiende por sistema informático el conjunto de dispositivos interconectados entre sí, y que su función sea la ejecución de programas que realicen el tratamiento de datos. [11]

Definir y explicar las siguientes herramientas de ciberseguridad

Herramientas:

Metasploit

Se le llama al Framework que sirve como entorno de prueba para generar algoritmos de instrucción en diferentes plataformas, con el objetivo de explotar un punto venerable en un sistema de información, este mismo que trabaja con diferentes programas como shells, codes, entre otros. Con base en lo anterior se puede ver que Metasploit, es un sistema de software, pero también es un framework que sirve como un auxiliar para realizar la explotación de vulnerabilidades.

Metasploit, funciona el método modo web y el modo consola.

En la modalidad web el usuario debe realizar la selección de cada una de las opciones dependiendo del tipo de ataque también se debe teclear el botón de Exploit al momento de terminar, con este proceso se realiza el intento para forzar el sistema que se encuentra comprometido. Seguidamente se puede realizar un ataque por shell, lo que genera que salga una pantalla que refleja la conexión a http.

Para la opción de consola se proporciona de una línea de comandos, lo que permite tener un soporte para profesional encargado o para el atacante para tener la

[11] OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

posibilidad de realizar línea por línea el exploit que se va a utilizar. Es la opción más apropiada para informáticos que cuenten con un conocimiento para el uso de exploits, toda vez que es una herramienta que les ayuda a conocer los requerimientos del exploit que se necesitan utilizar. Esto no quiere decir que se deba descartar la opción de modo web.

Nmap

Es una herramienta utilizada para la explotación de red y usada hacia la realización de auditorías informáticas, su código es abierto, y se utilizan paquetes IP, identificar los equipos que se hallan activos en la red, además de los servicios que estos ofrecen y los sistemas operativos que tiene instalados, también se puede ver el cortafuegos que se manejando entre otras características importantes. De acuerdo con lao anterior Nmap, es una herramienta que se puede ser utilizada para realizar auditorías en cualquier red o sistema informático.[12]

Una prueba de penetración se estructura por medio de fases y dado que Nmap, interactúa con la red y los dispositivos para realizar el escaneo, es utiliza en la fase reconocimiento activo del sistema.

OpenVas

Es un scanner de vulnerabilidades por lo general es distribuidos bajo licencias y sirve para integra servicios y herramientas, además de genera actualizaciones continuas, para detectar riesgos de diferente calibre, de bajo riesgo para el usuario como vulnerabilidades graves que puedan afectar dispositivos o redes. Tiene la capacidad de generar un informe con las soluciones que se pueden ejecutar. Además, tiene una base de datos muy amplia de la cual cuenta con datos de más de 50.000 vulnerabilidades y test de diferentes tipos.

Se pueden generar pruebas autenticadas y no autenticadas y configuraciones para personalizar el rendimiento de las explotaciones en gran escala.[13]

[12] DOMÍNGUEZ, Hernán M., et al. Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple “Contraseñas”, pruebas de concepto con software libre y su remediación. *Maskana*, 2016, vol. 7, p. 87-95.
[13] ALTUBE VERA, Rafael. ¿Qué es OpenVAS?.11 noviembre 2020.

Servicios en línea

ExploitDB

Esta herramienta sirve para sacar un provecho al fallo de seguridad, donde tiene como objetivo el ingreso a un equipo de forma que la vulnerabilidad pueda ser aprovechada por este servicio. Esta herramienta centra los exploits utilizados para explotar las vulnerabilidades encontradas en los sistemas, con un trabajo mucho más practico.

Al ingresar al sistema la herramienta busca las vulnerabilidades lo cual le permite colocar filtros locales o remotos, cuando se identifica la vulnerabilidad se puede abrir y descargar el exploit, además verifica si está activo o no.

Por medio de la herramienta se puede clonar de la maquina local con el propósito de modificar el script de búsqueda y así adaptarlo a las necesidades.[14]

CVE

Las CVE, son las bases de datos públicas, identificadas por un código que se le asigna a cada al momento de ser registradas las vulnerabilidades además de identificar y clasificar cada una, esta lista cuenta con más de 178.600 comunes.

El código CVE que se le asigna a cada una de las vulnerabilidades, sirve para que se identifiquen de forma unívoca.[15]

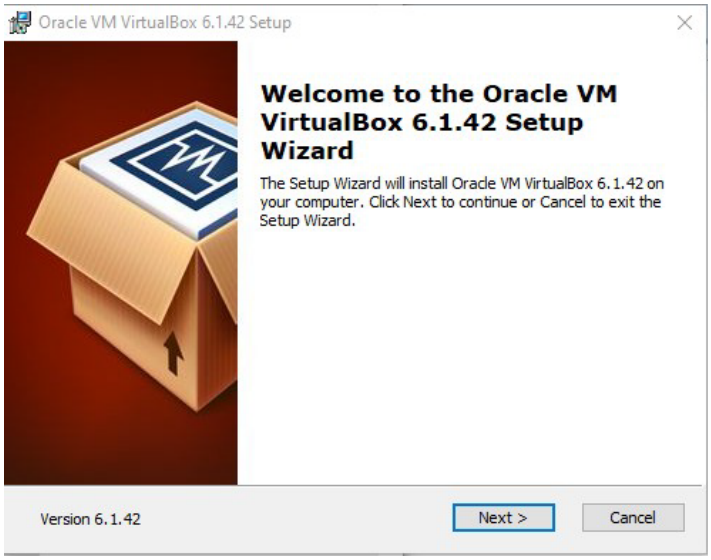
Descargar la herramienta virtualizadora “VirtualBox”

[14] GONZÁLEZ THOLA, Diego Fernando, et al. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam.

[15] FRANCO, David A. PEREA, Jorge L. TOVAR, Luis C. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Universidad de Cartagena, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, Vol. 24(5), 13-22 (2013).

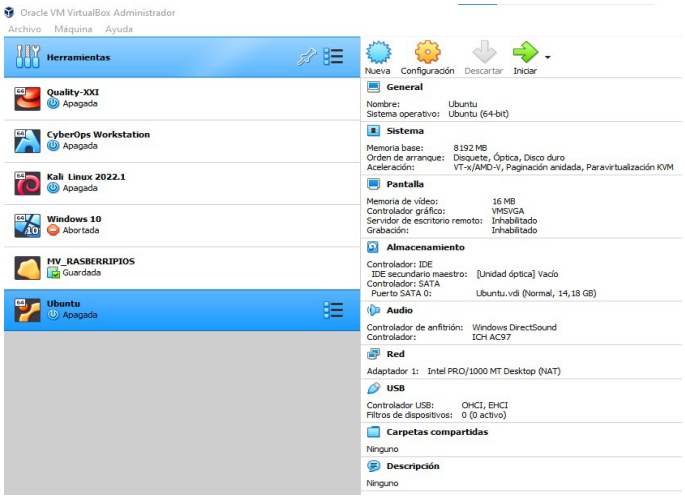
1. Instalación inicial de la maquina VirtualBox.

Ilustración 1: Versión de VirtualBox



Autoría propia

Ilustración 2: Interfaz VirtualBox



Autoría propia

Etapa 2 - actuación ética y legal.

Evidenciar los proceso ilegales y no éticos que estén estipulados en el acuerdo de confidencialidad entre Diana Patricia Galviz Galviz y whitehouse security.

Para las empresas los acuerdos de confidencialidad son una herramienta que se utiliza para proteger los activos informáticos; estos acuerdos se establecen como objetivo guardar confidencialidad sin revelar a terceros datos sensibles de la empresa. Un acuerdo es basado en el principio de la responsabilidad del profesional y de la buena fe. Aun no se ha establecido una legislación expresa dentro del ordenamiento jurídico colombiano, por lo tanto, se aplica la de contratos y sus obligaciones.

Dentro del acuerdo de confidencialidad Anexo # 3 se evidencia que hay varios temas de alteración ilegal y no éticos, los cuales se describirán a continuación.

Cláusula Primera: Objetivo

No divulgar directa, indirecta, , **autoridades legales** y **procesos ilegales** dentro de Whitehouse Security no podrán ser divulgados:

Observación: En la estructura del acuerdo de confidencialidad se puede apreciar que si la empresa realiza procesos ilegales dentro de sus operaciones no podrán ser divulgadas ante las autoridades, pero como profesional ético se está en la obligación de informar a las autoridades sobre los procesos ilegales que se evidencien al momento de desarrollar las actividades en una empresa, ya que estos delitos que no son divulgados ante la ley, donde se oculta información o se pretende sacar un provecho de la situación, son hechos que se estaría cometiendo como una falta ante la ley ya que esta no divulgación le estaría convirtiendo en cómplice del delito.

Cláusula Segunda: Definición de información confidencial

Número 2. **datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos**".

Observación: en este punto se habla de chuzadas, intercesión de información y accesos abusivos, como profesional de seguridad de la información no puede permitir que se pase por alto cualquiera de las situaciones anteriormente mencionadas en un sistema de información, ya que esto estaría generando un riego para los activos de la empresa, además se estaría cometiendo delitos que pueden ser castigados bajo la Ley 1273 de 2009 ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO[16], por lo que algo abusivo conlleva a realizar procedimientos más allá de lo permitido, este articulo menciona las faltas al ser vulnerada y que tendrían consecuencias como prisión por 48 a 96 meses, también multas de 100 salarios mínimos legales mensuales vigentes. También se está vulnerando el ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS, también se menciona sobre la intercesión de datos por lo que estaría vulnerando este artículo que tiene como consecuencias pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Cláusula cuarta: obligaciones de la parte receptora

Número 3: **No denunciar**, **actividades sospechosas de espionaje o cualquier otro proceso**.

Número 4: **Abstenerse de denunciar, información confidencial e ilegal.**

Observación:

Observación: el acuerdo habla de no denunciar ante las autoridades las actividades sospechosas de espionaje por lo que se puede intuir que la empresa obtiene información de forma ilegal y busca asegurar que sus empleados al momento de

[16] Colombia. Congreso de la República "Ley 1273 de 2009" Diario Oficial No. 47.223 de 5 de enero de 2009, [En Línea] 2009. Dsiponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

tener conocimiento de estos procesos no los lleven a conocimiento de las autoridades.

información confidencial.

Número 8

Observación: contraer una responsabilidad ante las autoridades de datos o información que se tenga bajo su poder ante algún allanamiento o investigación es un acto ilegal debido a que dicha información fue suministrada por la empresa o obtenida en desempeño de la actividad laboral es por eso por lo que la responsabilidad de dicha información de acuerdo con lo que se establece por la ley es que es responsable de la misma el representante legal de la empresa.

Cláusula octava: solución de controversias

Acuerdo. <u>Acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security</u>.

Observación: Se menciona que hay que mediar para la solución de conflictos que se presenten entre las partes en la ejecución del acuerdo. Y que en caso de que se encuentre información ilegal se deberá recurrir a un abogado privado para que la empresa quede exenta de cualquier responsabilidad, con esto se intuye que se cometen actos no éticos, ya que la información que sea recolectada dentro de las funciones laborales el trabajador no tiene como saber si esta información es legal, por lo tanto, la empresa está en la obligación de respaldar a sus empleados en caso de que requieran un abogado y no buscarlo de forma externa. . En este caso se estaría vulnerando el ARTÍCULO 269H. [17]

Caso de la OPERACIÓN ANDROMEDA BUGGLY

En el caso de la operación ANDROMEDA BUGGLY, se vulneraron varios artículos de LEY 1273 DE 2009, teniendo en cuenta que se encontraron falla de seguridad

[17] Mintic. (2009). Ley 1273 [LEY_1273_2009]. Mintic. (pp. 1-4).

por falta de diciplina, además de que no se realizaban los controles pertinentes sobre el personal que frecuentaba la independencia militar. Entre ellas la falta de planeación y control en las actividades que se realizadas tanto por el personal militar como civil. Además, había un flujo de personas que ingresaban al interior de la institución y contaban con alto un conocimiento en la parte informática y no tenían una supervisión ni controles para el acceso a la información.

En el proceso de selección de los agentes que integraron la operación ANDROMEDA BUGGLY, no se contó con un estudio de seguridad y al momento del allanamiento no se le informo inmediatamente al superior que se encontraba al mando de la diligencia, pese la gravedad de la situación.

Andrómeda solamente estaba autorizada para producir inteligencia de conocimiento técnico. Sin embargo, con la declaración del hacker Andrés Sepúlveda se pudo ver que estaban vendiendo información donde sostenían comunicaciones de las Farc y que había sido recolectada dentro de las actividades de la unidad. Además de que algunos de los oficiales de forma individual manejaban irregularidades en cuanto al manejo y clasificación de la información

7. Utilizando como instrumento a un tercero de buena fe.[18]

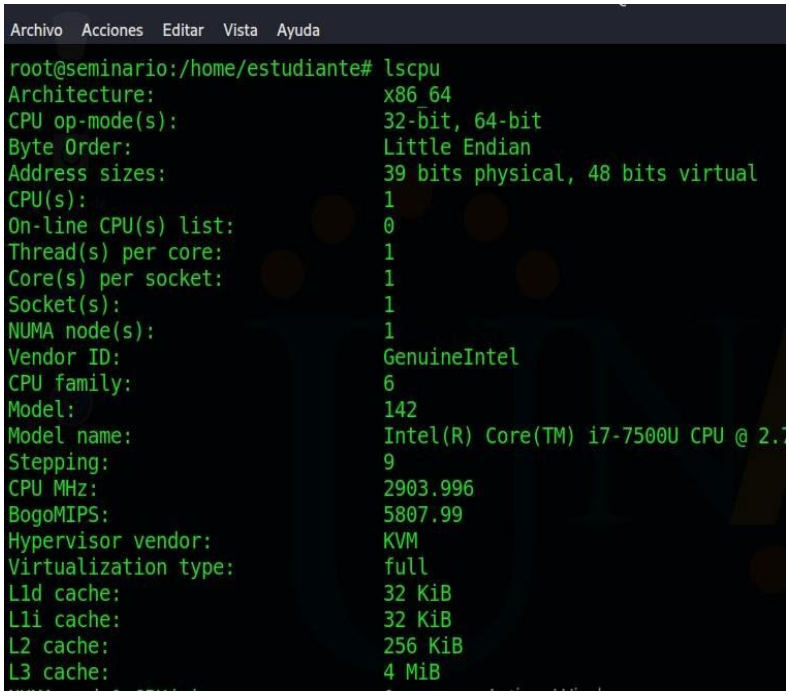
Etapa 3: Ejecución pruebas de intrusión

Teniendo en cuenta que en la etapa 1, no se contaba con el enlace para la instalación del banco de trabajo, antes de iniciar con los pasos de la presente actividad, se dejara plasmado el proceso.

Para dar inicio con la actividad se adjunta imagen con las características del hardware de la maquina atacante Kali Linux

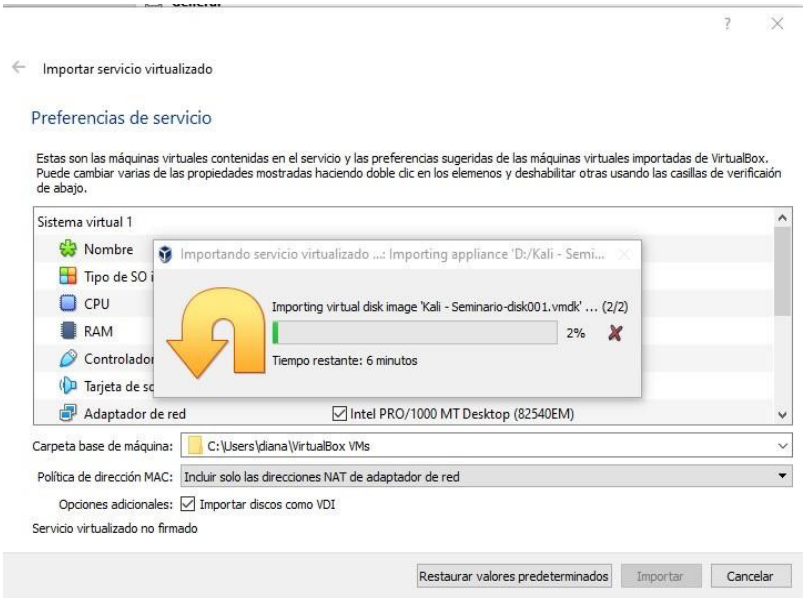
Ilustración 3:Características del hardware de Kali Linux

[18] EL TIEMPO, Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue, 2015. Recuperado de: https://www.eltiempo.com/archivo/documento/CMS-15141236



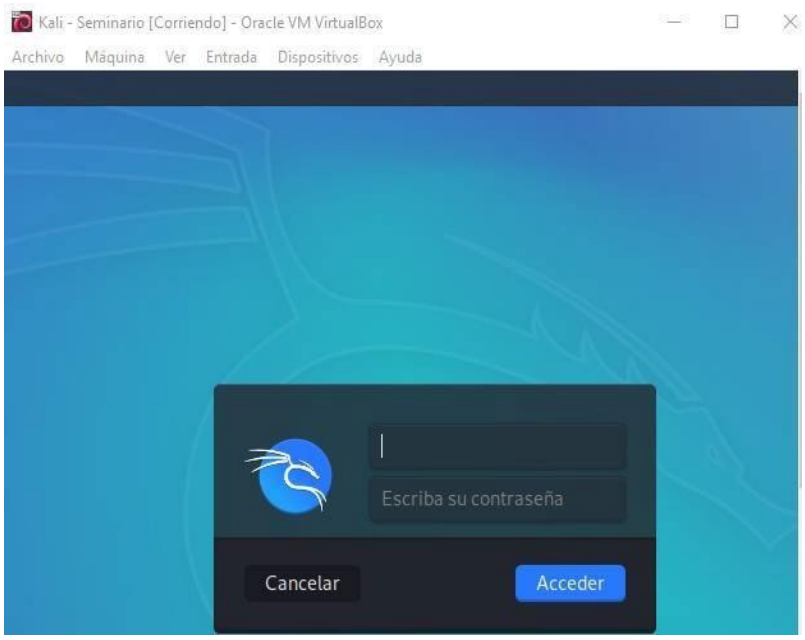
Fuente: elaboración propia

Ilustración 4:Importación del servicio virtualizado de Kali Linux



Fuente: elaboración propia

Ilustración 5:Usuario y contraseña



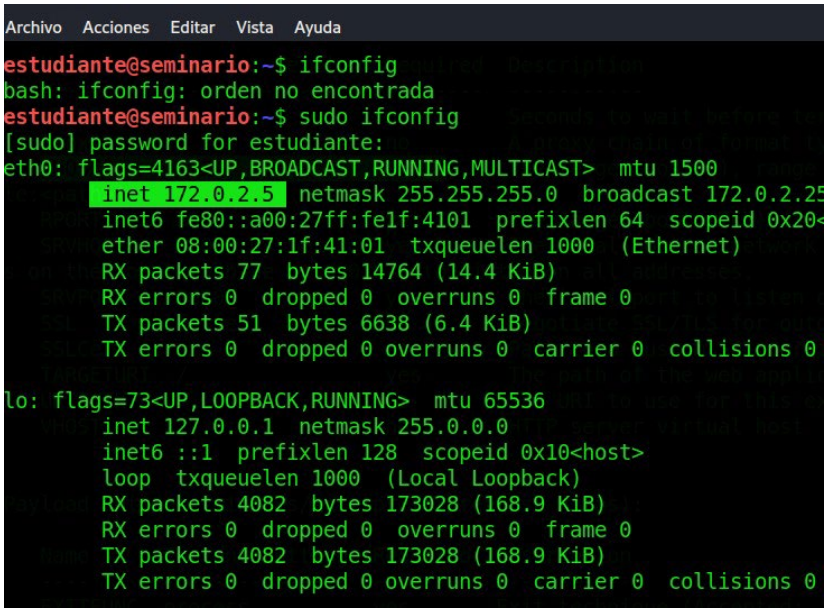
Fuente: elaboración propia

Se termina con el proceso de importación se requiere de un usuario y contraseña, como credenciales de acceso y son las siguientes:

Usuario: estudiante

Contraseña: unad2020

Ilustración 6:Direccionamiento IP en Kali Linux

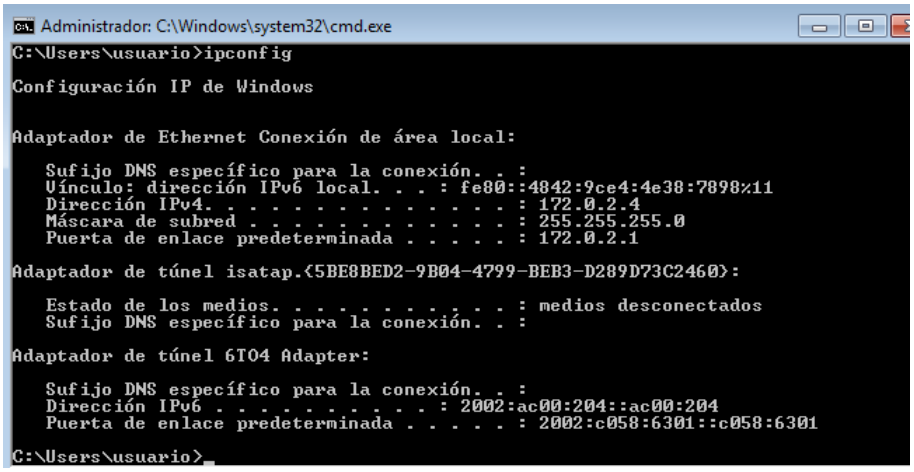


Fuente: elaboración propia

Se realiza la verificación de la IP, en Kali Linux, la cual corresponde a **172.0.2.5**

Para realizar pinga la máquina virtual de windows 7 X64 se debe conocer el la IP, por lo tanto, se ingresa ipconfig, para identificarla como se verá en la siguiente imagen.

Ilustración 7:Dirección IP Windows 7X64



Fuente: elaboración propia

Se realiza la verificación de la IP, en windows 7 X64, la cual corresponde a **172.0.2.5**

Ilustración 8:Conexión Kali Linux a Windowsping

Fuente: elaboración propia

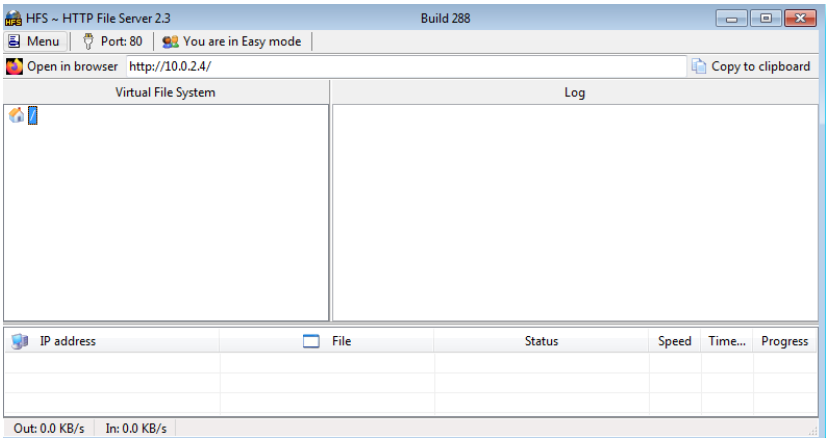
Se realiza ping desde la máquina de Kali Linux para verificar la conexión con la máquina windows 7 X64

3.1. EJECUCIÓN PRUEBAS DE INTRUSIÓN

Información recolectada del anexo 4

- windows 7 X64
- Aplicación llamada rejetto v. 2.3, tiene asociado un exploit que puede terminar en una Shell.

Ilustración 9:Rejetto v. 2.3

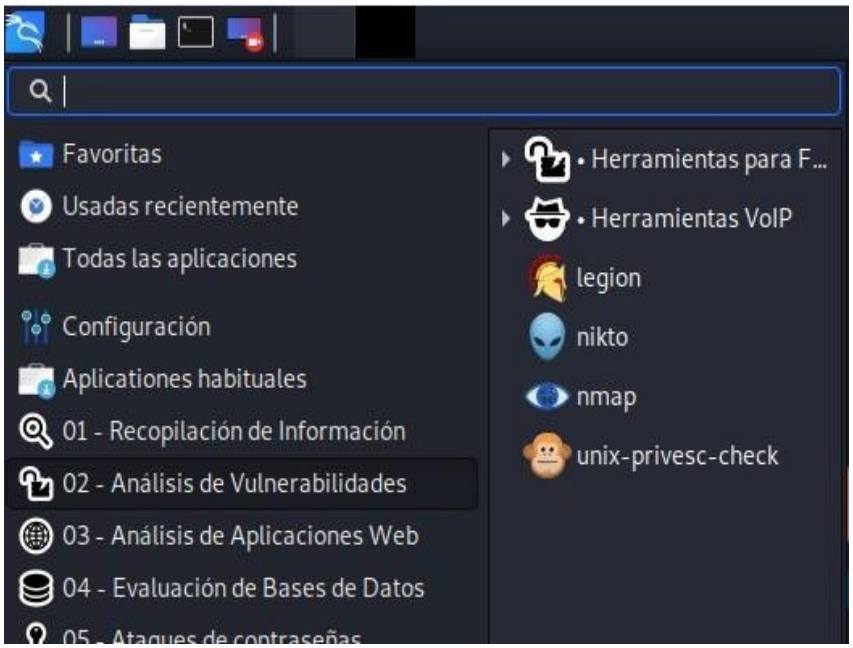


Fuente: elaboración propia

Nmap[19]

La aplicación Nmap viene instalada en Kali Linux

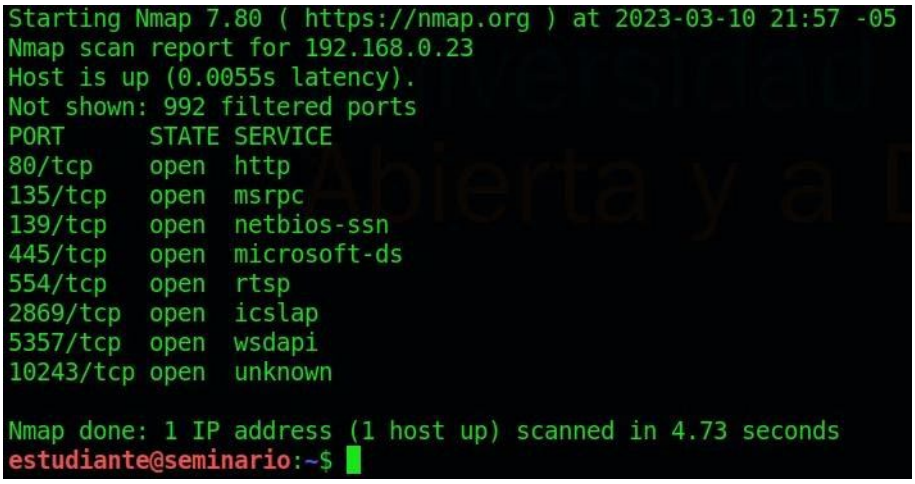
Ilustración 10:Nmap



Fuente: elaboración propia

[19] RIOS ALIAGA, Leonardo Julio. *Modelo para la detección de escaneo de puertos de la computadora en una red WLAN*. Tesis Doctoral. https://repositorio.umsa.bo/handle/123456789/29646

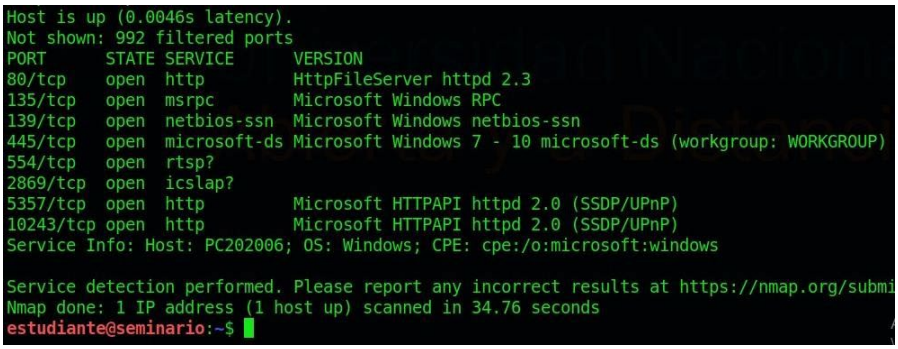
Ilustración 11:Escaneo de puertos



Fuente: elaboración propia

Como se puede ver los puertos 80, 135, 139, 445,554, 2869, 5357, 102443, se encuentran abiertos

Ilustración 12:Versión de los servicios que se aloja en los puertos

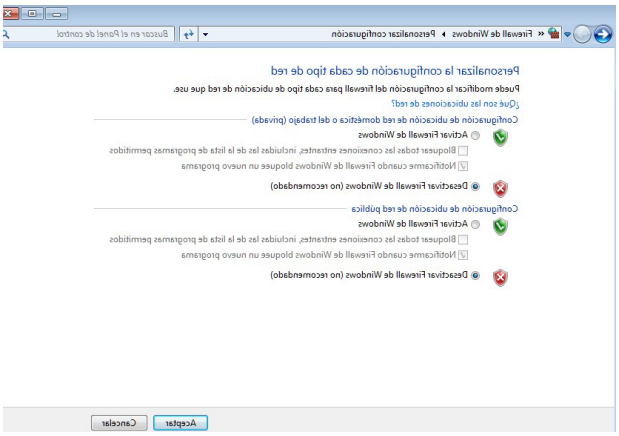


Fuente: elaboración propia

Con **Nmap** como se puede ver en la anterior imagen se visualizan los puertos que encuentra abiertos y son el puerto 80, 135, 139, 445,554, 2869, 5357, 102443, se encuentran abiertos al igual que lo se veía en la imagen anterior la diferencia en esta imagen es que se pueden ver no solo que se encuentran abiertos si no también

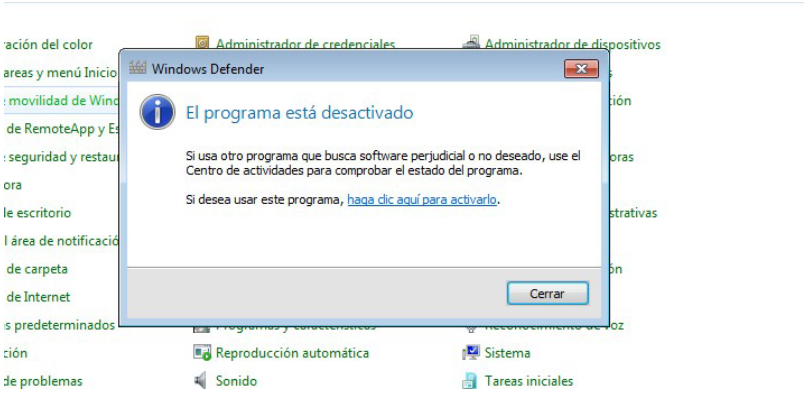
que cuentan con unos servicios como por ejemplo el puerto 80 tiene el servicio http, y versión HttpFileServer httpd 2.3b, lo que quiere decir que contiene un file Server el cual se puede convertir en una vulnerabilidad de acuerdo con su versión 2.3b. además muestra que el objetivo es un sistema operativo Windows.

Ilustración 13:Desactive el firewall en Windows



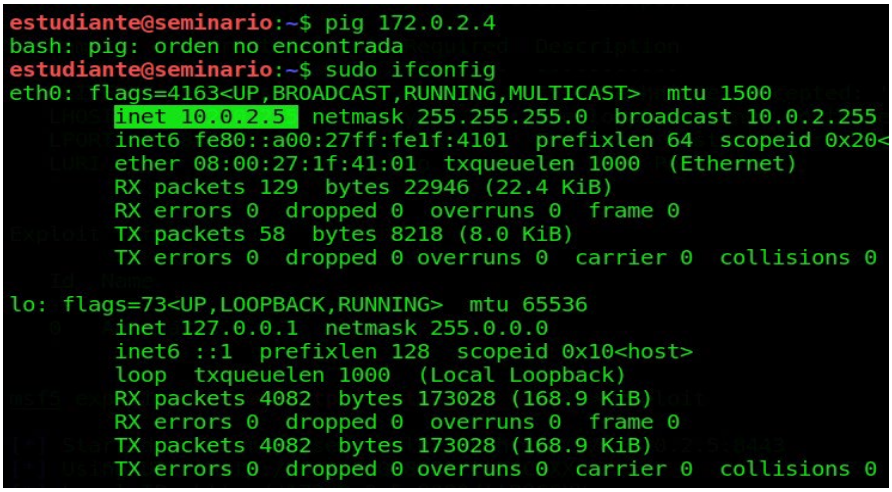
Fuente: elaboración propia

Ilustración 14:Desactive Windows Defender



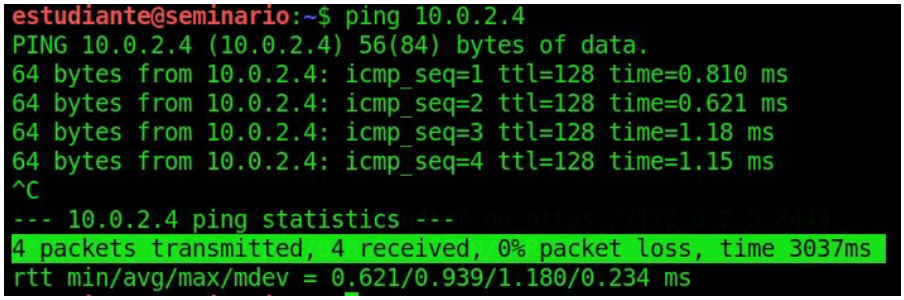
Fuente: elaboración propia

Ilustración 15:Ping 10.0.2.5



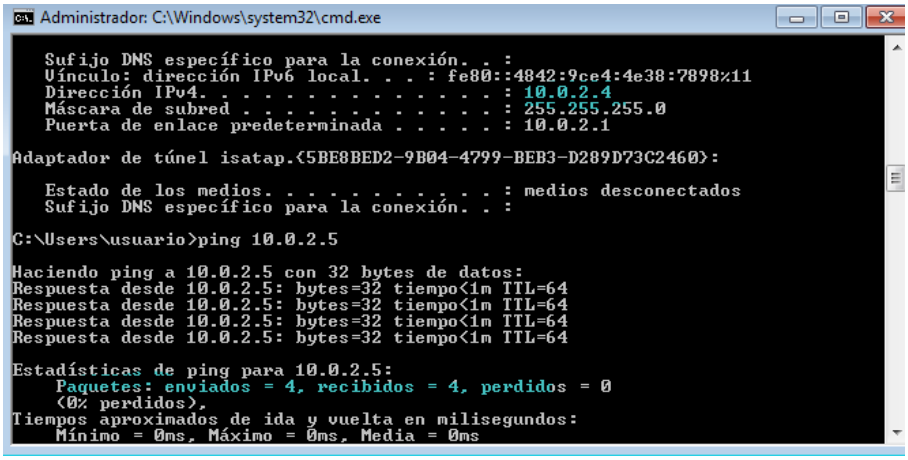
Fuente: elaboración propia

Ilustración 16:Ping 10.0.2.4



Fuente: elaboración propia

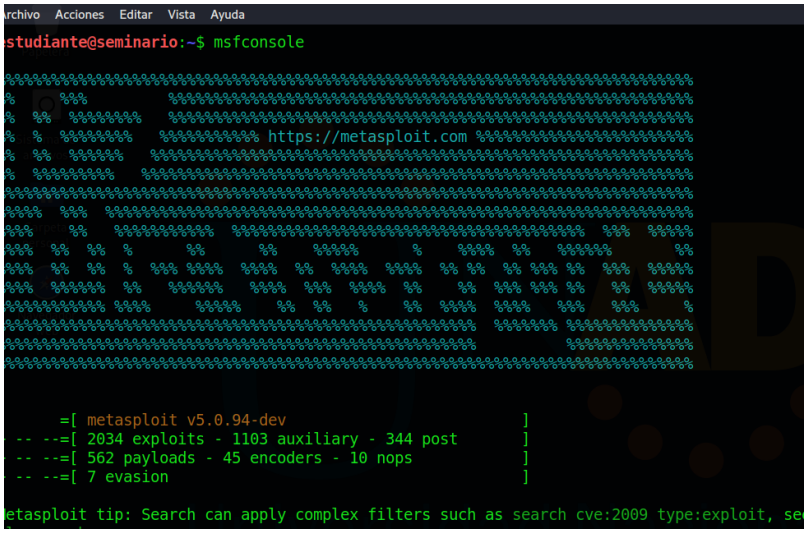
Ilustración 17; Ping 10.0.2.5



Fuente: elaboración propia

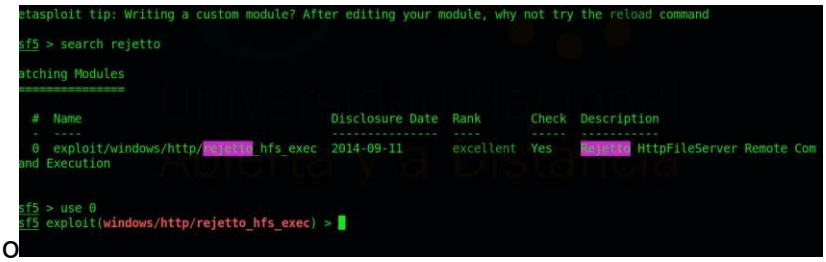
Hay conexión entre las maquinas

Ilustración 18:msfconsole



Fuente: elaboración propia

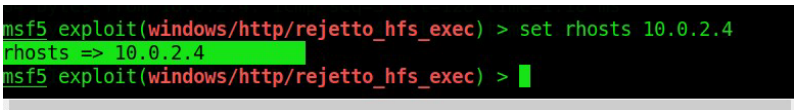
Ilustración 19:Search rejetto



o

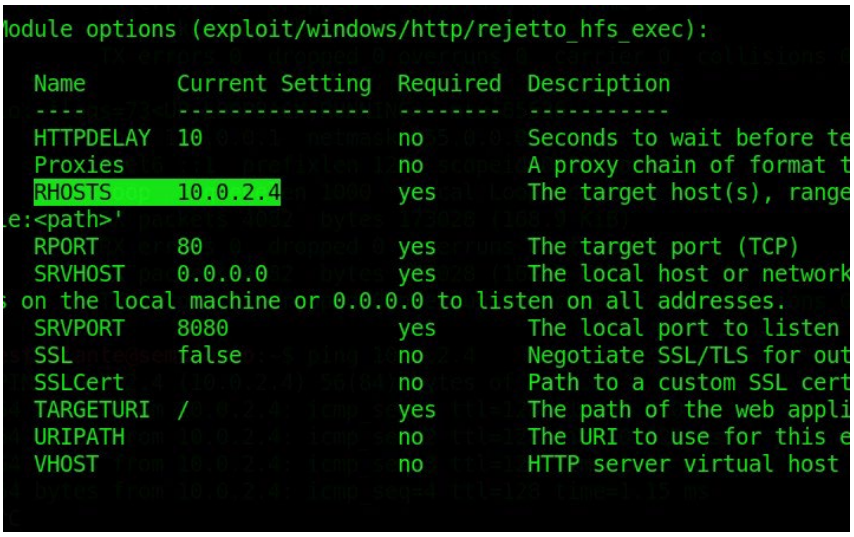
Fuente: elaboración propia

Ilustración 20:Set rhosts 10.0.2.4



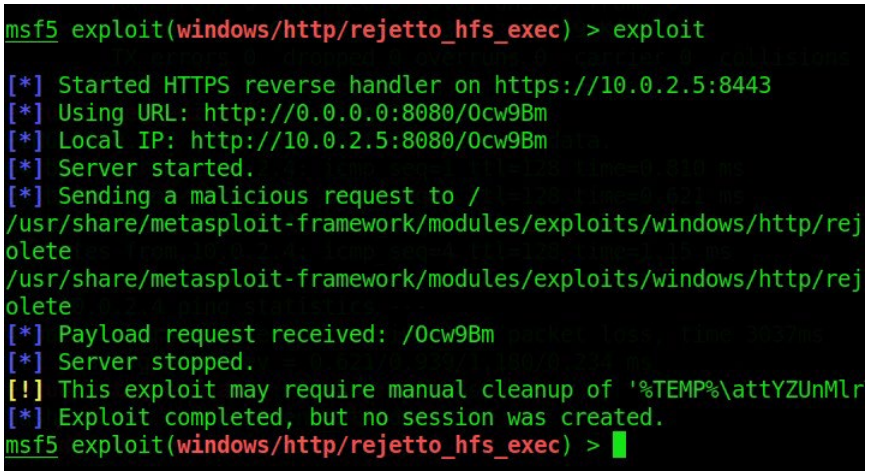
Fuente: elaboración propia

Ilustración 21:show options



Fuente: elaboración propia

Ilustración 22:Exploit



Fuente: elaboración propia

Análisis de Vulnerabilidades

Dentro de la fase del pentesting como herramienta se utilizó Nmap.

Nmap: herramienta que sirve para realizar el escaneo de puertos, además de los servicios que se encuentran alojados en ellos, también se puede ver que puertos se encuentran abiertos, filtrados o cerrados. Esto permite identificar las vulnerabilidades una vez detectados los puertos abiertos, sus servicios y versiones de estos.[20]

Comandos en nmap:

-sV: en los puertos que encuentra abiertos busca los servicios y la versión de los servicios que se alojan en esos puertos

Estrategias de contención

Al ser un ataque en tiempo real, se debe desconectar los equipos que se encuentren conectados a la red, o los equipos que se considere que pueden estar afectados con el ataque. Se debe tener en cuenta que al momento de descubrir la vulnerabilidad ya pudieron haber extraído información valiosa para la empresa o que ya se pudieron haber realizado daños en los equipos, por lo tanto, es necesario iniciar con la valoración tanto de los equipos como también de la información además del impacto que género. Se debe identificar el punto débil por el cual se generó el ataque y también los involucrados que permitieron que tuviera éxito.

Actividades para realizar

- Se deben realizar copias de respaldo de la información a las máquinas y activos afectados, y realizar la aplicación de técnicas forenses para determinar cuáles fueron los atacantes. Además de revisar las copias de seguridad que se hayan realizado antes del ataque para recuperan información que se haya perdido durante el ataque.
- Se debe documentar los procesos y resultados obtenidos.

[20] Linux-Console.net. Una guía práctica para Nmap (Network Security Scanner) en Kali Linux. Recuperado de: https://es.linux-console.net/?p=1608#gsc.tab=0

- Evitar la instalación de herramientas remotas, ya que esto puede generar a fetaciones en el sistema atacado.
- Se debe realizar la revisión por un profesional que cuente con los conocimientos necesarios y las herramientas pertinentes para que la integridad de los activos no sea afectada.

Medidas de prevención

Debido a que se generó el atraque a través de la vulnerabilidad que tenía la aplicación rejetto, instalada en la máquina windows 7 X64, se deben establecer medidas para que no se vuelvan a presentar este tipo de ataques.

- El sistema operativo debe tener actualizaciones en su última versión, con el fin de que implementen las mejoras, rendimiento y seguridad que debe tener.
- Las aplicaciones que se instalen deben ser licenciadas, además de ser instaladas por personas autorizadas, por lo tanto, se deben generar credenciales de acceso para instalación.
- Se debe realizar la revisión de los puertos para identificar cuales se encuentran abiertos y que servicios se encuentran en cada uno. Las aplicaciones por lo general requieren de estar alojadas en un puerto para su adecuado funcionamiento, por lo que se recomienda cambiar el puerto por otro que sea menos frecuentes pero que sean reconocibles al servicio.
- Los usuarios que cuenten con acceso remoto no deben tener permisos de privilegios de administrador, con el fin de que no pueda habilitar ningún servicio.
- Cada servidor debe tener un usuario administrador con contraseñas de acceso.
- Contar con un firewall que se encuentre activado en cada una de las maquinas estableciendo reglas de filtrado de acuerdo con las necesidades de cada usuario.
- El antivirus debe ser licenciado y con actualizaciones periódicas.

Etapa 4: Contención de ataques informáticos

Ilustración 23: situación problema: análisis Blue Team

Situación problema: Análisis Blue team

WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

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

Es importante al iniciar con una indagación para conocer las políticas que se encuentran establecidas en la empresa, ya que, al conocer el modelo de gestión de incidentes de seguridad de la información, se puede decir que se tiene uno de los elementos que ayudará a identificar cuáles fueron las falla que permitieron que el ataque en tiempo real se ejecutará. Además de establecer medidas estratégicas para evitar que otros equipos puedan ser atacados.

De lo contrarios es importante que la empresa inicie con la implementación de dichas políticas que permitan la tomade decisiones de forma acertada, teniendo en cuenta que la vulnerabilidad se presentó debido a la aplicación que se estaba ejecutando en el ordenador Windows X64.

De acuerdo con lo anterior la indagación busca encontrar las medidas para la contención de los incidentes, con el fin de que se pueda identificar las vulnerabilidades que se encuentran presentes y así mismo poder evitar daños en la infraestructura de la empresa, para implementar la contención de lo9s ataque es

que la empresa dentro de sus políticas debe definir en qué momento se debe apagar el sistema, además de desconectar la red y deshabilitar los servicios.

Los criterios que se definen para la contención de los incidentes deben quedar documentados, esto con el propósito de que los informes que se presenten sean claros, y de este modo se puedan tomar las decisiones pertinentes.

b. ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

El proceso de endurecimiento del del sistema se debe implementar con base en las políticas establecidas, ya que por medio de la hardenización se puede asegurar que los servidores de la empresa estén protegidos ante cualquier ataque cibernético que se pueda presentar, así mismo, reducir los puntos posibles donde el atacante puede entrar sin autorización.

Teniendo en cuenta que ya se produjo un ataque en tiempo real es necesario que las medidas para garantizar la seguridad de los servidores por medio de herramientas de automatización de endurecimiento, herramientas de administración y configuración, escáneres de cumplimiento y herramientas gratuitas de código abierto, debido a que la empresa no cuenta con un presupuesto para adquirir herramientas pagas.

Después de establecer una política de hardenización, se deben establecer las 3 etapas que la componen con el propósito de obtener resultados acordes con las necesidades de seguridad que se reflejan en esta empresa.

Inicialmente se debe realizar el reconocimiento de la infraestructura TI, lo que permite realizar las pruebas que permitan bloquear cualquier vector de ataque, es por eso que se requiere conocer todas dependencias que se encuentren en la red, para finalmente crear un entorno de prueba que simule la red, así mismo, aplicar los

cambios que conllevan a tener claridad del impacto que genera la regla a cada aplicación o servicio.

Posterior a estas pruebas se debe relacionar los resultados a las directivas de la empresa, con el propósito de tomar las decisiones de acuerdo con los impactos que se generen en cada una de las reglas a implementar.[21]

Después de que sean aprobados los resultados de la prueba por las directivas en cada uno de las aplicaciones y servicios se debe continuar con el proceso aplicación y cumplimiento con la asistencia de herramientas.

Por último, se requiere de un monitoreo para supervisar y corregir los cambios intencionales o involuntariamente que se puedan generar.

c. ¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Tabla 1:Equipos Blue team y equipos de respuesta a incidentes informáticos

Blueteam	**Equipo de respuesta a incidentes informáticos**
Identifica las vulnerabilidades que se presentan en un sistema	Ofrece protección ante los ataques que se presenten
Realiza el proceso de identificación, clasificación y priorización para la gestión de vulnerabilidades, además de categorizar los activos	Gestiona los incidentes de seguridad por medio de las etapas de detención, contención, erradicación y recuperación

[21] MARTÍNEZ CARPINTERO, María Cristina. GITT. Desarrollo de un entorno virtual para pruebas de hacking y hardenización. 2020.Recuperado de: https://ruidera.uclm.es/xmlui/handle/10578/26086

Analiza las vulnerabilidades encontradas en los sistemas	Realiza monitores constantes en el sistema para recolectar información como evidencia
Identifica y verifica que las vulnerabilidades se encuentren mitigadas	Verifica que el incidente haya sido atendido y remediado

En la anterior tabla se relacionan las diferencias que se encuentran en los equipos Blueteam y un equipo de respuesta a incidentes informáticos.[22]

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

Si la indicación es que se trabaje con CIS "Center For Internet Security" se implementaría como controles para la administración de accesos a las cuentas, para salvaguardar, defender y mitigar los ataques que se presentan con mayor frecuencia contra sistemas de información.

Teniendo en cuenta que la principal función de CIS es proteger la empresa u organización de ataques cibernéticos y teniendo ya el antecedente del ataque generado por la aplicación rejetto, se implementaría para salvaguardar del hacking de aplicaciones web, uso debido de privilegios, accesos autorizados y malware.[23]

d. Explique y redacte las funciones y características principales de lo que es un SIEM.

SIEM, "Gestión de eventos e información de seguridad", es una herramienta con la cual se puede realizar la recolección de información de forma centralizada para ser enviada a los dispositivos de seguridad que se encuentran en la red. Esta también

[22] MORALES MORALES, Ricardo, et al. Capacidades técnicas, legales y de gestión para equipos blue team y red team. Recuperado de https://repository.unad.edu.co/handle/10596/40283
[23] MORENO MORENO, Adriana, et al. Diseño e implementación en Avianca de los controles 5 (administración de cuentas) y 6 (gestión de control de acceso) de la guía de controles cis-center for internet security (r) y diseño de la metodología para la integración de aplicaciones en la herramienta de gestión de identidades. 2022. Recuperado de file:///C:/Users/diana/Downloads/Tesis%20Grado%2021%20Abril.pdf

la encargada de analizar, recolectar y normalizar la información de tal manera que pueda ser utilizada para establecer las posibles amenazas que se puedan generar en el sistema.

Funciones de SIEM

- Centraliza el almacenamiento de la información que recibe desde Los dispositivos y logs, para realizar análisis en tiempo real.
- Ayuda a la toma de medidas defensivas de forma inmediata.
- Realiza la recopilación de información con el propósito de generar informes qué permiten la identificación de eventos a través de los análisis.
- Normaliza el proceso de información con horas y fechas de modo que las búsquedas que se realicen tengan resultados efectivos y rápidos

Características de SIEM

- **Monitoreo:** realiza monitoreos periódicos en los archivos que transitan en la red, con el fin de garantizar la integridad, confiabilidad y disponibilidad de la información.

- **Análisis:** el profesional encargado de monitorear los archivos que transitan por la red debe contar con los conocimientos necesarios para detectar el tráfico que se encuentre alterado y así mismo crear alertas que peritan tomar las medidas necesarias para identificar la amenaza presente.

- **Gestión:** se identifican las alertas, además de realizar la gestión de los logos que se encuentran relacionados con las acciones que se desarrollan en la mitigación de las vulnerabilidades encontradas.

- **Respuesta:** realizar el proceso de integración de todos los dispositivos de seguridad, además de establecer acciones automáticas que puedan mitigar o detener los ataque se generen

    e. Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las

herramientas de contención son diferentes a las herramientas dedetección.

- **Firewalls:** Es una herramienta que se puede implementar en el hardware y en e software, con el fin de que se pueda establecer cuáles son los servicios a los cuales se le puede generar accesos. Además, se pueden establecer niveles de monitorización, control y respuesta que se requiere en la empresa.[24]

- **Proxi:** Esta herramienta es una solución que se puede implementar en la capa de aplicación con el propósito que se intercepte toda la información que transite por la red, garantizando de esta forma que los accesos sean seguros, autorizados y confiables. [25]
- **VPN**: con la implementación de una VPN, se puede establecer la privacidad en la navegación de la red empresarial, ya que al ser una red privada permite la autenticación y cifrado que se puede generar entre dos puntos finales. Una vez cread o el túnel de la VPN, se puede tener acceso a diferentes recursos y servicios.

[24] CUENCA, Jackson. Firewall o cortafuegos. *Universidad Nacional De Loja*, 2016.Recuperado de: https://www.researchgate.net/profile/Jackson-Cuenca/publication/295256426_FIREWALL_O_CORTAFUEGOS/links/56c8a7ed08ae96cdd06baf7c/FIREWALL-O-CORTAFUEGOS.pdf

[25] GÓMEZ, Carlos E.; SEPÚLVEDA, Luis E.; CANDELA, Christian A. Servidor Proxy Caché: Comprensión y asimilación tecnológica. *Revista INGE CUC*, 2012, vol. 8, no 1, p. 149-162. Recuperado de: https://d1wqtxts1xzle7.cloudfront.net/75224566/Dialnet-ServidorProxyCache-4869011-libre.pdf?1637941565=&response-content-disposition=inline%3B+filename%3DServidor_Proxy_Cache_Comprension_y_asimi.pdf&Expires=1679879570&Signature=Kw39mTtshsiRMwB42NrHYo8OiHDKa~OPAhrMQLzAHyP6z3fCLGct8sf9qwN6VALKCH2vd76wSwatOe-G-7HUTe4Mt~xwxb371ChYOLba56rDZZIKBpgzCu83YikL1ZyYEghDiDVaJkgz1rh1tXjpiqj~c93PFpMA40TnCqu7v0YdF1963YU2MzxGY-iBI8awXvyc0CNAzPPX5pmDcWhNQ0mhXR5ntGB8gxUizgYQrfCSt-t5u7F8aSlVOYzQPN1uXYwWMD3pHuLMdVwyTnj-giygqCJinQCXfRUJTUqu3LhF9BoC077i8lMldjQ6kaqbpmPcUL9KxlYMLevD0nw9IQ &Key-Pair-

4. CONCLUSIONES

Es importante que las empresas tengan presentes los procesos de seguridad de la información ayudan a proteger sus activos informáticos, no quiere decir que si no se ha presentado ningún evento no se corra riesgos de sufrirlos en cualquier momento, es por eso qué los equipos de Red Team & BlueTeam, son estrategias que no se deben descargar si su propósito es proteger la infraestructura tecnológica de la empresa.

Los procesos que realizan los equipos de Red Team & BlueTeam, dan una clara visualización de los puntos que se deben fortalecer, además de los tiempos en los que se deben realizar los monitoreos.

5. RECOMENDACIONES

Desde el área de seguridad informática se relacionan a continuación las siguientes recomendaciones y estrategias que permitan contar con una infraestructura TI, segura y confiable.

- Actualización permanente de los sistemas operativos y programas que se manejen, para asegurar que los parches de seguridad se encuentren al día, también es importante contar con un servidor de actualizaciones.
- La instalación de los sistemas operativo y software licenciado es una de las estrategias que puede ayudar a que obtener las actualizaciones de seguridad, protegiendo de amenazas como los troyanos y virus que traen los productos piratas.
- Se recomienda establecer una política de seguridad si no se cuenta con ella, ya que esto permite identificar cuáles son los puntos más relevantes a los que se les debe establecer un contante monitoreo.
- Dentro de la política se debe establecer las capacitaciones a empleados para crear culturas responsables de la seguridad de la información ya que muchas vulnerabilidades pueden ser a causa de errores humanos, debido a que en repetidas ocasiones no tienen el conocimiento de los riesgos que se pueden generar ante el descuido de procesos inadecuados.
- Los equipos que hagan parte de un sistema de seguridad deben contar con los conocimientos necesarios, ya que esto permite realizar los procesos de monitorio con mejor precisión y óptimos resultados.
- Los procesos que se realicen deben quedar documentados, esto con el fin de que los informes que se realicen sean claros y entendibles

bien sea para presentar a las directivas como también para tener un historial que pueda ayudar a otros profesionales a identificar cuáles son los riesgos que se viene presentando y así mismo poder agilizar su trabajo dentro del área.

Enlace del vídeo de sustentación

https://www.youtube.com/watch?v=jXtoAKONwKg

6. BIBLIOGRAFIA

AMÉZQUITA DURAN, Jorge Alonso, et al. Capacidades técnicas, legales y de gestión para equipos blue team & red team. 2021.recuperado de: https://repository.unad.edu.co/handle/10596/43170

AVG. ¿Qué es un exploit en seguridad informática? [consultado el 30 de noviembre de 2022]. Recuperado de: https://www.avg.com/es/signal/computer-security-exploits

ALTUBE VERA, Rafael. ¿Qué es OpenVAS?.11 noviembre 2020. Recuperado de: https://openwebinars.net/blog/que-es-openvas/

BUITRAGO, Felipe Márquez. Aplicación de la ley estatutaria 1581 de 2012 a la red social facebook en colombia. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 2016, no 15, p. 1.

ECHARA PALACIOS, Yenifer Yirlesa, et al. Análisis jurídico de la ley 1273 del 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informáticos. 2020. Recuperado de: http://www.repositorio.unacar.mx/jspui/handle/1030620191/200

CANO, Jeimy J. Ciberataques. *Revista Sistemas*, 2020, no 157, p. 67-74 disponible en https://sistemas.acis.org.co/index.php/sistemas/article/view/129/101

CUENCA, Jackson. Firewall o cortafuegos. *Universidad Nacional de Loja*, 2016.Recuperado de: https://www.researchgate.net/profile/Jackson-Cuenca/publication/295256426_FIREWALL_O_CORTAFUEGOS/links/56c8a7ed08ae96cdd06baf7c/FIREWALL-O-CORTAFUEGOS.pdf

DOMÍNGUEZ, Hernán M., et al. Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple “Contraseñas”, pruebas de concepto con software libre y su remediación. *Maskana*, 2016, vol. 7, p. 87-95. Recuperado de: https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1079

FRANCO, David A. PEREA, Jorge L. TOVAR, Luis C. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Universidad

de Cartagena, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, Vol. 24(5), 13-22 (2013). Recuperado de: https://www.scielo.cl/pdf/infotec/v24n5/art03.pdf

GONZÁLEZ THOLA, Diego Fernando, et al. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam. Recuperado de https://repository.unad.edu.co/handle/10596/48105

GARZÓN GARCÍA, Janier Rolando. Protección de datos personales Ley 1581 octubre 2012. 2015. Tesis de Licenciatura. Universidad Piloto de Colombia. Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/2937

MAROTO, Juan Puime. El ciberespionaje y la ciberseguridad. En *La violencia del siglo XXI. Nuevas dimensiones de la guerra*. Instituto Español de Estudios Estratégicos, 2009. p. 45-76. Recuperado de: file:///C:/Users/diana/Downloads/Dialnet-ElCiberespionajeYLaCiberseguridad-4549946%20(2).pdf

Mintic. (2009). Ley 1273 [LEY_1273_2009]. Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

POSSO RODELO, Johana; BARRIOS BARRIOS, Mauricio. Diseño de un modelo de control interno en la empresa prestadora de servicios hoteleros ecoturísticos nativos activos eco hotel la cocotera, que permitirá el mejoramiento de la información financiera. 2014. Tesis Doctoral. Universidad de Cartagena. Recuperado de: https://repositorio.unicartagena.edu.co/handle/11227/2130

SÁNCHEZ CASTILLO, Zulay Nayiv, et al. Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. 2017. Recuperado de: https://repository.unad.edu.co/handle/10596/11943

SANTIAGO PEREZ, Judith Del Carmen, et al. METASPLOIT. una visión introductoria. 2011. Recuperado de: http://www.repositorio.unacar.mx/jspui/handle/1030620191/200