MANUAL DE BUENAS PRACTICAS DE SEGURIDAD INFORMÁTICA EN REDES DOMESTICAS

DIDIER FERNANDO HURTADO VALERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI.
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

MANUAL DE BUENAS PRACTICAS DE SEGURIDAD INFORMÁTICA EN REDES DOMESTICAS

DIDIER FERNANDO HURTADO VALERO

Proyecto de Grado - Monografía presentada para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor:
Miguel Andrés Ávila Gualdrón
Magister en Ciberdefensa

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIA BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, Fecha de sustentación

DEDICATORIA

A Dios, que me regala esta experiencia de vida, a mi amada hija que ha sido el motor que mueve esta etapa de mi vida, a mis padres que han sido el fuerte soporte del esfuerzo, sacrificio y trabajo que representa este trabajo y a todos quienes han hecho parte de esta experiencia.

AGRADECIMIENTOS

Con el más grande y sincero sentimiento de agradecimiento a Dios y a mi familia quienes hacen posible la realización de este trabajo, adicionalmente a la Universidad Nacional Abierta y a Distancia UNAD por brindarme la mediación y el conocimiento para la realización como especialista.

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

AMENAZA: Cualquier elemento que pueda generar daños dentro de un sistema, esto puede ser perdida, sustracción, destrucción o alteración de la información, esto implica una situación adversa para los activos que puede llegar a causar serios problemas en la información.

ACTIVO DE INFORMACIÓN: Es cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización

ADWARE: Programa creado con ánimo de lucro tiene la característica de mostrar publicidad de forma automatizada. Aunque se asocia al malware, no tiene que serlo forzosamente, ya que puede ser un medio legítimo usado por desarrolladores de software que lo implementan en sus programas, generalmente en las versiones shareware, haciéndolo desaparecer en el momento en que adquirimos la versión completa del programa. Se convierte en malware en el momento en que empieza a recopilar información sobre el ordenador donde se encuentra instalado

ANTIVIRUS: Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware.

ALGORITMO DE CIFRADO: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida. Existen dos tipos de cifrado atendiendo a las características de las claves de cifrado, estos son el cifrado simétrico y cifrado asimétrico.

AUTENTICACIÓN: Procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

BOTNET: Una red de equipos construida con el fin realizar tareas automáticas, controlados de forma remota y con la capacidad de causar daños siguiendo instrucciones.

CABALLO DE TROYA: Es un tipo de virus que utiliza un programa legítimo para infiltrar código malicioso dentro de una o varias computadoras.

CIBERCRIMEN: Actividad con carácter de delito donde se usan recursos tecnológicos con el objetivo de cometer un crimen.

EXPLOITS: Códigos maliciosos que se utilizan aprovechando las vulnerabilidades de programas y sistemas operativos.

FIREWALL: Elementos de software hardware con la capacidad de identificar y bloquear intrusiones dentro de un sistema.

GUSANOS: Tipo de código malicioso con la capacidad de propagarse dentro de un sistema, en estos casos el usuario no puede percibirlo.

INGENIERIA SOCIAL: Técnica para el robo de información, donde se engaña al usuario con el fin de tomar datos personales para ser usados posteriormente con fines de fraude.

INTERNET: Interconexión de redes conocido como www (World Wide Web)

KEYLOGGER: Código que permite tomar de una maquina lo que se está tecleando, registra los pulsos del teclado y los envía a un destino como puede ser un servidor u otro equipo.

PHARMING: Técnica que altera los hosts redirigiendo el tráfico y modificando direcciones ip, tiene la capacidad de capturar información confidencial.

PHISHING: Técnica que permite la captura de información por medio del montaje de sitio y páginas web falsas.

SOFTWARE MALICIOSO: Programa no deseado y potencialmente peligroso que puede causar graves daños a un sistema informático.

SPYWARE: Programas que se crean con el fin de robar información, se introducen dentro de un sistema aprovechando las vulnerabilidades de seguridad de este.

VULNERABILIDAD: Debilidad en seguridad con la que puede llegar a contar un activo o un sistema informáticos.[1]

[1] COURSE TECHNOLOGY. 2004. Diccionario de Informatica E Internet: Computer and Internet Technology Definitions in Spanish. Montreal : Ed. Cengage Learning, 2004. 221 p. ISBN 9780619267889.

RESUMEN

En la era digital, uno de los activos más valiosos es la información, no solamente para las empresas sino, también, para las personas, por ende, es natural pensar que la información corre riesgo y se encuentra ante constantes amenazas identificadas y catalogadas, bien sean virus, malware, adware, spyware, ciberdelincuencia y muchas más.

Amenazas que día a día crecen dada la conexión a internet desde distintos tipos de dispositivos como computadoras, equipos portátiles, servidores, equipos celulares, tabletas etc., que utilizan la red para la comunicación en diversas formas.

El tema está centrado en la seguridad en redes domésticas, partiendo de la identificación de vulnerabilidades, seguridad en redes informáticas y algunos ataques que pueden sufrir estas, con el fin de entregar una serie de recomendaciones, métodos de detección y prevención de actividad maliciosa, que permita minimizar los riegos en este tipo de redes.

Para esto, se da a conocer conceptos del tema de la seguridad informática, junto a algunos métodos y técnicas disponibles para detectar, corregir y sobre todo prevenir daños que puedan surgir por incidentes relacionados con el mal uso o mala configuración en redes domésticas.

Este conocimiento aporta al lector la seguridad que debe tener al usar tecnología, fundamentándolo en temas de ciberseguridad y riesgos, amenazas latentes en internet, las vulnerabilidades que puede llegar a tener un sistema y la forma de mitigar y prevenirlos.

Hoy en día la información está expuesta a riesgos tanto físicos como lógicos, siendo los riesgos físicos los que se presentan por la ubicación física de los equipos de cómputo dentro de un entorno y afectan el hardware, y pueden ser causados no de forma intencional sino muchas veces de forma accidental, a diferencia de los riesgos lógicos, que se caracterizan por ser creados por las propias personas con el fin de realizar daños en los sistemas bien sean de una compañía o en el hogar.

Dentro de lo que puede pasar por riesgos lógicos se encuentra el robo de información, robo de cuentas bancarias o claves personales con el fin de realizar transferencias de dinero sin autorización y todo tipo de fraudes.

Teniendo en cuenta lo anterior, en este documento se busca realizar la identificación de ciertas vulnerabilidades y riesgos de seguridad en redes domésticas, al igual, que el desarrollo del respectivo análisis para el diseño de unos pasos metódicos orientados a buenas prácticas que el usuario final pueda tener en cuenta para minimizar los riesgos en redes domésticas y resguardar su valiosa información.

Lo anterior, enmarcado dentro de los pilares de la seguridad informática, es decir, para la protección de la: confidencialidad, integridad y disponibilidad de la información, para garantizar que la información sea divulgada de forma segura, no sea modificada o alterada, y este disponible bajo protocolos de seguridad.

El usuario de servicios de tecnología en el hogar está expuesto a ataques provenientes de otros usuarios conocidos comúnmente como hackers, quienes pueden infiltrarse en una red violando la seguridad y extrayendo información sensible sin ningún consentimiento.

Por esta razón, la realización de pruebas para la identificación de vulnerabilidades y el apoyo documental de este documento ayuda a develar riesgos y prepara al usuario para minimizar los mismos siguiendo mediante la aplicación de buenas prácticas en seguridad informática.

Palabras clave: Seguridad en redes, zona desmilitarizada, cortafuegos, hacking, hacking ético, máquina virtual, malware, phishing, cracker.

ABSTRACT

In the digital age, one of the most valuable assets is information, not only for companies but also for people, therefore it is natural to think that information is at risk and faces constant threats that have been identified and cataloged Be it viruses, malware, adware, spyware, cybercrime and a great many that add to them. Threats that grow every day given the Internet connection from different types of devices such as computers, laptops, servers, cell phones, tablets, etc., which use the Internet for communication in its various forms.

The content is focused on the topic of security in home networks, starting from the identification of vulnerabilities, security in computer networks and some attacks that may suffer, in order to deliver a series of recommendations and methods of detection and prevention of malicious activities, that allow minimizing the current risks in this type of networks.

Concepts of the subject of computer security are disclosed, accompanied by some methods and techniques available to detect, correct and above all prevent damages that may arise from incidents related to misuse or misconfiguration in home networks.

This knowledge provides the reader with the security they should have using technology, basing it on cybersecurity and risk issues, latent threats on the internet, the vulnerabilities that a system may have and the way to mitigate and prevent them.

The information is exposed to both physical and logical risks, being the physical risks those that are presented by the physical location of the computer equipment within an environment and affect the hardware, and can be caused not intentionally but often by accidentally, as opposed to logical risks, which are characterized by being created by people in order to damage systems, whether they are in a company or in the home. Among what can go through logical risks is the theft of information, theft of bank accounts or personal keys to make money transfers without authorization and all kinds of fraud.

It seeks to identify certain vulnerabilities and security risks in home networks, as well as the development of the respective analysis for the design of some methodical steps oriented to good practices that the end user can take into account to minimize risks in networks home and safeguard your valuable information.

The foregoing, framed within the pillars of computer security for the protection of: confidentiality, integrity and availability of information, to ensure that the information is disclosed safely, is not modified or altered, and is available under protocols of security.

The user of technology services at home is exposed to attacks from other users, who can infiltrate a network violating security and extracting sensitive information without any consent, for this reason. The tests to identify vulnerabilities and the documentary support of this document help to bring risks to light and prepare the user to minimize risks by following good practices.

Keywords: Network security, demilitarized zone, firewall, hacking, ethical hacking, virtual machine, malware, phishing, cracker.

INTRODUCCIÓN

Día a día se presentan incidentes de seguridad informática, acompañados de nuevas técnicas y atacantes que intentan evadir la seguridad y vulnerar de alguna forma la información con diferentes propósitos, el riesgo aumenta por el desconocimiento de los riesgos y la falta de conciencia de los usuarios, por ende, el tema de la seguridad se ha vuelto coyuntural y debe ser tomado con propiedad en todos los ámbitos de la vida diaria.

Este tema abarca detección de intrusos, programas maliciosos, redes inseguras y otros, y desde ellos realizar constantes pruebas que permitan ampliar el conocimiento acerca de prácticas seguras y protección de la información ante la constante lluvia de ataques que se vive actualmente.

Aunque pueda parecer que todo marcha bien, la realidad es que no existe un sistema 100% seguro, o que esté fuera de ser blanco de ataques o infiltración, por lo cual, se requiere tener una búsqueda constante de vulnerabilidades y métodos eficientes que permitan la mejora constante de la seguridad.

Por lo anterior, el tema de análisis de seguridad en redes domésticas cobra especial relevancia en la cotidianidad personal y profesional, lo que lo convierte en un tema relevante dentro de la seguridad informática.

A pesar de lo que se escucha acerca de los riesgos existentes y los peligros que se viven en el ámbito tecnológico, al parecer el interés va en contravía de los incidentes en seguridad informática. Incluso, dentro de la gerencia de las organizaciones esto parece no ser una prioridad, o se tiene poco interés en el tema.

Según una encuesta realizada por la consultora Ernest & Young, más del 80% de consultados coincidió en que “la seguridad informática no se encuentra entre las prioridades de los CEO de las empresas. Ese estudio se realizó en 1235 organizaciones de distintas industrias que representan algunas compañías líderes en 51 países”. [2]

De acuerdo con esta misma encuesta, también se concluye que lograr la conciencia del usuario final es lo más difícil de lograr, porque, aunque se les brindan

[2]ERNEST & YOUNG. 2004. El Diario Exterior. *La seguridad informática en las empresas no es la prioridad, a pesar de los ataques.* [En línea] 22 de 11 de 2004. https://www.eldiarioexterior.com/articulo.asp?idarticulo=2356.

capacitaciones constantes, la mayoría de las personas continúan dejando sus contraseñas a la vista, escritas en cuadernos y notas encima de los escritorios o lugares visibles para cualquier persona, también cabe resaltar que persisten en usar contraseñas de bajo nivel de seguridad para el ingreso a los sistemas en sus lugares de trabajo y también en el hogar.

Así como hay quienes se encargan de hacer redes cada vez más seguras, hay otros actores como los crackers que se encargan de buscar cada día nuevas vulnerabilidades, explorando formas de hacer daño dentro de una red, husmeando o sacando información sin autorización y sin que nadie se dé cuenta, con o sin ánimo de lucro.

Es importante destacar que todos los sistemas se encuentran en una constante evolución, por lo tanto, es necesario permanecer actualizado en temas de seguridad informática, aún más si tenemos en cuenta que nos encontramos en la llamada era de la información, en la que el margen de error se reduce y a los profesionales se les vuelve un verdadero reto proteger los pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad)

Por tal motivo, es importante realizar una constante investigación documental que permita ampliar el conocimiento acerca de los riesgos actuales y potenciales en el ciberespacio e identificar las vulnerabilidades existentes en una red doméstica, para lograr la realización de un análisis de seguridad informática que permita poner en práctica nuevas técnicas que aseguren la información y minimice la exposición a ataques que vulneren la seguridad.

Dentro de los aspectos que permiten entender el presente trabajo se debe comenzar por tener claro que lo que se quiere proteger es la información y los datos sensibles, tratando temas como: análisis de vulnerabilidades, firewalls, políticas de seguridad, términos y protocolos para la transmisión de información, al igual, que algunos servicios y buenas prácticas que permitirán mejorar el uso de las redes y beneficiaran al usuario y aumentará la seguridad presente en los dispositivos y los servicios de comunicación.[3]

[3]BACH, Mario. 2017. INFORMÁTICA 2ºBACH MARIO. *SEGURIDAD INFORMÁTICA VI.* [En línea] 19 de 10 de 2017. http://2bconsmario.blogspot.com/2017/10/seguridad-informatica-vi.html.

1. DEFINICIÓN DEL PROBLEMA

Las personas usan los sistemas de información y la infraestructura de internet de forma cotidiana, y es común que todos confíen plenamente en la implementación de seguridad por defecto de su proveedor de servicios, debido a que se tiene un desconocimiento general de las vulnerabilidades que pueden tener los sistemas dentro del hogar.

Esto permite, que en muchas ocasiones pase desapercibido ante el usuario algunos riesgos de seguridad presentes en los sistemas informáticos, tales como errores de configuración, faltas a las buenas prácticas en seguridad o fallas propias del software utilizado, generando una falsa percepción de seguridad que oculta los riesgos existentes.

1.1 ANTECEDENTES DEL PROBLEMA

A la par del avance tecnológico surge cada día nuevos ataques y peligros en el uso de servicios en red, con métodos más sofisticados dirigidos a los usuarios de redes domésticas.

El comercio electrónico es uno de los medios que más se utiliza para elaborar ataques, debido a que por medio de técnicas como la ingeniería social se ofrecen productos, servicios y recompensas que logran atraer a los usuarios para ser engañados y robar su información personal, en la mayoría de los casos los ciberdelincuentes están en una búsqueda constante de beneficios económicos por medio de la explotación de las brechas de seguridad existentes en las redes.

La presente monografía tiene como punto de partida referencial una exploración a la documentación contenida en el trabajo de grado como Especialista en Seguridad Informática realizado por Anggie Katherin Ovalle Vélez titulado “Uso de herramientas informáticas para descubrir vulnerabilidades en las redes Wifi-domésticas” y presentado a la Universidad Católica de Colombia. Dicho documento tiene como objetivo el diseño de un manual de identificación de vulnerabilidades en redes hogareñas por medio de la realización de pruebas con el fin de vulnerar la seguridad de redes WiFi.[4]

[4] OVALLE, Anggie Katherine. 2019. Uso de herramientas informáticas para descubrir vulnerabilidades en las redes wifi domesticas. Bogotá : s.n., 2019.

En este trabajo, se encontró que generalmente se usa de forma inadecuada la seguridad en los dispositivos del hogar, por algunas razones sencillas como: la desactualización de software y la falta de medidas por parte del usuario en el control de los dispositivos conectados a su red por el desconocimiento del tema.

Adicionalmente, en el trabajo de grado titulado “Protocolos para la mitigación de ciberataques en el hogar” realizado por Camilo Alfonso Guzmán Flórez y Cristian Andrés Angarita Pinzón y presentado a la Universidad Católica de Colombia en el año 2017, se identifican vulnerabilidades y riesgos con el fin de tomar medidas [5]preventivas y correctivas para incrementar la seguridad de la red del hogar mediante la propuesta de un protocolo para mitigar ataques en la red doméstica.

Luego de la realización de este trabajo se encontró que el uso inadecuado de la tecnología trae consecuencias contraproducentes para la población que abarcan desde al ámbito económico hasta el social del individuo, además, se deduce que la implementación de niveles de seguridad en el hogar es baja, adicionalmente, considera que las investigaciones acerca del tema de seguridad informática en el hogar son bajas, por lo cual, investigaciones de este tipo permiten profundizar en este tema y generar una mayor seguridad para los usuarios en sus redes domesticas

Desde los inicios y expansión de las redes informáticas se presentan problemas de seguridad, razón por la que la inversión de recursos en materia de seguridad informática ha aumentado para maximizar la atención de incidentes y la recuperación ante desastres cibernéticos.

En el último trimestre de 2019 los incidentes cibernéticos tuvieron un aumento del 54% respecto al año inmediatamente anterior, hallazgo que hace parte del estudio de tendencias del cibercrimen en Colombia, realizado por entidades como Tanque de análisis y creatividad de las TIC, la Cámara Colombiana de Informática y Telecomunicaciones, y el Centro de Capacidades para la Ciberseguridad de Colombia C4 de la Policía Nacional.[6]

[5] GUZMAN, Camilo Alfonso y ANGARITA, Cristian Andres. 2017. PROTOCOLOS PARA LA MITIGACION DE CIBERATAQUES EN EL HOGAR. Bogotá : s.n., 2017.

[6] TECNOSFERA, REDACCION. 2019. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. El Tiempo. Bogotá. Recuperado de: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790 (30 de Octubre). 2019. 2019.

Según el estudio se muestra que el delito más denunciado en Colombia es el hurto por medios informáticos, seguido del robo de identidad. El estudio indica que la mayor motivación para cometer los crímenes en Colombia es el beneficio económico, por lo cual se encuentran modalidades como phishing con el 42%, suplantación de identidad con 28%, envío de malware con 14%, y fraudes con pagos en línea con el 16% del total de ataques reportados.

Este mismo reporte reitera que el ramsomware es una de las principales amenazas para Colombia ya que este tipo de ataque en el país está por encima de otros de la región como Perú (16%), México (14%), Brasil (11%) y Argentina (9%).[7]

Está de acuerdo en que lograr la conciencia de la gente es lo más difícil, porque para no ir tan lejos, la mayoría de las personas dejan sus contraseñas a la vista, no graban sus contraseñas, sino que las escriben en papeles y las dejan a la vista de todo el mundo, o también usan contraseña con bajo nivel de seguridad para el ingreso a sistemas.

1.2 FORMULACIÓN DEL PROBLEMA

El usuario final requiere de un alto nivel de conciencia del riesgo informático, siendo este uno de los mayores obstáculos al momento de aplicar medidas de seguridad informática en el uso doméstico de redes, al igual que, la dificultad para el usuario en la identificación de las vulnerabilidades de la red.

Dada la conectividad que tenemos hoy en día y el uso de variados dispositivos conectados a una red dentro del hogar las vulnerabilidades se multiplican, la toma de medidas de seguridad por parte del usuario puede ser un beneficio en seguridad sin necesidad de contar con conocimientos altamente técnicos.

Teniendo en cuenta lo anterior surgen los siguientes interrogantes:

- Pregunta Principal.

[7] Ibid.

¿Como un manual de buenas prácticas de seguridad informática basado en la identificación de algunas vulnerabilidades presentes en las redes domésticas, podría minimizar los riesgos presentes en este tipo de redes?

- Preguntas Secundarias.

¿Cuál es el origen de las redes domésticas, características y vulnerabilidades?

¿Como se podrían explotar algunas vulnerabilidades presentes en una red doméstica?

¿Qué pasos o mecanismos de seguridad informática permiten asegurar este tipo de redes?

2. JUSTIFICACIÓN

La falta de conciencia y desconocimiento de los riesgos en redes informáticas, presentan una gran vulnerabilidad para el uso seguro de las mismas por parte del usuario final.

Por lo anterior, es importante que desde el uso doméstico del internet los usuarios sean conscientes de las amenazas presentes en el ciberespacio y como protegerse para mantener de forma segura su información. Siendo la presente monografía una ayuda en la identificación de vulnerabilidades para sus redes personales, y una guía de buenas prácticas para aumentar los niveles de seguridad en la red.

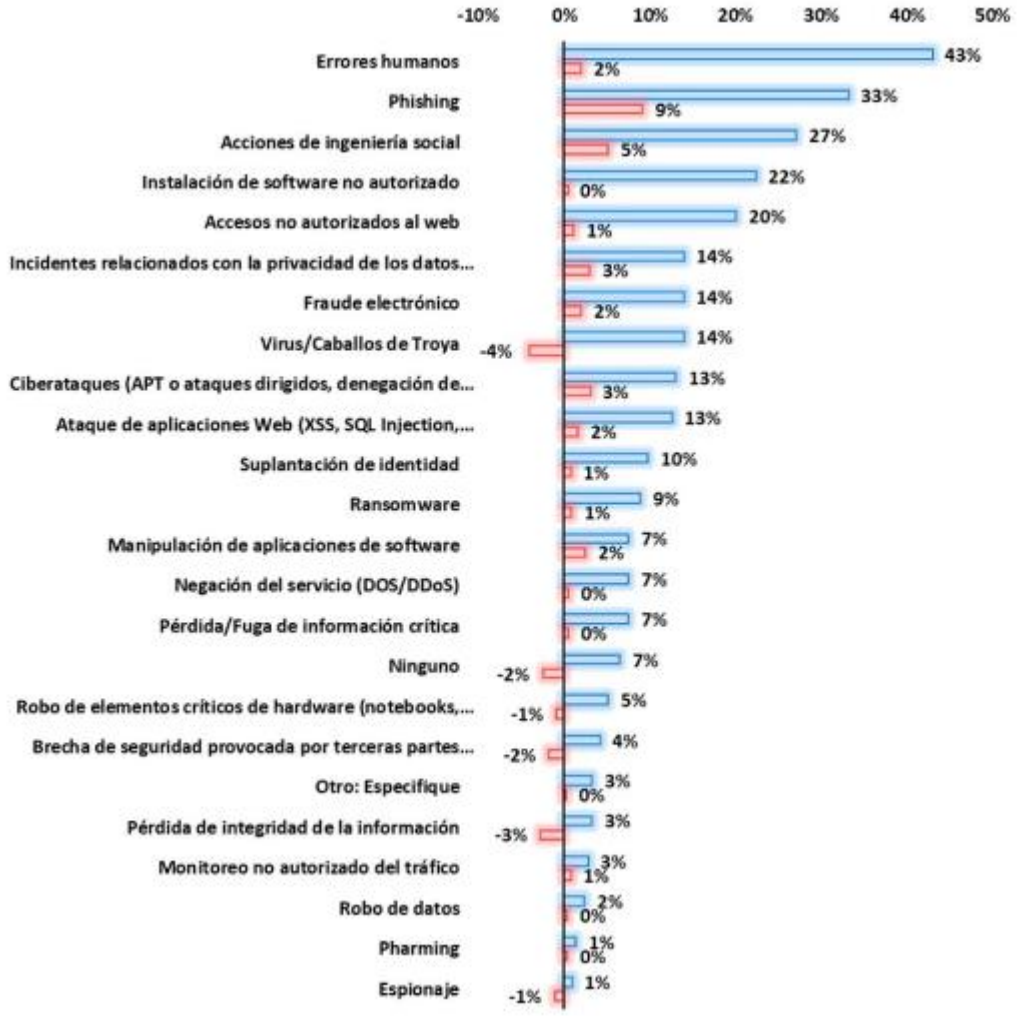
El usuario es el eslabón más débil dentro de la seguridad informática,[8] las personas a diferencia de los computadores no pueden seguir instrucciones de forma rigurosa y estricta, de aquí la importancia de ocuparse de este tema para poder mitigar el riesgo, y así lograr cerrar la brecha de seguridad realizando un manual de buenas prácticas una vez identificadas las vulnerabilidades.

Los incidentes que involucran los errores humanos son los principales dentro del uso de redes informáticas, lo anterior ocurre no solo en el hogar sino también en el ámbito empresarial que junto al phishing encabezan la lista de incidentes presentados según una encuesta realizada por la revista Sistemas de la ACIS (Asociación Colombiana de Ingenieros de Sistemas)[9], así se ve en la siguiente ilustración:

[8] GOMEZ, Alvaro. Enciclopedia de la Seguridad informática. 2a Edicón. Madrid : Ra-Ma, 2014.830 p ISBN 978-84-9964-038-5. Cap 3

[9]ACIS Asociacion Colombiana de Ingenieros de Sistemas. Seguridad y Ciberseguridad.. Numero. 155, Abril- Junio de 2020 Bogotá : ISSN 0120-5919. Pag.35

Figura 1. Encuesta de Seguridad Tipos de Incidentes



Fuente: ASCI Asociación Colombiana de Ingenieros de Sistemas

La dependencia de las redes de información y los problemas de seguridad que se presentan en las mismas pueden llegar a comprometer seriamente la información del usuario, día a día crecen los problemas de seguridad, de igual forma crecen en gran cantidad los atacantes de redes que sin autorización husmean y se infiltran en la red para obtener todo tipo de beneficios.

En términos generales se dice que las redes son inseguras, por lo cual cobra especial relevancia temas como la detección de intrusos, el malware o programas malignos, y la seguridad en internet

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Elaborar un manual de buenas prácticas de seguridad informática basado en la identificación de algunas vulnerabilidades presentes en las redes domésticas, que permita minimizar los riesgos presentes en este tipo de redes.

3.2 OBJETIVOS ESPECÍFICOS

- Describir a luz de la teoría el origen de las redes domésticas, características y algunas vulnerabilidades.
- Realizar simulaciones de explotación de algunas vulnerabilidades que se pueden presentar en una red doméstica a través de un ambiente virtual controlado.
- Diseñar unos pasos metódicos que permitan asegurar este tipo de redes a través de mecanismos de seguridad informática.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Los tres pilares de seguridad de la información son: La confidencialidad, la integridad y la disponibilidad.

La información goza de gran valor actualmente, está compuesta por datos, números, medidas, que dado el valor que se les da aporta conocimiento. Tanto persona como compañías encuentran en el uso de datos un activo que suma valor a los intangibles en la era de la información.

Los pilares se fundamentan en la importancia de usar la información generando un beneficio al mayor rendimiento posible minimizando el riesgo en el manejo de los datos.[10]

Es característico en estos pilares contar con cierta capacidad o robustez para tener un sistema de seguridad confiable, usable y seguro, lo que supone que si hace falta o es débil alguno de ellos habrá exposición a ataques y se forma un vacío de seguridad.[11] En detalle los pilares de la seguridad informática son:

- Confidencialidad: Su objetivo es lograr que la información no sea divulgada a personal no autorizado. Es muy importante porque no es seguro que una persona tenga acceso a información sin restricción alguna, de ser así, se corre el riesgo de pérdida, alteración o sustracción de información, por lo cual se debe garantizar que cada sistema o usuario tenga acceso solo a los recursos necesarios en función de sus tareas.

- Integridad: Garantizar que la información no sea modificada o eliminada, que se mantenga estable y, por medio de la autenticación, solo permitir que el personal autorizado tenga acceso a la misma y de esta forma no comprometer voluntaria o involuntariamente la información.

[10] ROMERO, Martha, et al. 2018. Introduccion a la seguridad informatica y análisis de vulnerabilidades. Alicante : Area de Innovación y desarrollo, 2018, págs. 41-49.

[11] Ibid., p. 25

- También comprende el hecho de trabajar la información adecuada y no usar información errónea considerando que esto puede ser tan nocivo como la misma pérdida de información. Sutiles cambios o manipulación de la información pueden conllevar a una cadena de errores que tengan como consecuencia la toma de decisiones equivocadas. [12]

- Disponibilidad: Con los avances tecnológicos, en este momento se puede tener acceso a la información de la oficina desde el hogar. Hay una línea muy delgada de seguridad entre la disponibilidad de la información en el momento que se requiera y el uso de protocolos de seguridad para mantener la confidencialidad e integridad de los datos. Si la información es integra y confidencial pero no se tiene disponible para usarla de poco sirve. Por ejemplo. la perdida en la disponibilidad de la información sucede en los ataques DDoS que puede causar que una página web no esté disponible, y no se tendría disponible la información.

Cuando hablamos de seguridad informática nos referimos a la seguridad de los sistemas, de la infraestructura y de la información digital. Su protección incluye, pero no se limita a los controles de acceso a las aplicaciones, a los logs, cifrado de información en discos duros y bases de datos, protección de los canales de comunicación, en general se busca asegurar cualquier tipo de información usada o generada por un sistema sin importar que dicha información esté en tránsito o en reposo.

El termino seguridad de la información tiene un significado más amplio, en cuanto abarca todo tipo de amenazas que pueda sufrir la información. En este sentido no solo busca proteger los sistemas, sino todo lo relacionado al manejo de la información, esto incluye controles de acceso, seguridad de los contratos físicos, facturas y demás documentos físicos que sirvan como soporte para el desarrollo de procesos que involucren tecnología, así mismo, la seguridad de la información busca cumplir con los aspectos legales directamente relacionados con la confidencialidad y privacidad de los datos de los clientes.

La seguridad física hacer referencia a todos los medios tangibles para proteger la infraestructura, son todas las barreras y medios de acceso controlados que se pueden colocar en un sistema o en un centro de datos o equipo en específico.

Este tipo de seguridad se plantea para sortear desastres naturales, evitar accesos no autorizados, robo, fraude y/o sabotaje, a nivel de personal se habla de guardias

[12] Ibid., p. 26

de seguridad que vigilen el acceso de personas no autorizadas, a nivel de hardware se incluyen los métodos de acceso con sistemas biométricos, cámaras de seguridad e identificación digital como tarjetas códigos de barras entre otros.

También se puede tener en cuenta en esta clasificación los dispositivos y servidores de backup a nivel de hardware que alojan copias de seguridad derivadas de las copias principales en caso de un desastre cuya criticidad es total.

4.1.1 Red Wi Fi

Es una conexión que se forma sin la necesidad de usar cables, por este motivo se ha propagado rápidamente su uso. Un ejemplo de ello es el aumento del uso de la telefonía móvil.

Wi-Fi permite la conexión de gran cantidad de dispositivos tales como portátiles, celulares, equipos de escritorio, Smart TV entre muchos otros.

El uso principal de esta tecnología es la conexión de todos estos dispositivos compartiendo el acceso a internet ADSL o cable, y compartir recursos entre si mediante lo que se conoce como un punto de acceso o access point, en el hogar el punto de acceso suele ser el router.[13]

4.1.2 Componentes de una red Wi Fi:

La red Wi Fi puede estar compuesta por dos o más dispositivos, para que la comunicación sea posible cada dispositivo debe contar con un adaptador de red, el cual, a su vez, es un dispositivo que cuenta con transmisor, receptor y antena (como un equipo de radio).

Los dispositivos conectados usan un mismo protocolo para comunicarse, los protocolos de componen de dos grupos: 1. Se ocupa de la comunicación inalámbrica de los dispositivos (protocolo Wi-Fi), y el 2. Se ocupa del intercambio de información entre los dispositivos (protocolo TCP/IP).

[13] CARBALLAR, Jose Antonio. Wi-Fi lo que necesita conocer. Madrid : RC Libros, 2010.

El estándar de Wi-Fi está establecido en la norme IEEE 802.1 lb, donde se describen los detalles técnicos para la comunicación de forma inalámbrica a una velocidad de 11Mbps, la velocidad máxima del estándar original, lo que ha continuado en desarrollo aumentando la velocidad.

4.1.3 Ventajas de la red Wi-Fi:

Cuando dos o más dispositivos se encuentran interconectados se encuentran ventajas como:

- Compartir el acceso a internet y servicios de comunicaciones.
- Permite compartir impresoras, escáner, discos duros, cámaras etc.
- Permite compartir información y aplicaciones.[14]

4.1.4 Redes inalámbricas públicas:

En comparación con las redes cableadas, las redes inalámbricas tienen menos control para definir quien se conecta, ya que si se encuentra dentro del rango de alcance del punto de acceso en principio podría conectarse, actualmente estos últimos tienen un gran radio de alcance, con lo cual, un vecino se podría conectar a nuestra red, claro está necesita el SSID y la calve de acceso (en caso de tenerla).

En caso de redes públicas basta con saber la red a la que queremos conectarnos y generalmente no cuentan con contraseña, estas brindan acceso a internet en sitios públicos y de forma gratuita.

Es importante tener en cuenta que el tráfico de la información por estas redes no cuenta con ninguna seguridad como podría ser encriptación, lo cual obedece a no tener una contraseña de protección, por lo cual fácilmente se puede monitorear el

[14]CARBALLAR, Jose Antonio. Wi-Fi lo que necesita conocer. Para que sirve Wi-Fi. Madrid : RC Libros, 2010. 211 p. ISBN: 978-84-937769-0-9

tráfico de la red, lugar ideal para que un intruso pueda obtener contraseñas de usuarios, actividad en redes sociales, datos de tarjetas de crédito entre otras. Aunque existen métodos de protección en estas redes como podría serlo una red VPN, de la cual se hablará más adelante en detalle.[15]

Por otra parte, dentro del hogar la configuración del punto de acceso usualmente se deja por defecto, lo cual es conocido por los ciberdelincuentes, y al localizar una red con baja seguridad pueden lanzar un ataque mediante la configuración un punto de acceso dirigiendo la señal a la antena del atacante, y los usuarios autorizado se conectarán sin darse cuenta al punto de acceso del pirata informático robando la información. [16]

4.2 MARCO CONCEPTUAL

Para una mejor comprensión de la presente monografía, a continuación de describe los elementos más relevantes dentro del tema de seguridad informática en redes.

Dentro del amplio tema de seguridad informática, encontramos componentes que hacen parte de este mundo y que bien vale la pena tratar a fondo, empezando por un tipo de seguridad llamado Seguridad lógica el cual hace referencia al tipo seguridad que se implemente a nivel lógico es decir a nivel de software, se complementa perfectamente con la física para aumentar aún más la protección de nuestro sistema, a este tipo de seguridad se le relaciona con antivirus y programas derivados como analizadores de malware, spyware, antispam, analizadores USB y antivirus de segundo diagnóstico, los sistemas de detección de amenazas o sistemas de detección de intrusiones o IDS intrusión detection system son un complemento ideal en la red de un sistema junto con un buen firewall para maximizar la seguridad[17]

En la seguridad tecnológica intervienen los programas de firmas digitales que nos brindan autenticidad en la información, las autenticaciones de usuarios en nuestros sistemas van desde nuestras bases de datos B.D. hasta autenticación en la propia

[15]AGUADO, David Prudencio**.** Seguridad Informáticva para el Hogar. Como asegurar nuestra red. Madrid : Bubok Publishing, 2012. 93 p. ISBN: 8468604674

[16] SAAVEDRA, Gabriel Andres. Seguridad en redes inalambricas domesticas. Monografía para Ingeniero de Sistemas. Bogota. Universidad Libre de Colombia. Facultad de Ingeniería de Sistemas. 2011. 59 p.

[17] RIOS, Julio. Monografias.com. Seguridad Informática. [En línea] [24 de Septiembre de 2020] Disponible en: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml.

estación de trabajo, la aplicación de criptografía o métodos criptográficos a la información crítica es otro método de seguridad lógica.

A nivel lógico existen muchas más herramientas y metodologías a utilizar que se complementan con el hardware, el nivel de protección e implementación varía según el tipo de organización e información que esta maneja

La seguridad física comprende las medidas que se toman contra desastres naturales, incendios, equipamiento, inundaciones, picos y ruidos electromagnéticos, cableado, aplicado medidas físicas para prevenir el daño o pérdida de recursos.

Los hackers son usuarios que tienen un conocimiento experto en tecnología y que busca manipular los sistemas informáticos para hacer funciones diferentes a lo que fueron creados, el término es utilizado a modo de título en la comunidad otorgado a aquellos que hacen aportes notables, es un experto en una o varias áreas de dominio específicas.[18]

El objetivo del hacker puede ser beneficioso o malicioso, de aquí su denominación en hacker de sombrero blanco (White hat hacker) o hacker de sombrero negro (black hat hacker).

Aunque también existe el concepto de hacker de sombrero gris, que es el que está en el lado beneficioso y malicioso.

A continuación, nos enfocaremos en las definiciones de White hackers y black hackers un poco más detallado.

White hackers, nace debido a los múltiples ataques de hackers a sistemas de informática, se han creado nuevos conceptos para “evitar” este tipo de ataques. Muchas empresas se dedican a contratar a hackers para que revisen posibles fallas en el sistema de seguridad y/o vulnerabilidad. A estos hackers se les conoce como White hacker o White hat hackers (pirata informático de sombrero blanco).

[18] PACHECO, Federico. Hackers al descubierto. s.l. : Creative Andina Corp, 2010. 421p.

De este nuevo concepto de hackers legales que ayudan a las empresas en su sistema de seguridad aparecen otros nuevos conceptos como bug bountie (recompensa por encontrar un fallo), bug (fallo), Hackerone (compañía que se dedica a impulsar a los White hat hackers).

Black hackers o crackers, a diferencia de los White hackers (quienes poseen un código de ética) buscan violar los pilares de la seguridad (disponibilidad, confidencialidad e integridad) informática.[19] Las razones por las que realiza esta violación van más allá de retos personales, estos hackers son ilegales ya que las consecuencias de sus actos buscan crear caos. Los ataques más frecuentes son robo de identidad, vandalismo en los sistemas, creación de virus como gusanos, ataques a las redes de ordenadores.

4.2.1 Tipos de desastres:

- Desastres naturales, fuego, tormentas, incendios, inundaciones.
- Los tipos de amenazas que puedan llegar a ser ocasionadas hombre
- Disturbios y sabotajes tanto internos como externos.
- La infraestructura donde se encuentran los equipos de cómputo debe ser no inflamables
- El entorno del edificio donde se encuentren los equipos debe ser seguro es decir no estar cerca de fábricas que manipulen materiales explosivos y peligrosos.
- Se debe construir un falso piso con materiales no combustibles y resistentes al fuego. [20]

4.2.2 Seguridad del equipamiento:

Los equipos de deben mantener en lugares donde se controle el ingreso de las personas, además deben tener detector de incendios y buena ventilación.
Algunas consideraciones técnicas en este aspecto son:

- La temperatura no debe estar sobre los 18ºC y la humedad no debe ser mayor a 65%

- Se debe contar con equipo de extinción de incendios, manuales y automáticos.

[19] Ibid. p. 22
[20] MAGERIT. Metodología de Análisis y Gestión de Riesgos de Sistemas de Información. Libro 2 Magerit 3.0.

- Inundaciones:

- Es la acumulación excesiva de agua por fallas en drenaje o fenómenos imprevistos, para mitigar este riesgo se puede construir un techo impermeable para evitar el paso de agua y contar con puertas que de la misma forma puedan contener el agua que pudiese bajar de pisos superiores por las escaleras.[21]

4.2.3 Instalaciones eléctricas.

Es recomendable que un especialista diseña las instalaciones de una sala de cómputo, dado que este es uno de los puntos que más riesgo representa por que la electricidad está circulando por todo el sistema de computadoras.

4.2.4 Cableado.

Figura 2. Cableado UTP

Fuente: Imagen de dlohner en Pixabay.

El cableado puede ser telefónico, coaxial o de fibra óptica, que son los más utilizados para la construcción física de las redes. Los riesgos que se presentan en el cableado son: interferencias, cortes del cableado, daños del cableado. En la vivienda puede ser utilizado para: señales de radio y televisión, señales de control de datos a media y baja velocidad.[22]

[21] DIAZ, Gabriel. Procesos y Herramientas para la seguridad en redes. Madrid : Uned Publicaciones, 2014. ISBN 978-84-362-6838-6.

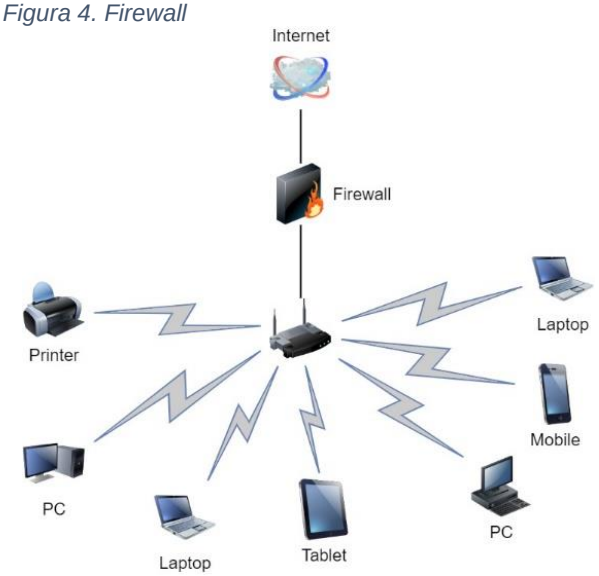
[22] JUNESTRAND, Stefan, PASSARET, Xvier y VASQUEZ, Daniel. Domótica y hogar digital. Integracion de sistemas del hogar digital. Madrid : Thomson Ediciones S.A, 2005. 174 p. ISBN: 84-283-2981-9

Figura 3. Fibra óptica

Fuente: Imagen de Michael Schwarzenberger en Pixabay

4.2.5 Firewall

Figura 4. Firewall



Fuente: Drawio

El Firewall es un componente o un sistema de componentes que se encuentran dentro de una red y que consta de políticas de seguridad que establece la organización con el fin de conservar la seguridad de la información.

Es uno de los elementos más utilizados para protección de redes y sistemas informáticos, está diseñado para proteger una red de intrusos y accesos no autorizados.

Un Firewall es Gateway o puerta bloqueada que se abre solo para dejar pasar los paquetes de información que hayan pasado ciertos filtros. Los Firewall son utilizados mayormente por grandes organizaciones.[23]

El Firewall puede constar de varios dispositivos y se ubica en medio de dos redes, contiene información sobre las políticas de seguridad establecidas, protegiendo una red segura como lo puede ser una red corporativa de una red de riesgo como lo es internet.

El uso de Firewall busca cumplir los siguientes objetivos:

- El tráfico que pasa de fuera hacia adentro y viceversa debe pasar por el Firewall.
- Solo puede pasar el tráfico que este permitido por las políticas de seguridad.

El Firewall solo puede proteger solo el perímetro comprendido por la red, si se presenta un ataque dentro de la red no puede ser impedido, si el firewall logra ser vulnerado se pierde la protección del total de la red. Teniendo en cuenta que la información debe pasar por el Firewall, es una buena práctica dar seguridad adicional encriptando los datos que transitan por la red. [24]

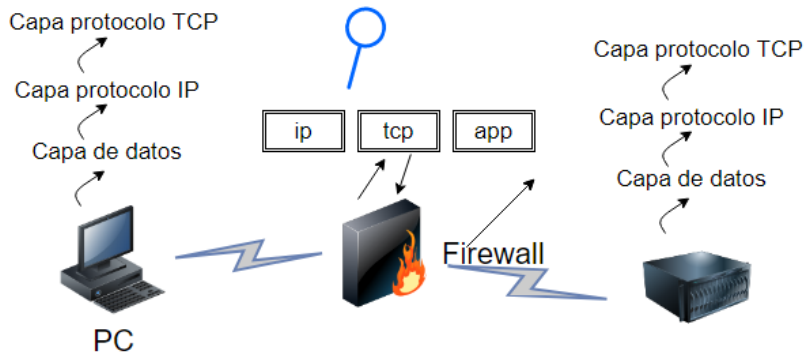
4.2.6 Tipos de Firewall

Filtrado de paquetes: Los Firewall de filtrado de paquetes trabajan sobre el nivel de Transporte y Nivel de Red del modelo OSI dado el funcionamiento y estructura de este tipo de Firewall, son económicos y su desempeño se considera bueno y no es percibido por el usuario.

[23] KOMAR, Brian. et al. 2003. Firewalls for dummies. Segunda edición. New York : Wiley Publixhing Inc., 2003. pág. 428 p. ISBN 0-7645-4048-3.

[24]RIOS, Julio. "Seguridad Informática".{En Línea} {10 de Abril de 2020} (https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.html.)

Figura 5. Firewall de cifrado de paquetes

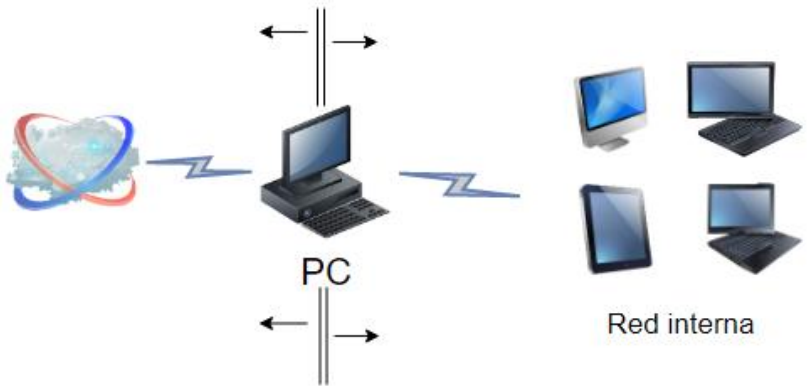


Fuente: Huawei.com

Dual-Homed Host: Estos dispositivos se caracterizan por estar conectados perímetro interior y también al perímetro exterior, y no permite el paso de IP (IP-Forwarding desactivado).

Un usuario en el perímetro interior que desee una conexión exterior se conectará primero al Firewall, el proxy atenderá la petición, y de acuerdo con la configuración de seguridad y hará de puente entre el exterior y el usuario al interior utilizando dos conexiones: una que parte desde la máquina del perímetro interior y va hasta el Firewall y otra conexión que va desde el Firewall hasta la maquina host del servicio exterior.[25]

Figura 6. Dual-Homed



Fuente: Elaborado por el autor

[25] KOMAR, Brian. et al. Firewalls for dummies. Segunda edición. New York : Wiley Publixhing Inc., 2003. 428 p. ISBN 0-7645-4048-3.

Screened Subnet: Consta de aislar la maquina más atacada y vulnerable del Firewall, siendo el Nodo Bastion. Se establece una DMZ o zona desmilitarizada de forma que si el atacante logra la intrusión no consiga el control total de la subred protegida. [26]

Proxy-Gateway de aplicaciones:
El filtrado de paquetes puede contar con debilidades, para contrarrestarlas, se ha creado por parte de desarrolladores software de aplicación capaz de filtrar las conexiones, esto se conoce como servidor Proxy el cual se ejecuta en una máquina que se llama Bastion Host o Gateway de aplicación.[27]

Screened Host: Es la combinación de un Host Bastión con un Router, y utiliza el filtrado de paquetes como primera barrera de seguridad. Se permite solo un número reducido de servicios, en el Choke se filtran los paquetes peligrosos y se ejecuta el Proxy de aplicaciones. El Screened host puede asegurar los equipos de la red interna.[28]

Figura 7. Screened Host

Fuente: Elaborado por el autor.

Si bien el Firewall es un método de protección efectivo, también tiene sus desventajas, por ejemplo, protege solo capas bajas del modelo OSI, no tiene la posibilidad de proteger las más altas como presentación y aplicación, así mismo

[26] KOMAR, Brian. et al. Firewalls for dummies. Segunda edición. New York : Wiley Publixhing Inc., 2003. 428 p. ISBN 0-7645-4048-3.

[27] Ibid., p 303.
[28] Ibid., p 174.

está fuera del Firewall el poder esconder la topología de red de la red privada por lo que puede representar una vulnerabilidad al contar con esta información, si las políticas de seguridad llegan a ser complejas puede no soportarlas,

El Gateway conocido también como puerta de enlace, es un dispositivo tipo ordenador configurado para interconectar redes con protocolos y arquitectura diferente en todos los niveles de comunicación, traduciendo la información del protocolo de una red a la red receptora.[29]

4.3 MARCO HISTÓRICO

El hecho de contar con equipos de cómputo dentro del hogar hace algunos años no se había concebido, que haría un computador dentro de una casa o un apartamento, a partir de la incorporación del computador personal en el hogar las redes domesticas se han expandido, evolucionado e impulsado por hechos de gran magnitud como la pandemia actual covid-19. La rede en el hogar tiene alta relevancia hoy en día y el usuario se interesa más en el correcto funcionamiento de los servicios informáticos en casa.

En sus inicios los computadores no fueron concebidos para compartir información entre estos, ni que llegarán a usarse de forma masiva en los hogares, ya que su uso estaba dirigido a los ámbitos militares y científicos, pero dada la evolución del hardware, software y las redes se introdujo las redes de computadores en los hogares respondiendo a dos puntos importantes como la aparición del ordenador personal y la evolución de internet como los conocemos actualmente.

4.4 ESTADO ACTUAL

Actualmente la interconexión es la cotidianidad para las personas en general, todo tipo de dispositivos se conecta dentro de la red doméstica y con ello las vulnerabilidades se multiplican, por lo que el nivel se seguridad también debe subir.

Las personas pueden tomar medidas básicas para el uso seguro de la tecnología entre los cuales se encuentra el uso de contraseñas fuertes, autenticación de doble factor, privacidad de datos en redes sociales, pero se desconocen otras vulnerabilidades que pueden tener las redes en sus hogares, o tipos de ataques

[29] ECURED. Puerta de Enlace. [En línea]. Disponible en: https://www.ecured.cu/Puerta_de_enlace.

como el phishing que es muy común, o temas como configuración y actualización de router pueden ser un punto débil para los sofisticados ataques contemporáneos.

A medida que crece el uso de dispositivos digitales en el hogar, crece a su vez la actividad de los cibercriminales, siendo internet el centro de las actividades domésticas, donde se requiere seguridad informática en el consumo de:

- Series y películas: Donde se debe tener cuidado con el sitio que ofrece el servicio, acceder solo a sitios de confianza, ya que hay un gran número de sitios gratuitos que llevan consigo riesgos que pueden pasar inadvertidos por el usuario recolectando información, usando spam y phishing, o requiriendo la instalación de software para la visualización que puede resultar maligno.

- Videojuegos: Es común encontrar juegos que utilizan los llamados cracks para que el juego funcione, estos programas pueden[30] causar daños a las computadoras por que pueden contener keyloggers y redirectores DNS.

- Compras en línea: Muchos sitios inseguros pueden robar información del usuario.

4.5 MARCO TECNOLÓGICO

El aumento de dispositivos tecnológicos en el hogar se ha desarrollado tecnología como las redes wi -fi que son las que permiten la conexión de forma inalámbrica de dispositivos como ordenadores portátiles, los cuales son computadores que cuentan con la facilidad de ser transportados y que su rendimiento es como el de los computadores de escritorio[31], los cuales a su vez se definen como el ordenador personal, diseñado para estar en un lugar estático como una mesa o escritorio.

Otro tipo de dispositivos que suele usarse en el hogar son los teléfonos móviles inteligentes o smartphones, los cuales son dispositivos que cuenta con sistema

[30] CUNHA, Daniel. Películas, compras y videojuegos en Internet: los riesgos de seguridad durante los días de cuarentena. welivesecurity eset. {En línea}. {Citado el: 25 de Abril de 2020} disponible en: (https://www.welivesecurity.com/la-es/2020/03/26/peliculas-compras-videojuegos-internet-riesgos-seguridad-dias-cuarentena/.)

[31] Colaboradores de Wikipedia. Computadora portátil [en línea]. Wikipedia, La enciclopedia libre, 2020 [fecha de consulta: 11 de enero del 2021]. Disponible en https://es.wikipedia.org/w/index.php?title=Computadora_port%C3%A1til&oldid=131790226

operativo y con la capacidad de conectarse a internet para realizar muchas de las tareas que pude hacer un computador de escritorio o un computador portátil.[32]

Las consolas de videojuegos son dispositivos electrónicos con el fin de entretener al usuario ejecutando juegos en video basados en cartuchos, discos, tarjetas de memoria y actualmente a través de internet.

El uso de tablets por parte de los miembros de la familia es algo muy común, para tareas escolares y del trabajo, las tables inicialmente eran productos de la ciencia ficción vistas en películas como StarTrek, las tablets son similares a los teléfonos celulares ya que es un tipo de computador portátil, pero consume menos energía y es más liviano y se usa para tares igualmente livianas.[33]

Adicionalmente, en el hogar ahora se cuenta con dispositivos como impresoras y aparatos electrodomésticos inteligentes como Smart-TV, neveras, lavadoras, aire acondicionado y un sinfín de dispositivos con la capacidad de conectarse a la red.

4.6 MARCO LEGAL

El avance y desarrollo tecnológico ha llegado al ámbito del hogar, el manejo de la información en casa aumenta gradualmente y al considerarse la información un bien de las personas se ha otorgado protección jurídica.

Específicamente hablando de delitos informáticos, estos se entienden como la actitud contraria a la que tiene la persona que tiene el computador o instrumento (concepto atípico) o las conductas típicas, antijurídicas y culpables en las que se tiene las computadoras como instrumento o fin.[34]

En Colombia existe la ley de Delitos informáticos Ley 1273 del 5 de enero de 2009, la cual tiene como antecedentes el decreto 1360 de 1989 que es la reglamentación del software con componentes de derechos de autor, lo cual surge por los reclamos

[32] Colaboradores de Wikipedia. Computadora de escritorio [en línea]. Wikipedia, La enciclopedia libre, 2021 [fecha de consulta: 11 de enero del 2021]. Disponible en <https://es.wikipedia.org/w/index.php?title=Computadora_de_escritorio&oldid=132211680>.

[33] Vivir Mejor. Que es y para que sirve una Tablet?. [en línea]. Vivir mejor.mx, 2021 [fecha de consulta: 11 de enero del 2021]. https://vivirmejor.mx/tecnologia/que-es-y-para-que-sirve-una-tablet/

[34] OJEDA, Jorge, et al. Delitos informáticos y entorno jurídico vigente en Colombia. Cuad. Contab. vol.11 no.28 Bogotá Jan./Dec. 2010. ISSN 0123-1472

presentados por violación a los derechos de los desarrolladores de software, por lo cual se empezó a proteger la producción intelectual de los creadores de estos producto, dado pie a la construcción de normas penalmente sancionatorias para la violación de derechos de autor y otras como la ley 599 de 2000 que trata en el artículo 192: Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático.[35]

La Ley 1273 de 2009 complementa el Código Penal y crea un nuevo bien jurídico tutelado a partir del concepto de la *protección de la información y de los datos*, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones.[36]

El delito sobre "violación de datos personales" (*hacking*) lo trata el artículo 269F y está orientado a proteger los derechos fundamentales de la persona (como dignidad humana y libertad ideológica). Se da cuando un individuo sin estar facultado sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en ficheros, archivos, bases de datos o medios similares con el fin de lograr utilidad personal o para otros.

El artículo 269G trata de la "suplantación de sitios *web* para capturar datos personales". Sucede cuando el suplantador (*phisher*) o delincuente informático crea una página y un dominio similar al de la entidad a la cual desea abordar, lo ubica en un *hosting* (espacio en un servidor) desde donde envía correos *spam* o engañosos (por ejemplo, empleos). Al no distinguir la página original de la falsa, las personas inocentemente suministran información personal y claves bancarias que el suplantador almacena en una base de datos y luego ordena la transferencia del dinero de la víctima a cuentas de terceros quienes prestan sus cuentas o servicios (testaferros), que luego reclama o distribuye.[37]

[35] Ibid, p. 41
[36] Ibid, p. 42.
[37]

5. ENFOQUE METODOLÓGICO

Para el desarrollo de este trabajo se ha creado una estructura que consta de tres fases y brindan al lector información suficiente desde el inicio, tomando como punto de partida información acerca de las generalidades en redes informáticas y redes domésticas, para que una vez se cuente con esta información se comprenda mejor el paso dos, en el cual, se lleva a cabo un proceso para la identificación de vulnerabilidades, que permite llegar a la tercera fase y como consecuencia elaborar el manual de buenas prácticas, que a su vez entrega al usuario una serie de recomendaciones documentadas.

Dicho esto, las fases se componen de la siguiente forma:

5.1 FASE 1. LAS REDES DOMÉSTICAS.

- Orígenes de las redes y como se abrieron camino hasta la parte doméstica.
- Características e importancia de una red doméstica.
- Tipos de redes domésticas y protocolos de comunicación.
- Formas de identificación y autenticación en redes.
- Amenazas y vulnerabilidades comunes en redes.

5.2 FASE 2. SIMULACIONES DE EXPLOTACIÓN

- Configuración del ambiente virtual de simulación.
- Fases que se utilizaran para las pruebas de explotación de vulnerabilidades.
- Identificación y análisis de algunas vulnerabilidades. (Para esta parte se aplica la metodología basada en PTES)

5.3 FASE 3. MANUAL DE BUENAS PRÁCTICAS DE SEGURIDAD EN REDES DOMÉSTICAS.

- Aclaraciones previas. (Intención, para quien, estructura).
- Detección de dispositivos conectados.
- Contraseñas seguras.
- Acceso por MAC.
- Antivirus.
- Firewall.

- Protección contra spoofing.
- Actualizaciones.
- Cifrado.
- VPN.

5.3.1 Recomendaciones de seguridad en redes domésticas.

- Importancia de la Seguridad en redes.
- Aseguramiento de redes.
- Mecanismos ante riesgos de seguridad.

6. FASE 1. LAS REDES DOMESTICAS

Esta fase se compone de una amplia documentación, presenta los conceptos y principios básicos del tema seguridad informática en redes, describiendo como se iniciaron las redes de computadores y como se ha llegado a usar a nivel doméstico, el contenido de esa fase, así como las subsiguientes presta especial atención a la importancia que tiene el usuario de la red, es decir un enfoque en el factor humano como eslabón destacado de seguridad.

6.1 ORÍGENES DE LAS REDES Y COMO SE ABRIERON CAMINO HASTA LA PARTE DOMÉSTICA

Figura 8. Ilustración de referencia redes

Fuente: Imagen de jeferrb en Pixabay

A principios del siglo XIX se intentó establecer las primeras comunicaciones por medios de redes en Francia y Suecia, mediante mecanismos conformados por brazos y persianas se codificaba la información de acuerdo con la posición que tomaba cada uno de estos elementos. Mediante torres que se debían tener visibles entre si se repetía la información de una a la otra hasta llegar a su destino.

Un tiempo después comenzó la comunicación mediante medios como las redes telegráficas y redes telefónicas, desarrollado por Graham Bell quien es conocido por inventar el teléfono. La primera red telefónica se implementó en Estados Unidos cerca de Boston.[38]

[38] BARCELÓ, Miquel. 2008. Una historia de la informática. Barcelona : Ed. UOC, 2008. pág. 164 p. ISBN 9788497887090.

En los años 60 se empezó a ver los que son la red de conmutación de paquetes lo cual consisten en fragmentar mensajes en parte que se llaman paquetes encaminados hacia un destino y ensamblados una vez llegan a su destino. En Reino Unido se realizó los primeros experimentos con estos tipos de redes y hasta finales de los 60 esta tecnología llegó a Estados Unidos, donde fue implementada y usada por ARPA la agencia para investigación de inteligencia americana, lo cual le trajo grandes beneficios con su implementación en pro de la defensa nacional.[39]

ARPANET fue el inicio de lo que hoy conocemos como Internet, creado por ARPA, en estas redes los dispositivos se conectaron por medio de IMP, y el ordenador se desarrolló por la compañía Honeywell y se instaló el primero en UCLA, posteriormente en los estados de Standford y Utah. Se dice que aun hoy en día existen y se usan los nodos instalados en aquella época.

Este fue el punto de partida para que posteriormente mediante acuerdo entre varias naciones se realizaran las alianzas necesarias para desarrollar los protocolos de comunicación que permitieran que la información que se envía a través de aquellas redes fuera comprensible para todo el mundo.

En los años 80´s la informática empieza su incursión dentro del ámbito doméstico, se empieza a usar ordenadores para el uso de tareas rutinarias dentro del hogar, entonces las conexiones eran muy pocas y se realizaban mediante línea telefónica. Nacieron los ruteadores que se encargaban de las redes locales, bien sea por Ethernet, Token Ring, o Arcnet y traducir los datos al lenguaje de los operadores telefónicos.

Estos son utilizados por los proveedores de servicios de internet o ISP´s, los ruteadores en el hogar hacen la función de NAT (Network Adress Traslation), de este modo las computadoras dentro de la red tienen acceso a internet usando una sola dirección ip.[40] Lo anterior también obedece a la escases o agotamiento de las direcciones ipv4, por lo que la mayoría de proveedores entregan una dirección y un ruteador que pueda enrutar entre una dirección visible pública y las direcciones que puedan haber dentro de la red doméstica los paquetes de datos dentro del tráfico de la red del hogar.

[39]FISHER, Royal**.** Seguridad en los sistemas informáticos. De máxima prioridad a la seguridad. Madrid : Ediciones Diaz y Santos. 1988. 262 p. ISBN: 0-13-464727-0

[40] HERNANDEZ, Joel. esemanal. Historia y evolución de las redes. [En línea] [18 de Abril de 2020] Disponible en: https://esemanal.mx/2008/04/historia_y_evolucion_de_las_redes_/.

6.2 CARACTERÍSTICAS E IMPORTANCIA DE LAS REDES DOMESTICAS

Las redes domésticas tienen las siguientes características:

Tipo de cableado: Se usa cableado UTP, STP, Coaxial, Fibra Óptica entre otros. También es usual el uso de red inalámbrica.

Velocidad de transmisión: La velocidad de transmisión aumenta día a día, inicialmente era de unos kb ahora se cuenta con velocidad decenas de GB de velocidad en el hogar.

La longitud de los cables: Suele estar cerca de los 100m, puede modificarse y ampliarse por el uso de repetidores dentro del hogar.[41]

La importancia de las redes domésticas es que permite el uso de recursos informáticos dentro del hogar, estos pueden ser de distinto tipo como impresoras, módems, fax, telefonía IP, computadoras de escritorio, computadoras portátiles, dispositivos para internet de las cosas (IOT), cámaras de vigilancia, teléfonos celulares, contando con una completa infraestructura de comunicaciones dentro del hogar. Se puede compartir archivos y datos para los usuarios de la red, se pude centralizar el uso en una computadora que puede ser la principal dentro de la red doméstica, además de puede ampliar o escalar de acuerdo a las necesidades.

Actualmente, con la pandemia COVID-19 el uso de la red doméstica adquiere un mayor valor, debido a que las empresas han tenido que implementar el teletrabajo y el trabajo en casa como medida de contingencia para no para en sus actividades productivas.

Antes del inicio de la cuarentena el 25 de marzo en Colombia había 122.000 teletrabajadores según el más reciente estudio de penetración de esta modalidad laboral en empresas del país hecho por los ministerios del Trabajo y de Tecnologías

[41] WIKI.IES. Wiki,ies.Haria Informatica. Caracteristicas y componentes de las redes locales. [En línea] [11 de Agosto de 2020] Disponible en: https://smr.iesharia.org/wiki/doku.php/rde:ut1:caracteristicas#caracteristicas_de_las_redes_locales.

de la Información y las Comunicaciones en la actualidad esa cifra se ha multiplicado.[42]

6.3 TIPOS DE REDES DOMESTICAS

6.3.1 Red Alámbrica:

Es la conexión desde el router hasta los dispositivos de la red por medio de un cable Ethernet, la ventaja de este tipo de red es que la velocidad es mayor que una conexión inalámbrica y tiene mayor seguridad pero como desventaja resulta tener menor flexibilidad, los cables de Ethernet tiene una clasificación que se marca de la forma Cat5 o Cat6 o similar, en el anterior ejemplo el número mayor determina una mayor velocidad para la transmisión y ancho de banda, la categoría 5 soporta hasta 100 Mbps, el categoría 5e soporta hasta 1 Gbps y el categoría 6 hasta 10 Gbps.

6.3.2 Redes inalámbricas

Es la conexión sin cables hacia el enrutador, en cambio utilizan conexión de radio móvil más conocido como Wi-Fi, esta conexión se hace por medio del punto de acceso que es el que transmite las señales wi-fi para que los dispositivos del hogar se puedan conectar, a estos dispositivos se les designa como clientes wi-fi, para esta conexión de usa distintos tipos de señales llamados estándares wi-fi, los routers del proveedor pueden ser compatibles con un estándar o con varios.

Principalmente la diferencia de los estándares esta la frecuencia y la velocidad que soportan. Por ejemplo, el estándar 802.11b maneja la frecuencia de 2.4 Ghz y una velocidad de hasta 11 Mbps y el estándar 802.11ac soporta frecuencia de 5Ghz y una velocidad de 800 Mbps. Los enrutadores solo pueden transmitir una señal de radio estándar wi-fi a la vez.[43]

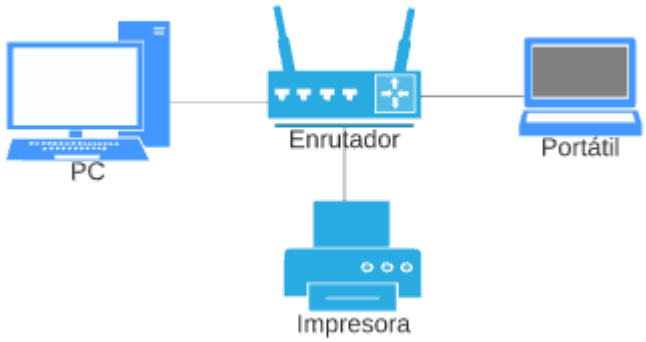
[42] AGUIERRE, Sebastian. Vivir en el poblado. El teletrabajo durante la cuarentena en Colombia: ¿cómo hacen vigilancia las ARL? [En línea] [19 de Mayo de 2020]. Disponible en: https://vivirenelpoblado.com/teletrabajo-en-cuarentena-vigilancia-arl/.

[43] VERIZON. espanol,verizon,com. Resumen de Redes Domesticas. [En línea] [11 de Septiembre de 2020]. Disponible en: https://espanol.verizon.com/support/residential/internet/home-network/overview#:~:text=Hay%20dos%20tipos%20de%20redes,con%20cables%20o%20dispositivos%20inal%C3%A1mbricos..

6.4 PROTOCOLOS DE COMUNICACIÓN

6.4.1 TCP/IP – Transmision Control Protocol e Internet Protocol

Figura 9. Protocolo TCP/IP



Fuente: Elaborado por autor

Varios protocolos que ofrecen transporte de datos en Internet el de Red Controlan los mecanismos de transferencia de datos e invisibles al usuario Tcp divide la información en unidades paquetes para unirlos al final detecta errores, IP Internet Protocol Reparte los paquetes de información direccionándolos al destino establecido a través de una red conmutada. Hay otros protocolos como FTP – Protocolo de transferencia de archivos HTTP – Protocolo de transferencia de hipertexto.[44]

Existen varios tipos de protocolos de red:

Protocolos de comunicación de red: protocolos de comunicación de paquetes básicos como TCP / IP y HTTP.

Protocolos de seguridad de red: implementan la seguridad en las comunicaciones de red entre servidores, incluye HTTPS, SSL y SFTP.

---

44 KIO NETWORKS. Protocolos de comunicación de redes. [En línea] 11 de Septiembre de 2020. https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes#:~:text=Los%20protocolos%20para%20la%20transmisi%C3%B3n,son%20POP%2C%20SMTP%20y%20HTTP..

Protocolos de gestión de red: proporcionan mantenimiento y gobierno de red, incluyen SNMP e ICMP.

Un grupo de protocolos de red que trabajan juntos en los niveles superior e inferior comúnmente se les denomina familia de protocolos.

El modelo OSI (Open System Interconnection) organiza conceptualmente a las familias de protocolos de red en capas de red específicas. Este Sistema de Interconexión Abierto tiene por objetivo establecer un contexto en el cual basar las arquitecturas de comunicación entre diferentes sistemas.

A continuación, listamos algunos de los protocolos de red más conocidos, según las capas del modelo OSI:

Protocolos de la capa 1 - Capa física

USB: Universal Serial Bus
Ethernet: Ethernet physical layer
DSL: Digital subscriber line
Etherloop: Combinación de Ethernet and DSL
Infrared: Infrared radiation
Frame Relay
SDH: Jerarquía digital síncrona
SONET: Red óptica sincronizada

Protocolos de la capa 2 - Enlace de datos

DCAP: Protocolo de acceso del cliente de la conmutación de la transmisión de datos
FDDI: Interfaz de distribución de datos en fibra
HDLC: Control de enlace de datos de alto nivel
LAPD: Protocolo de acceso de enlace para los canales
PPP: Protocolo punto a punto
STP (Spanning Tree Protocol): protocolo del árbol esparcido
VTP VLAN: trunking virtual protocol para LAN virtual
MPLS: Conmutación multiprotocolo de la etiqueta.[45]

45

Protocolos de la capa 3 - Red

ARP: Protocolo de resolución de direcciones
BGP: Protocolo de frontera de entrada
ICMP: Protocolo de mensaje de control de Internet
IPv4: Protocolo de internet versión 4
IPv6: Protocolo de internet versión 6
IPX: Red interna del intercambio del paquete
OSPF: Abrir la trayectoria más corta primero.
RARP: Protocolo de resolución de direcciones inverso
Protocolos de la capa 4 – Transporte.

IL: Convertido originalmente como capa de transporte para 9P
SPX: Intercambio ordenado del paquete
SCTP: Protocolo de la transmisión del control de la corriente
TCP: Protocolo del control de la transmisión
UDP: Protocolo de datagramas de usuario
iSCSI: Interfaz de sistema de computadora pequeña de Internet iSCSI
DCCP: Protocolo de control de congestión de datagramas
Protocolos de la capa 5 - Sesión

NFS: Red de sistema de archivos
SMB: Bloque del mensaje del servidor
RPC: Llamada a procedimiento remoto
SDP: Protocolo directo de sockets
SMB: Bloque de mensajes del servidor
SMPP: Mensaje corto punto a punto
Protocolos de la capa 6- Presentación

TLS: Seguridad de la capa de transporte
SSL: Capa de conexión segura
XDR: Extenal data representation
MIME: Multipurpose Internet Mail Extensions
Protocolos de la capa 7 - Aplicación

KIO NETWORKS. *Protocolos de comunicación de redes.* [En línea] 11 de Septiembre de 2020. https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes#:~:text=Los%20protocolos%20para%20la%20transmisi%C3%B3n,son%20POP%2C%20SMTP%20y%20HTTP..

DHCP: Protocolo de configuración dinámica de host
DNS: Domain Name System
HTTP: Protocolo de transferencia de hipertexto
HTTPS: Protocolo de transferencia de hipertexto seguro
POP3: Protocolo de oficina de correo
SMTP: protocolo de transferencia simple de correo
Telnet: Protocolo de telecomunicaciones de red.[46]

6.5 FORMAS DE IDENTIFICACIÓN Y AUTENTICACIÓN EN REDES

6.5.1 Controles de acceso

Figura 10. Ilustración de referencia Control de acceso

Fuente: Imagen de ar130405 en Pixabay

Los controles de acceso determinan que usuario puede acceder a cuál recurso, se puede implementar en los sistemas operativos, las bases de datos y las aplicaciones, para esto se tienen los siguientes estándares:

6.5.2 Identificación y autenticación:

La autenticación es la primera línea de defensa en sistemas, previene el ingreso de personal no autorizado y el seguimiento de quienes lo están.

La identificación es el momento en el que el usuario de a conocer en el sistema y la autenticación es la verificación de la identidad.

[46] KIO NETWORKS. Protocolos de comunicación de redes. [En línea] [11 de Septiembre de 2020]. Disponible en: https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes#:~:text=Los%20protocolos%20para%20la%20transmisi%C3%B3n,son%20POP%2C%20SMTP%20y%20HTTP..

Existen 4 técnicas que son:

- Algo que el individuo conoce. Por ejemplo, una contraseña, un PIN, una clave criptográfica.
- Algo que el individuo posee. Por ejemplo, un token
- Algo que se es: como huella digital, voz.
- Algo que pueda hacer. Por ejemplo, patrones de escritura.[47]

6.5.3 Roles:

Mediante la asignación de roles se puede controlar el acceso a la información, por ejemplo, se puede dar autorización a la gestión de costos solo a quienes sean directores del área.

6.5.4 Transacciones:

Se realiza solicitando una clave para realizar una transacción determinada

6.5.5 Limitación de los servicios:

El administrador del sistema puede limitar el acceso aplicaciones a cierto número de usuarios.

6.5.6 Modalidad de acceso:

Hace referencia al modo en que el usuario puede acceder la información: Lectura, escritura, ejecución, borrado, creación, búsqueda.

6.5.7 Vulnerabilidad en redes:

[47] GOMEZ, Alvaro. Enciclopedia de la Seguridad informática. 2a Edición. Madrid: Ra-Ma, 2014. 830 p. ISBN 978-84-9964-038-5.

Figura 11. Ilustración de referencia vulnerabilidades en redes

Fuente: Imagen de Darwin Laganzon en Pixabay

Es toda condición que puede permitir un ataque a la seguridad dentro de una red. Vulnerabilidades en los navegadores. Uno de los fallos intrínsecos de los navegadores es el llamado “Buffer OverFlow”, los cuales explotan los buffers que usa la aplicación para guardar los datos del usuario, por ejemplo, las URL buscadas, se guardan en buffer y pueden ser aprovechadas.[48]

6.5.8 Riegos de la información:

6.5.8.1 Robo:

Se suele usar la expresión robar tiempo de maquina cuando los colaboradores realizan tareas en el computador que no están relacionadas con su labor, la información sensible puede ser fácilmente copiada, así mismo el software y cintas que son fácilmente extraíbles sin rastro alguno.[49]

6.5.8.2 Fraude:

Engañar y sobornar con información privada de industrias y de sus empleados. Por medio de las maquinas se ha logrado robar miles de dólares, causando pérdidas a diversas industrias. [50]

[48] BUSTAMANTE, Ruben. Seguridad en Redes. Hidalgo: Universidad Autonoma del Estado de Hidalgo, 2005.

[49] Ibid., 22 p.

[50] Ibid., 23 p.

6.5.8.3 Sabotaje:

El sabotaje es uno de los medios más utilizados por los delincuentes y que causan más daño a las empresas, ya que puede provenir de autores externos como internos. Las cuentas pueden ser borradas fácilmente por medio de imanes, los cableados pueden ser cortados, o se pueden usar elementos corrosivos, inflamables etc.[51]

6.5.9 Tipos de delitos informáticos

Figura 12. Ilustración de referencia Delitos Informáticos

Fuente: Imagen de Sang Hyun Cho en Pixabay

La ONU reconoce los siguientes delitos:

Fraudes cometidos mediante manipulación de computadoras:

- Manipulación de datos de entrada: conocido como sustracción de datos, es fácil de cometer, difícil de descubrir. Es de los más comunes.

- Manipulación de programas: Es la modificación de programas la inclusión de rutinas. También es difícil de descubrir ya que es cometido con altos conocimientos informáticos.[52]

[51] BUSTAMANTE, Ruben. Seguridad en Redes. Hidalgo: Universidad Autonoma del Estado de Hidalgo, 2005.

[52] STEL, Enrique. 2014. Seguridad y ciberdefensa del espacio. Buenos Aires : Ed. Dunken, 2014. pág. 192 p. ISBN 9789870271871.

- Manipulación de datos de salida: El ejemplo más común es el fraude en cajeros automáticos falsificando instrucciones para la computadora la fase de adquisición de datos.

- Manipulación informática: Aprovecha las repeticiones de las operaciones de computadoras. Es un técnico llamado de “salchichón”, donde las “rodajas” son transacciones financieras imperceptibles.[53]

6.5.10 Vulnerabilidades físicas:

Las vulnerabilidades físicas son aquellas que afectan materialmente la infraestructura de una organización, entre las cuales se encuentran los desastres naturales, ya que en caso inundación o incendio se podría perder la disponibilidad de la información.

También comprende las vulnerabilidades físicas la falta de control de acceso, por ejemplo, cuando no se cuenta con sistemas biométricos en las puertas de entrada a datecenter, si cualquier persona puede ingresar sin permiso puede ser un riesgo de pérdida de información.[54]

6.5.11 Vulnerabilidades lógicas

Este tipo de vulnerabilidades son aquellas que pueden afectar la infraestructura tecnológica y la operación, pudiendo ser fallas de configuración, actualización y desarrollo.[55]

De configuración se pueden presentar por ejemplo en un sistema operativo, en configuración de servidores o Firewall que no esté realizando una gestión adecuada de la seguridad. Las de actualización se presentan cuando no se actualiza

---

[53]TORRES, Katia. La ONU y los Delitos Informaticos. {En línea} {23 de Febrero de 2020}. disponible en: (https://prezi.com/i9pr2hukxiyu/la-onu-y-los-delitos-informaticos/.)

[54] ROMERO, Martha, et al. Introduccion a la seguridad informatica y análisis de vulnerabilidades. Alicante : Area de Innovación y desarrollo, 2018, págs. 41-49.

[55] Ibid. p.42

periódicamente los sistemas, cuando el software es obsoleto se suele no prestar actualizaciones lo que crea brechas de seguridad.

Las vulnerabilidades de desarrollo son errores que se presentan en diseño e implementación y que permiten ataques por ejemplo de código SQL. Para detectar estas vulnerabilidades se utilizan las pruebas de penetración y las auditorias, también es común el uso de escáneres de vulnerabilidades.

6.5.12 Escáneres de vulnerabilidades:

Existen una gran variedad de escáneres de pago y gratuitos, generales y especializados, ofreciendo herramientas no solo se escaneo sino también de prueba de vulnerabilidades. Los hay dirigidos sistemas operativos como a aplicaciones web. La familia Metasploit cuenta con herramientas que permiten escanear y obtener vectores de ataque puntuales. OpenVAS permite el escaneo y además evaluar las políticas del equipo y analizar procedimientos de gestión en pruebas de penetración.

6.6 TIPOS DE VULNERABILIDADES:

Desbordamiento de Buffer: Ocurre cuando en la programación no se tiene en cuanta el control del espacio de la memoria del programa, con esto puede ocurrir que externamente se introduzca código adicional en el espacio de memoria disponible u se ejecuta antes que todo, es esto lo que sucede con los payloads.

Errores de configuración: Dentro de los errores de configuración se encuentran fallas como las contraseñas por defecto, los permisos inadecuados para usuarios, encriptación obsoleta, protocolos SSH desactualizados o mal implementados.[56]

Errores Web: Son múltiples las fallas de seguridad que se pueden producir por errores de validación de inputs, scripts inseguros, error de programación de aplicaciones que pueden ser aprovechados por ataques XSS o inyección SQL, siendo éste último uno de los más utilizados actualmente dada la facilidad de

[56] ROMERO, Martha, et al. 2018. Introduccion a la seguridad informatica y análisis de vulnerabilidades. Alicante : Area de Innovación y desarrollo, 2018. 123 p.. ISBN: 978-84-949306-1-4

implementación y puede modificar las cadenas de consulta SQL en la base de datos, por su parte el XSS puede infectar un sitio web mediante la ejecución de scripts maliciosos que pueden llegar a obtener información de usuarios.

Errores de protocolo: Muchos de los protocolos usados actualmente no se desarrollaron teniendo en cuenta el apartado de seguridad informática y menos aún el crecimiento de los incidentes a través del tiempo, lo que ocurre por ejemplo con el protocolo HTTP, el cual no realiza la encriptación de los datos transmitidos, si bien esto puede no ser necesario en todos los sitios web si lo especialmente hoy en día donde se realizan transacciones comerciales y bancarias, por lo que sería necesario utilizar certificados como SSL o TLS.

6.6.1 Detección de Vulnerabilidades:

La detección de vulnerabilidades se realiza mediante herramientas especializadas para tal fin, usualmente el escaneo se realiza para detectar puertos abiertos y detectar los servicios que por allí corren, se detectan:

Escaneando vulnerabilidades: Con herramientas automáticas como Nmap o Nessus que buscan fallos en base a servidores, cuentan con la ventaja de realizar el trabajo por sí misma.

Análisis manual: Los análisis manuales tiene la gran ventaja de encontrar vulnerabilidades que los análisis automáticos no pueden encontrar, lo cual complementa perfectamente y permite que no se escapen detalles.

Consultando información: En fuentes documentales y bases de datos buscar información que pueda servir como insumo de seguridad para la organización para conocer las vulnerabilidades en sus servicios.

6.6.2 Métodos de escaneo de vulnerabilidades

Caja Blanca: Se cuanta con una visión global de la red a escanear, acceso a los equipos con superusuario, se es un usuario legítimo en la labor de escaneo de la

red contando con toda la información disponible en cuanto a administración de la red y cuenta con acceso a todos los servicios de esta.[57]

Caja negra: En este método se proporciona información de acceso a la red. Por ejemplo, una dirección ip como punto de partida para la búsqueda de información, donde se debe sacar toda la información posible de dicha dirección ip explorando todas las posibilidades. Se puede tomar toda la información de los equipos dentro del rango de ip tomando información y documentándola más no se realiza ninguna instrucción, por lo que no se considera realizar pentesting.[58]

6.6.3 Remediación de vulnerabilidades:

Análisis de activos: La primera parte es la realización de un inventario y categorización de activos, equipos como computadoras, servidores, impresoras de incluye de forma ordenada, incluso las direcciones ip con la que se cuente en los equipos puede detectar los equipos que se conectan a la red y no se reconocen.

Escaneo de sistemas: Se escanea software, configuraciones, dispositivos y se registra las vulnerabilidades que se puedan tener. Se puede escanear igualmente las configuraciones de cumplimiento de estándares, para identificar en qué punto puede no cumplirse un estándar de seguridad.

Identificar vulnerabilidades: En este apartado se identifican las vulnerabilidades dentro del inventario de la organización, las cuales son los resultados arrojados por el escaneo de sistemas, se debe tener en cuenta que el escaneo puede tener falsos positivos.

Clasificación y priorización de los riesgos: Esto se trata de corregir las fallas de seguridad que más puedan afectar a la organización, ya que puede ser difícil corregir todos los fallos a la vez o incluso en un periodo de tiempo por ser necesario una cantidad de recursos.[59]

---

[57] VEGA, Edgar. 2020. Planificación y Ejecuciíon de Evaluaciones de Seguridad Informática desde un Efoque de Ethickal Hacking. Alicante : Area de Innovacion y Desarrollo, 2020. pág. 98 p. ISBN 978-84-121459-4-6.

[58] Ibid., p 14.

[59] ROMERO, Martha, et al. 2018. Introduccion a la seguridad informatica y análisis de vulnerabilidades. Alicante : Area de Innovación y desarrollo, 2018. 123 p.. ISBN: 978-84-949306-1-4

Probar parches y configuración: El proceso de parcheo puede representar un riesgo para el funcionamiento del sistema, ya que es común que el software de parcheo tenga errores que no sean detectado. Por eso es una buena práctica inicialmente realizar el parcheo en una máquina y monitorear el funcionamiento. Igualmente, importantes es obtener los parches originales, directamente de los fabricantes.

Aplicar parches y configuraciones: Una vez se ha realizado las pruebas de los parches se procede a implementarlos en todas la maquinas, hay métodos de implementación para lotes de máquinas grandes, este proceso es dispendioso y se debe hacer seguimiento de cerca. [60]

Después de esto es necesario escanear nuevamente para asegurarse que se ha realizado una instalación adecuada de los parches y que todos los equipos se han parchado.

6.7 SEGURIDAD EN REDES

6.7.1 Vpn

VPN o Virtual Prívate Network aplicación para la red que permite hacer una extensión de la red local sobre una red pública no controlada tanto para IPv4 como IPv6 surge la necesidad de los trabajadores ya en la modalidad de soporte a distancia o teletrabajo garantiza la seguridad disponibilidad y confiable disminuye costos de desplazamiento y el en tiempo facilita la implementación de seguridad en los clientes ya que traslada las políticas de la empresa a sus terminales de trabajo, establecida en Internet con mecanismos de autenticación VPN punto a punto, consiste en conectar distintas sedes con la sede central, se implementa un servidor VPN.[61]

6.7.1.1 Tunneling

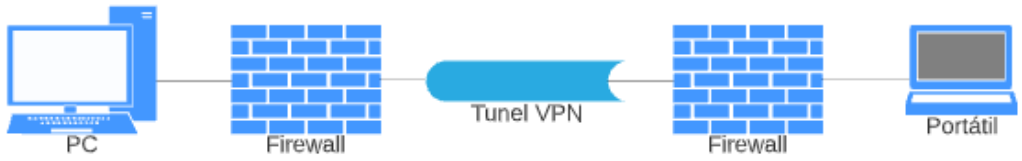
Consiste en encapsular un protocolo de red sobre otro creando un túnel dentro de una red, con los protocolos de comunicación como SSH.[62]

[60]Ibid. P. 46

[61] MARQUÉS, Guillermo. IPSec Redes Privadas Virtuales. s.l. : Ed. Lulu, 2016. pág. 66 p. ISBN 9781329824195.

[62] Ibid., 3 p.

Figura 13. Tunel vpn



Fuente: Elaboración del autor

6.7.1.2 VPN over LAN,

Acceso remoto, pero no utiliza internet sino la LAN. Se usa para aislar subredes o servicios de la LAN

6.7.1.3 VPN router a router.

La conexión a la red privada se realiza a través de un router. La autenticación se realiza desde los router

6.7.1.4 VPN firewall a firewall.

La conexión y autenticación se realiza a través de los firewalls. Las VPNs pues proporciona diversos servicios de seguridad tanto para IPv4 e IPv6. a la hora de implementar contingencias a violaciones de seguridad o falsificación y robo de información, basado en criptografía.

Estos servicios se implementan en la capa IP Control de acceso, Autenticación del origen de datos, Integridad sin conexión, Antireplay, Confidencialidad, Confidencialidad del tráfico de flujo limitada. Basándose en el uso de dos protocolos de seguridad, Authentication Header proporciona integridad sin conexión, autenticación del origen de los datos, y antireplay evitar que los atacantes inyecten o realicen cambios, y Carga de Seguridad Encapsulada ESP – (Encapsulating Security Payload) proporciona confidencialidad limitada de flujo de tráfico, a través de procedimientos. Acepta otras técnicas, como Kerberos. El intercambio de claves de Internet (IKE) protocolo usado comúnmente con el fin de establecer una Asociación de seguridad, su objetivo es la negociación también especifica el tiempo de vida de la sesión. [63]

[63]STALLINGS, William. Fundamentos se Seguridad en Redes Aplicaciones y Estándares. Seguridad en los sistemas. Segunda edición Madrid. Pearsons Education. 2004. 432 p. ISBN: 84-205-4002-1

6.7.2 DNSSEC (DOMAIN NAME SYSTEM SECURITY EXTENSIÓN)

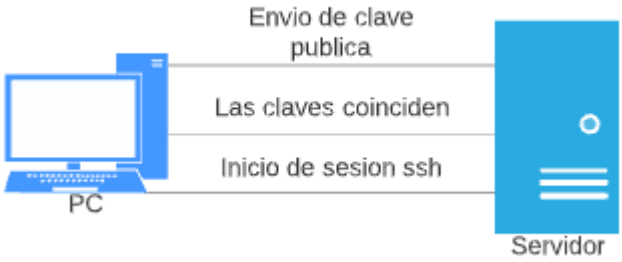
Añade una capa se seguridad a los servidores DNS dentro de un dominio. Funciona añadiendo firmas digitales en cada una de las partes: dominio, servidor dns y Registry. El proceso que usaría esta tecnología sería el siguiente:

El navegador del cliente comprueba los servidores dns asociados al dominio.
Si las formas coinciden con la del Registry, el navegador dará por válida la solicitud y mostrará el contenido.

Si las firmas no coinciden el sitio no será accesible.

6.7.3 Ssh

Figura 14. Protocolo SSH



Fuente: Elaborado por el autor

Este es un protocolo para administración remota, el cual permite modificar y controlar servidores de forma remota, por medio través de mecanismos de autenticación. Proporciona mecanismos de autenticación para el usuario remoto.

El servicio se creó como remplazo para el protocolo Telnet utilizando técnicas criptográficas para la comunicación desde y hacia el servidor. Los usuarios de los sistemas operativos Linux y MacOS pueden usar ssh en el servidor remoto desde la terminal, en Windows hay clientes para usar como Putty los comandos se ejecutan como si se estuvieran ejecutando en el equipo remoto.

La mayor ventaja de ssh es que utiliza el cifrado para la comunicación entre host y cliente, utiliza tres técnicas que son:

- Cifrado Simétrico
- Cifrado Asimétrico
- Hashing

OpenSSH soporta protocolos SSH-1 y SSH-2, por defecto cliente y servidor negocian la conexión SSH-2 primero, pasara a SSH-1 si no se completa, es posible escoger cual probará el cliente o el orden de prueba.[64]

6.7.3.1 Cifrado simétrico

Figura 15. Cifrado simétrico

Fuente: Elaborado por el autor

En esta forma se utiliza una clave secreta tanto para el cifrado como para el descifrado de los mensajes, para el host como para el cliente. Obviamente quien tenga la clave podrá descifrar los mensajes. Comúnmente se la llama clave compartida o cifrado secreto compartido.

[64]BARREN, Daniel, SILVERMAN, Richard y BYRNES, Robert**.** SSH, The Secure Shell, The Definitive Guide. Serverwide Configuration Segunda edición. California USA . Ed.OReilly Media, 2005. 645 p. ISBN: 0-596-00895-3

Se utiliza una o dos claves donde una clave se puede calcular por medio de la otra, las claves se utilizan durante el total de la comunicación, se utiliza un método acordado para derivar las claves entre el cliente y el servidor las cuales nunca son reveladas a terceros.

La seguridad de esta técnica radica en que la clave no se transmite entre cliente y host, si algún tercero logra capturar los datos no logrará descifrar la clave porque no conocer el intercambio de clave. Para cada sesión SSH se asigna un token secreto generado antes de la autenticación del cliente, lo que implica que también la contraseña escrita por el usuario por lo cual las contraseñas también están protegidas.[65]

6.7.3.2 Cifrado asimétrico:

Figura 16. Cifrado asimétrico

Fuente: Ilustrado por el autor

En este se utiliza claves separadas (2 claves) para cifrar y descifrar, estas dos claves se conocidas como clave pública y privada, cuando se juntan forman una clave pública-privada. La clave pública se comparte con todas las partes, pero la clave privada no se puede calcular mediante la clave pública. La relación determinada entre las dos claves puede llegar a ser bastante compleja.

La clave privada debe permanecer siempre privada para que la conexión sea completamente segura, el punto fuerte de este tipo de conexión radica en este hecho. El cifrado asimétrico no se utiliza durante toda la sesión ssh, solo se utiliza durante el algoritmo de intercambio de calves de cifrado simétrico. Antes de iniciar

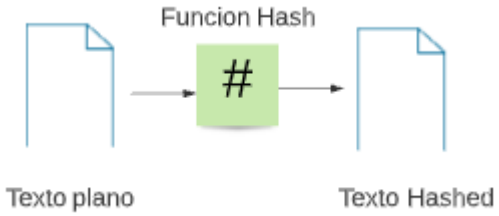
[65]HOSTINGER. Tutoriales Hostinger. "¿Qué Es El Protocolo SSH Y Cómo Funciona?" {En línea} {04 de Abril de 2020}. disponible en: (https://www.hostinger.es/tutoriales/que-es-ssh.)

una conexión ambas partes generan las claves público-privadas temporales y comparten sus respectivas claves privadas para producir la clave secreta compartida.

Una vez establecida la comunicación simétrica el servidor utiliza la clave pública del cliente para generar y transmitirla al cliente para su autenticación. Cuando el cliente descifra correctamente el mensaje quiere decir que cuenta con la clave privada para la conexión y comienza la sesión ssh.[66]

6.7.3.3 hashing:

Figura 17. Hashing



Fuente: Elaborado por el autor

Es otra forma de criptografía utilizada en SSH, se diferencia de las anteriores en que no están destinadas a ser cifradas, genera un valor de longitud fija lo que lo hace casi imposible de invertir, son muy utilizados para verificación de autenticidad de mensajes mediante unos códigos llamados HMACS, lo que asegura que el comando recibido no sea alterado de ninguna forma, es en algo similar al cifrado simétrico más un algoritmo de autenticación de mensajes donde cada uno de estos mensajes tiene un MAC que se calcula por medio de una clave simétrica y posteriormente es enviado fuero de los datos cifrados simétricamente como sección final dentro del completo paquete de comunicación.[67]

6.8 FUNCIONAMIENTO DE IPV4

[66]HOSTINGER. Tutoriales Hostinger. "¿Qué Es El Protocolo SSH Y Cómo Funciona?" {En línea} {4 de Abril de 2020} disponible en: (https://www.hostinger.es/tutoriales/que-es-ssh.)

[67] HOSTINGER. Tutoriales Hostinger. "¿Qué Es El Protocolo SSH Y Cómo Funciona?" {En línea} {4 de 04 de 2020} disponible en: (https://www.hostinger.es/tutoriales/que-es-ssh.)

En una red con protocolo TCP/Ip se le asigna una dirección lógica de 32 bits, la cual es dividida en las siguientes partes: la primera corresponde al número de la red y la segundad corresponde al número de la computadora. Estos 32 bits se dividen en 4 grupos de 8 bits cada uno, separados por puntos y escrito en formato decimal. Cada uno de los bits tiene su respectivo peso binario. Cada octeto tiene como valor mínimo 0 y como valor máximo 255.

6.8.1 Enrutamiento entre dominios sin clases

Se introdujo en el 93 y representa una gran mejora en la forma en que se interpretan las direcciones ip, da mayor flexibilidad al momento de dividir rangos de direcciones en redes separadas lo que permite eficiencia en el uso del protocolo ipv4 porque especifica prefijos de longitud variable, por otra parte, disminuye la carga de ruteadores principales de internet por un mayor uso de la jerarquía de direcciones.

Este estándar facilita el enrutamiento al permitir agrupar bloques de direcciones en una sola entrada de tablas de rutas. A estos se les llama bloques CIDR y comparten una misma secuencia de inicial de bits en la representación binaria de la dirección ip.

Los bloques CIDR en ipv4 se identifican de la siguiente forma; utilizando cuatro números decimales separados por puntos seguidos de una barra diagonal y un numero de 0 a 32. Estos números hacen referencia a la dirección inicial del bloque e incluye la máscara correspondiente.

Por otra parte, vale la pena mencionar que los prefijos cortos, es decir, los cercanos a cero incluyen más direcciones que los prefijos largos es decir los cercanos a 32. Esta característica tiene la particularidad de permitir que una misma dirección ip este incluida en prefijos de distinta longitud, los cual es especialmente útil para agregar prefijos de red y simplificar la cantidad de entradas en tablas de ruteo.[68]

6.8.2 Amenazas comunes en redes

Basados en análisis de cibercrimen de la policía nacional los incidentes más reportados son falsas ofertas publicadas en portales de comercio, seguido por el

[68]IPV6.MX.Fundamentos IPv4. {En línea} {10 de Abril e 2020} disponible en: (http://www.ipv6.mx/index.php/informacion/fundamentos/ipv4.)

phishing, el vishing y el smishing en este orden.[69] Las estafas de vishing y smishing consta de la difusión de un mensaje y contacto por parte del delincuente ofreciendo falsos premios y ofertas. Otras modalidades como el malware permiten que los delincuentes usen el ingenio para utilizar falsos correos de conocidas instituciones públicas como La Fiscalía General de la Nación, la DIAN, el SIMIT, que invitan al usuario a dar clic en links que contienen archivos infectados con virus que permite ver la actividad en el equipo atacado.[70]

Otras amenazas a las que se expone el usuario de red son:

Data corruption, daños en la información, Denial of service (Dos) servicios no disponibles, Leakage desviación de los datos, todos estos ataques están dirigidos remotamente.

Ingeniería social está enfocado a las personan que administran la información las engañan para obtener datos y poder superar las barreras o con falsos correos para que se modifiquen los datos originales esto se contrarresta con capacitaciones periódicas verificar los proveedores contar con un servicio técnico definido.

Ingeniería social inversa en este caso se publican paginas similares a las de los proveedores o se ofrece un servicio donde se pueda pedir información muchos de estos conocen las empresas a las que están atacando.

Evitar que el intruso tenga contacto con el sistema que se cuente con un servicio técnico experto y confiable.

Trashing (Cartoneo) esto buscan información en las papeleras los búferes de las impresoras ya que muchas personas copian sus contraseñas luego borran estos archivos o los envían al correo personal. [71]

Ataques de monitorización se observa el proceder diario de los usuarios para encontrar los datos que se buscan.

[69] POLICIA NACIONAL. 2017. Centro cibernetico policial. Amenzas del cibercrimen en Colombia 2016-2017. [En línea] [Marzo de 2019]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf.

[70] Ibid. p.5

[71] CHICANO, Esther. Auditoría de Seguridad Informática. Málaga : IC Editorial, 2014. 312 Pags. ISBN 978-84-16433-23-0.

Shoulder surfing en estos casos se busca encontrar los datos en las personas es espiar al en el momento de ingresar el password o tratar de encontrarlo en su entorno.

Decoy (Señuelos) programas parecidos que pregunten el login y el password o programas que guardan los primeros datos del teclado.
Scanning (Búsqueda) programas especializados en husmear dentro de las comunicaciones los puertos y se envía información o peticiones en diferentes puertos identificando los que responden.

Tcp connet scannig identifica los puertos tcp que están escuchando no es complejo el manejo, pero es fácil de detectar.
Tcp syn Scanning como los protocolos TCP están definidos en el vio de paquetes y define quien es el servido y cual el cliente como parte de su trama se capturan estos mensajes puertos y direcciones ip.

Fragmentation Scanning escaneo de puerto, pero los paquetes que se envían son fragmentados para que no se puedan identificar muy fácil.

Eavesdropping – packet sniffing se monitorean los paquetes que viajan en la red pueden ser local o en un router de internet toma direcciones ip iguales en forma promiscua y recibiendo todos los paquetes de esta red se pueden filtrar los datos basura y obtener información valiosa.

Snooping – Downloaning obtienen información original adicional ingresa para hacer copia de los documentos completos como correos.

Ataques de Autenticación tratar de ingresar tomando las mismas sesiones abiertas de los funcionarios o con el nombre del usuario.

Spoofing – looping tratar de hacerse pasar por otro en cascada ingresando a un equipo y desde allí ingresar a otro de más alto rango o servidor. Consiste en generar tráfico con un origen falseado de distinto modo lo que da origen a los distintos tipos de spoofing [72]

[72] DE LUIS, Erik. 2017. La seguridad de los menores en internet. Barcelona : Editorial UOC, 2017. 104 pags. ISBN 978-84-9116-963-5.

Spoofing se hacen sobre protocolos y es necesario conocer su funcionalidad y estructura los más comunes son:

Ip Spoofing se envían paquetes con direcciones ip falsas en caso de ser descubierto culpa al tercero por el que se está ingresando.

DNS spoofing en vía paquetes con udp engañando al servidor de dominio con una autenticación falsa.

web spoofing configura un sitio web idéntico al original en el cual se pueda interactuar con el usuario y preguntar los datos que se necesitan para pasar las barreras de acceso utilizando esta información para hacer cambios en el servidor original. [73]

Utilización de Backdoors llamadas puertas traseras como partes del código original que se tiene para agilizar la pruebas y que no se elimina cuando se pone en producción

Utilización de exploits se balen de las debilidades o agujeros de los algoritmos que se usan para encriptar contraseñas. [74]

Obtención de Passwords se prueba con posibles password incluso a varios equipos al tiempo Fuerza Bruta son millones de claves probadas para encontrar la correcta datos familiares.

Uso de Diccionarios se prueba de un listado de posibles password con gran cantidad de palabras que pueden ser posibles password compara la palabra encriptada con las del servidor original y descubrir el password.

[73] Ibid. pág. 44

[74] LAZARO, Francisco. Introducción a la informática Forense. Madrid : Editorial RA-MA, 2014. 340 pags.ISBN 978-84-9964-209-3.

Tampering o data didling modifica los programas instalados borrando archivos neurálgicos en la protección de la información predeterminar por sacar de producción el servicio para dejar fuera la competencia borrado de cuentas o deudas desviación de fondos.

Borrado de huellas es la tarea que se hace después de haber ingresado al sistema espera que no se enteren y se modifique la información que se quiere utilizar y poder ingresar de nuevo cuando se requiera.

Ataques mediante java applets programas basados en código por lo que expertos han encontrado algunos agujeros, aunque estos programas se refuerzan en la forma de utilizarse ya que piden autorización en cada cambio algunos han logrado vulnerar esta forma de hacer las operaciones.

Ataques con JavaScript y vbscript sitios web que funcionan con estos programas los atacantes utilizan las vulnerabilidades de los navegadores que son estándar y entre más viejos son más vulnerables.

Ataques mediante ActiveX esta tecnología desarrollada por Microsoft que funciona con certificados adicional a los controles activos y una firma digital del programador se leda la autonomía al usuario para que actúe de forma segura.

Errores de diseño implementación y operación en la red se están estudiando los sistemas operativos en busca de agujeros puertas traseras las aplicaciones de red y todos los servicios están en contando a diario errores que permiten el fácil ingreso.

6.8.2.1 Prevenciones de Estos Ataques

Para mitigar la mayoría de estos ataques con estar al tanto de su existencia y actualiza el sistema con los parches del proveedor principalmente en el sistema operativo, Asegurar las maquinas físicamente actualizar el personal en estos temas, controlar el broadcast desde fuera de la red, filtrar el tráfico ip Spoof, Auditorias en seguridad y detención, suscribirse a lista que brinden esta información.

Virus informático en general son pequeños programas de difícil detección que cuenta con información necesaria para utilizar otros programas y el hardware para multiplicarse en el mismo equipo u otro de la misma red algunos cambian de forma su función es alterar, y/o destruir programas, información o hardware se enfocan en

archivos ejecutable sectores de boot y tablas de partición de los discos, otros se ocultan en documentos como correos planillas de cálculo para causar mayores problemas y propagarse con facilidad.[75]

En la lista de contactos del que recibe el correo en páginas web se descargan vía ftp, aplicaciones de mensajería instantánea, grupos tratan de contagiar a todos los miembros

Tipos de Virus los Archivos ejecutables se adiciona a un archivo ejecutable (com, exe, dll, pif entre otros) al ejecutar estas tareas se aloja en la memoria de los equipos listo para infectar otras máquinas.

Virus en el sector de arranque se ubican en los primeros 512 bytes de una memoria disquete cuando un equipo inicia intenta iniciar desde el dispositivo y se infecta la máquina.

Virus residente se ubica en la memoria del equipo verifica los discos duros o extraíbles las memorias y sino están infectadas y almacenar su propio código.

Macrovirus infectan archivos de aplicaciones de oficina con fácil programación de macros me multiplica cuando se abre un nuevo documento.

Virus de mail se ocultan en las cuentas de correo en archivos tipo zip y al descomprimir se ejecuta estos utilizan las listas del usuario para propagarse.

Virus de sabotaje son más dirigidos ya que deben conocer el destino para poder ejecutar su acción dañan entornos o sistemas.

Virus de applets java y controles activex se programan sobre aplicaciones java o activex y se replican mientras estén conectados a una red de internet.

Reproductores – gusanos programas que se reproducen de forma continua hasta terminar con el espacio de los discos o de la memoria guarda información.

---

[75] PARDO, Ezequiel. 1993. Microinformática de gestión. Oviedo : Publicaciones Universidad de Oviedo, 1993. pág. 373 p. ISBN 84-7468-788-8.

Caballos de troya se introduce un programa dentro de otro para que funcione de manera normal y su detección se dificulte y poder dañar al sistema o tomar el control.[76]

Bombas lógicas se implanta programas para que dado un evento especial o una fecha determinada se ejecuten y sabotear el sistema dejándolo fuera de servicio o modificando información.

Modelo de virus informático consta de tres partes el de reproducción, ataque y defensa son subrutinas dentro del mismo programa.

Programas de Antivirus programas que cuentan con un gran listado de la huella que dejan los virus conocidos no evita la creación de nuevos virus se analizan archivos y documentos para detectar actividades sospechosas o similares a las conocidas.

Detectar el virus promedio de un Scanning revisa el código en busca de pequeñas porciones de código que puedan pertenecer a un virus Heurística analiza la información de usuario para detectar algún cambio en zonas generalmente no controladas el inconveniente son las falsas alarmas Chequeadores de integridad monitorea los sectores críticos detectando cambios en el pc.

Controlar el virus la posibilidad de erradicar el virus con la opción de restauración de algunos archivos dañados, o buscar una copia de seguridad archivos perdidos o dañados.

6.9 MECANISMOS ANTE RIESGOS DE SEGURIDAD

Los mecanismos de seguridad informática se componen de técnicas y herramientas que permiten disminuir el riesgo en la exposición de la confidencialidad, disponibilidad e integridad de la información.

[76] LEÓN, Mario. 2004. Diccionario de informática Telecomunicaciones y ciencias afines. Madrid : Ed. Babel, 2004. pág. 1348 p. ISBN 84-7989-626-4.

6.9.1 Autenticación:

Este mecanismo busca la identificación del usuario del sistema, por ejemplo, al ingresar a un equipo, una red o una base de datos. Es posible la autenticación de las siguientes formas:

- Lo que uno saber, por ejemplo, contraseñas
- Lo que uno tiene, por ejemplo, un token
- Lo que uno es, por ejemplo, huella digital y biometría

Es común utilizar uno o más métodos de autenticación, lo que trae como ventaja que la autenticación de un usuario se haga de la forma correcta y que el usuario autorizado realmente sea quien intenta acceder al sistema. Esta decisión, de usar uno o más o cuales usar se determina por el valor que se le da a la información que se busca proteger, la organización en consideración a esto lo determinará. Una vez se ha realizado la autenticación cada usuario dispone de unos roles o niveles de acceso a la información.[77]

El uso de contraseñas es ampliamente usado actualmente, pero muchas veces no se hace de la forma correcta, el éxito de este método está en gran parte determinado por el usuario, ya que al usar contraseñas fuertes y difíciles de adivinar o romper será igualmente más difícil para un atacante vulnerar el sistema de autenticación.

Las contraseñas deben ser en todo caso confidenciales y es responsabilidad del dueño resguardarla y que esta no se transferida de ninguna forma, por lo anterior es una mala práctica anotarla en papeles y prestarla a otra persona. Las contraseñas seguras deben tener un conjunto de caracteres lo suficientemente amplio como para evitar ser adivinada, junto con la incorporación de números y signos, minúsculas y mayúsculas, así como el cambio de contraseña de forma constante.

6.9.2 Autorización:

El proceso de autorización determina el cómo, cuándo y dónde un usuario tiene acceso a recursos corporativos. Los recursos se deben organizar en niveles y de

[77] AGUILERA, Purificación. Seguridad Informática. Madrid: Ed. Editex, 2010. ISBN 978-84-9771-657-4.

acuerdo con el nivel se le concede un grado de autorización, lo anterior basado en la importancia o valor de la información.

Para autorizar el uso de recursos se suele usar formularios y contraseñas, y es importante llevar un registro para controlar las autorizaciones, las cuales solo se conceden a quienes por el desarrollo de sus actividades en la organización lo requieran, en caso contrario siempre el acceso será denegado.[78]

6.9.3 Administración:

Elimina, mantiene y define el tipo de autorización de los usuarios de los sistemas. Es una actividad de gran dinamismo que requiere actualización constante, esto debido a la constate evolución d ellos sistemas y los riesgos que día a día aparecen en la red. Para esta tarea se utiliza software incorporado den los mismos sistemas operativos, o también se puede utilizar software específico para tal fin.

6.9.4 Auditoria y registro:

La auditoría es la vigilancia de los servicios de producción valiéndose del análisis de información. El registro por su parte el registro es un mecanismo que almacena los intentos de vulnerar un sistema con el fin de poder analizarlo posteriormente. La característica en común de estos dos procesos es que requieren de un análisis posterior, existen métodos manuales y automatizados para realizar estas tareas y la frecuencia con la cual se hace depende del nivel de riesgo y o crítico de la información.[79]

6.9.5 Código de detección de modificación:

Este mecanismo consiste en una suma que se agrega a los datos que se quieren transmitir, el receptor efectúa la comprobación por medio de la recepción de la suma junto a los datos. La suma es implementada por métodos criptográficos y debe arrojar el mismo resultado tanto en el emisor como en el receptor.

---

[78] AGUILERA, Purificación. Seguridad Informática. Madrid : Ed. Editex, 2010. ISBN 978-84-9771-657-4.

[79] MIFSUD, Elvira. "Listas de Control de Acceso" {En Línea} {30 de Mazo de 2020} disponible: http://recursostic.educacion.es/observatorio/web/ca/software/servidores/1065-listas-de-control-de-acceso-acl?start=3.

6.9.6 Código de autenticación del mensaje:

Similar al anterior, cuando el receptor realiza la comprobación puede estar seguro de la veracidad del emisor mediante una suma cifrada al enviar el mensaje.

6.9.7 Firma digital:

Consiste en una función relacionada a un documento con clave privada del firmante, por lo que la firma depende exclusivamente del mensaje y del emisor del mismo. Se utiliza para para servicios de no repudio debido a la certeza que tiene el receptor sobre el emisor del mensaje.[80]

6.9.8 Numero de secuencias de mensaje:

A cada paquete de transmisión en la que puede llegar a ser dividido se le asigna un número que poder ser cifrado o no cifrado, este número identifica el paquete por medio de una secuencia de bits, el receptor verifica que esta secuencia corresponde a los paquetes que está recibiendo, este proceso permite identificar la inserción o sustracción de paquetes dentro del mensaje.

6.9.9 Cifrado:

El cifrado impide que usuarios o procesos puedan entender la información transmitida transformándola para que sea ilegible. Por medio de técnicas de cifrado la seguridad de la información se logra por la protección cifrada junto a otros mecanismos de seguridad.[81]

6.9.10 Relleno de tráfico:

[80] BORJA, Lázaro. Certificación de la firma digital.Primera edición. Madrid: Ed. Forem, 2005. pág. 77. ISBN 84-933150-5-2.

[81] AGUILERA, Purificación. Seguridad Informática. Madrid : Ed. Editex, 2010. 240 p. ISBN 978-84-9771-657-4.

Consiste en enviar datos falsos junto a los datos verdaderos, con el fin de engañar a quien pueda estar monitoreando la red y analizando el tráfico haciendo difícil discriminar entre información útil y la que no lo es.

6.9.11 Certificación:

La certificación la realiza un tercero, un agente de confianza, el cual certifica la integridad, frecuencia y secuencia de los datos, así como del receptor y del emisor de estos. [82]

[82]SUAREZ, Rodrigo." Mecanismos de Seguridad Informática". {En línea} {19 de Abril de 2020} disponible en:. (http://blogs.acatlan.unam.mx/lasc/2016/04/19/mecanismos-de-seguridad-informatica/.)

7. FASE 2. SIMULACIONES DE EXPLOTACIÓN

En esta fase se realiza la vulneración de la red doméstica con lo cual se logrará identificar algunas de las vulnerabilidades existentes, basados en la metodología PTES (Penetration Testing Execution Standar). Este estándar consta de siete secciones elaboradas con el soporte de analista y expertos de seguridad con el fin de cubrir todos los aspectos relacionados con una prueba de penetración, dada la naturaleza de esta monografía se toma como referente basado en esta metodología la cuarta y quinta fase de PTEST comprendida como Análisis de vulnerabilidades, y Explotación, que a su vez comprende Análisis de tráfico, Factor Humano, Ataques Wi-FI.

7.1 CONFIGURACIÓN DEL AMBIENTE VIRTUAL DE SIMULACIÓN

El ambiente virtual de simulación comprende el uso de software de uso libre, se usa aplicaciones como virtual box para la virtualización de las máquinas, es decir, simular que se tiene más de un equipo utilizando en realidad solo una máquina física. En cuanto a sistemas operativos se usa Kali Linux, Debian y Windows 10, los dos primeros son distribuciones libres de Linux de las cuales se entrega información sobre características y uso a continuación:

7.1.1 Virtual box

Virtual Box es una aplicación que se usa para crear máquinas virtuales en las cuales se puede instalar sistemas operativos. Por ejemplo, si se tiene un computador con sistemas operativo Windows se puede ejecutar VirtualBox en el cual correrá un sistema operativo Linux, es decir los dos sistemas operativos estarán disponibles dentro del mismo computador. Esta virtualización se usa para realizar pruebas de distintos tipos en lo que suele llamarse un ambiente controlado.[83]

7.1.2 Instalación de virtual box

La instalación de VirtualBox se realiza sobre Windows 10. Es un proceso sencillo que no requiere mayores conocimientos de configuración y la mayoría del proceso

[83] GONZALEZ, Jesus. 2017. "Tutorial de Virtual Box para emular sistemas operativos". [En línea]. [04 de 08 de 2020.] disponible en: https://www.softzone.es/manuales-software-2/tutorial-de-virtualbox/.

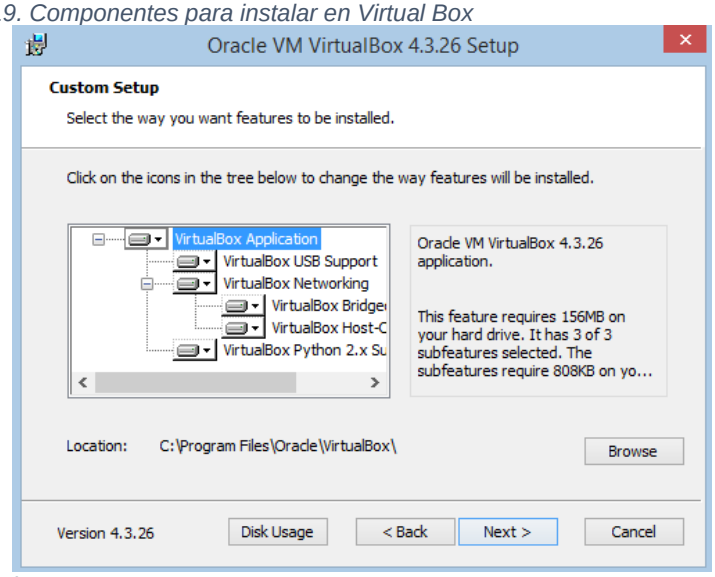
consiste en dar paso a la instalación, inicialmente se debe identificar el archivo de instalación el cual se puede descargar de la página oficial https://www.virtualbox.org/ para ejecutarlo en Windows, la Figura 13 muestra como inicia la instalación:

Figura 18. Inicio de la instalación Virtual Box

Fuente: El autor

La instalación de VirtualBox ofrece la posibilidad de configurar lo que se quiere instalar, así lo muestra la Figura 14, lo recomendado para el usuario es dejar la configuración como viene por defecto:

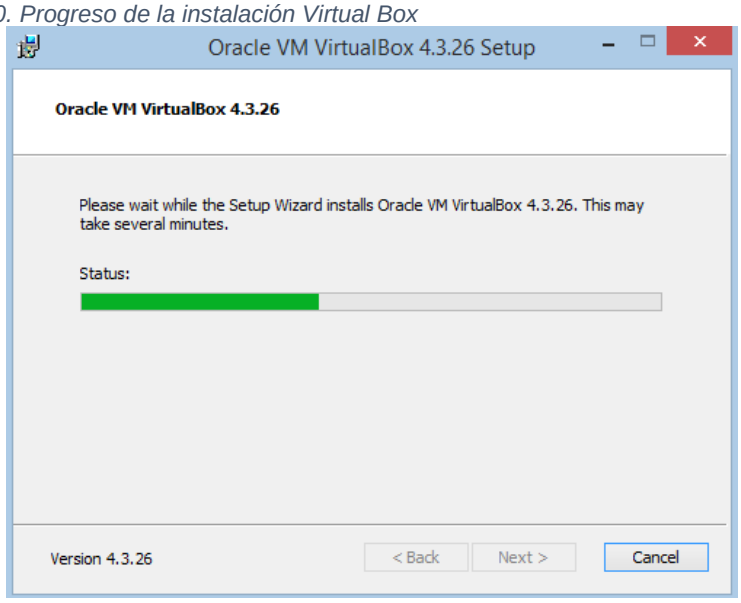
Figura 19. Componentes para instalar en Virtual Box



Fuente: El autor

La instalación comienza a correr y se puede ver el progreso de una barra de color verde como muestra la Figura 15, la instalación normalmente corre sin inconvenientes y tarda solo unos pocos minutos:

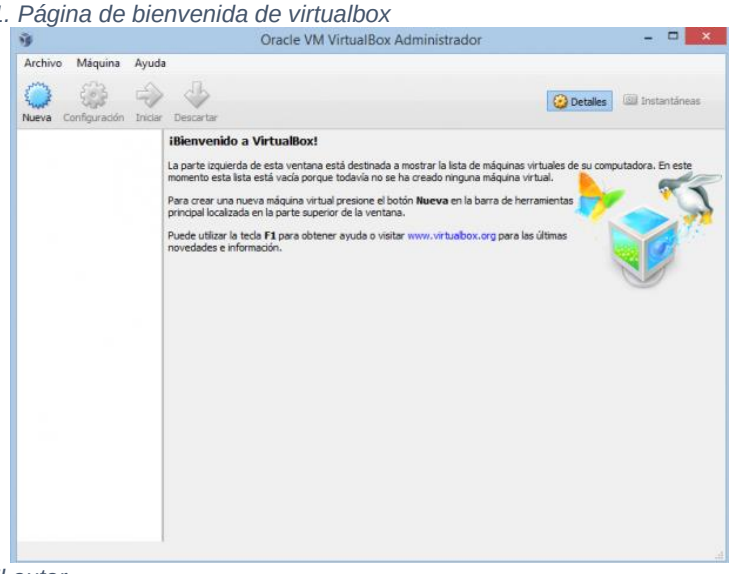
Figura 20. Progreso de la instalación Virtual Box



Fuente: El autor

Al finalizar la instalación se puede ejecutar inmediatamente la aplicación, no hay problema alguno al hacerlo así. La página de bienvenida ofrece información sobre el funcionamiento general de VirtualBox como lo muestra la figura 16:

Figura 21. Página de bienvenida de virtualbox

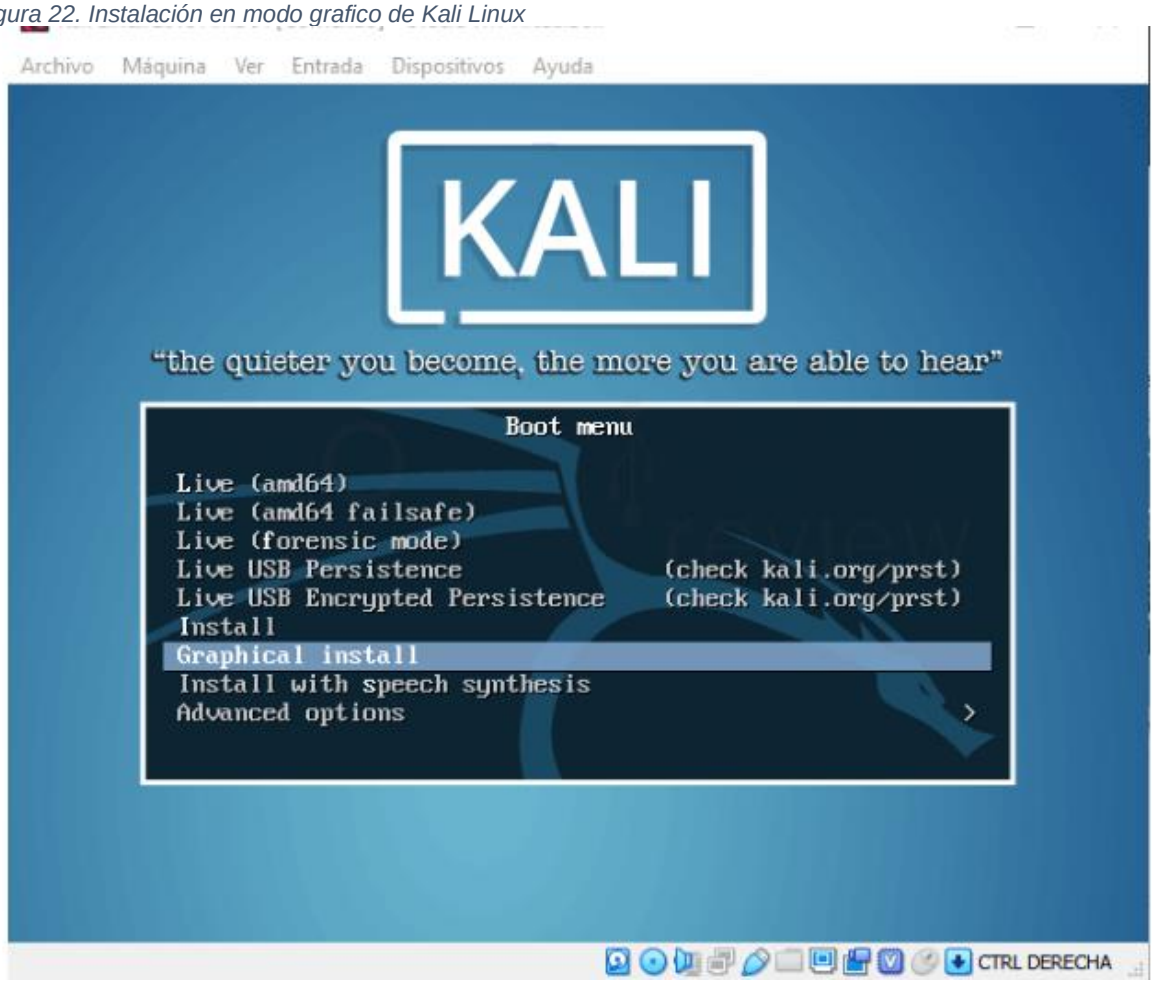


Fuente: El autor

7.1.3 Instalación de Kali Linux

Kali Linux es un programa especializado para detectar fisuras de seguridad en redes informáticas, se usa también para análisis informático forense con el fin de descubrir por donde se atacó un sistema y encontrar rastros de este. La idea en la creación de este software es la de desarrollar la seguridad de las redes informáticas, para lo cual cuenta con cerca de 300 herramientas y aplicaciones para tal fin que incluye desde escaneo de puertos hasta crackeador de contraseñas.[84]

Figura 22. Instalación en modo grafico de Kali Linux

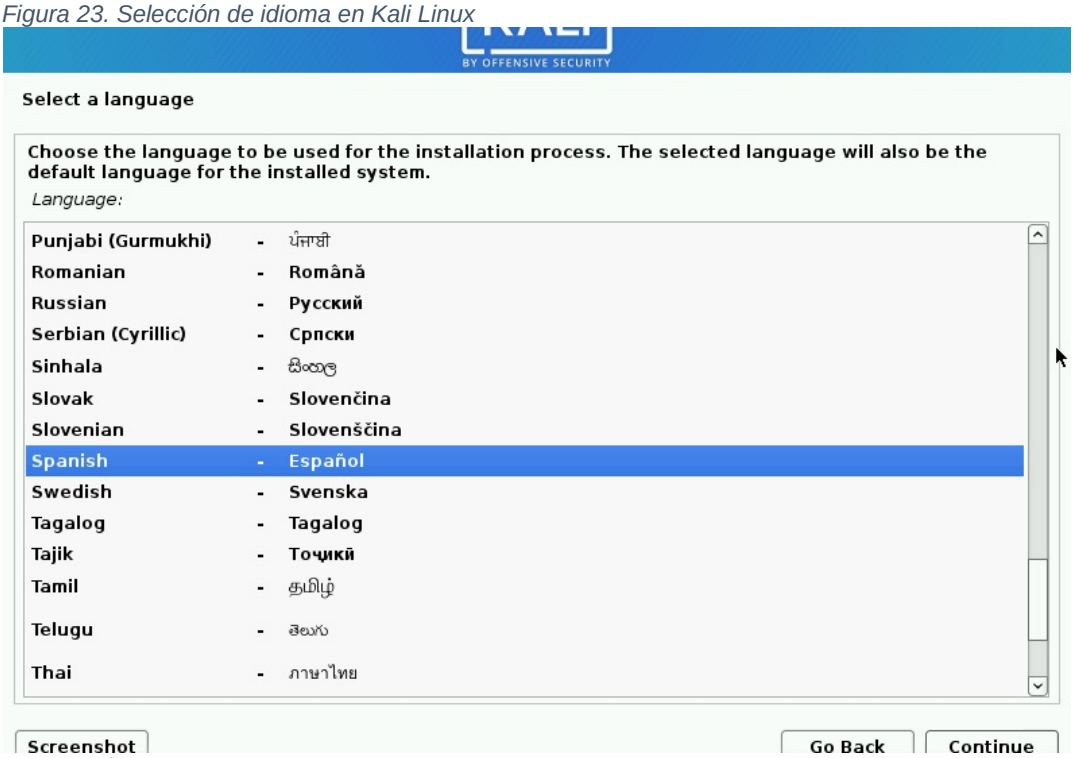


Fuente: El autor

[84] RUBEN, Andres. Que es Kali Linux y que puedes hacer con el. [En línea] [04 de 08 de 2020.] disponible en: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671.

Luego de iniciar la instalación en VirtualBox, Kali Linux permite seleccionar el idioma de instalación, el idioma que se selecciona en este punto es el que va a mostrar el sistema operativo durante el uso de este, para este caso se selecciona español como lo muestra la Figura 18:

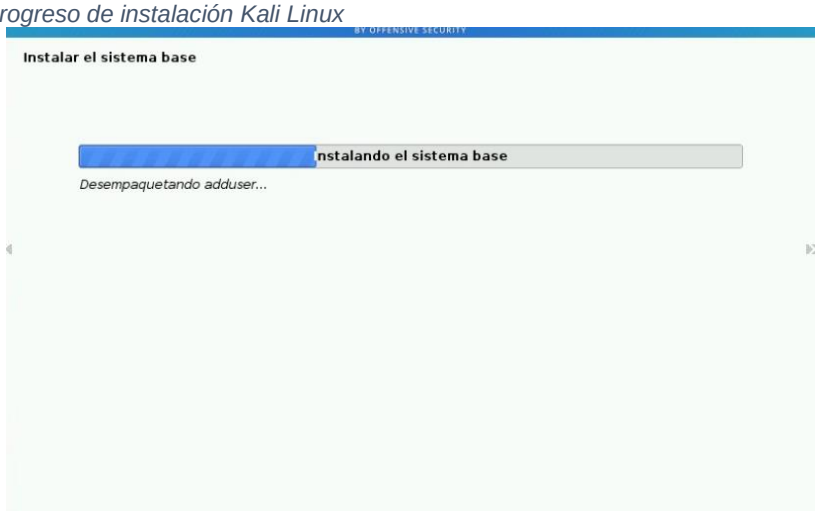
Figura 23. Selección de idioma en Kali Linux



Fuente: El autor

Posteriormente comienza la instalación de Kali Linux, una barra de color muestra el progreso de la instalación (Figura 19), en este punto se debe esperar a que corra completamente la instalación para que no se presente ningún problema, es útil tener presente no apagar el equipo físico en el cual se está realizando la instalación:

Figura 24. Progreso de instalación Kali Linux



Fuente: El autor

Después de correr la instalación se muestra un aviso donde lo indica, (Figura 19) posteriormente se puede dar inicio al sistema operativo Kali Linux dentro de la máquina virtual. Es bueno recordar que el usuario por defecto será root. es decir, con privilegios de administrador y la contraseña de ingreso es la que se haya indicado en la instalación:

Figura 25. Finalización de la instalación Kali Linux

Fuente: El autor

7.2 PASOS QUE SE UTILIZARAN PARA LAS PRUEBAS DE EXPLOTACIÓN DE VULNERABILIDADES.

Para realizar las pruebas, se realizarán las siguientes fases basados de la misma forma en la metodología PTES:

7.2.1 Interacciones previas:

Alcance: La realización de las pruebas del presente trabajo se enmarca dentro de una red de uso doméstico, la conexión de red se realiza de forma inalámbrica, soportado en software de virtualización de sistemas operativos, dentro de la red se analiza el tráfico que se encuentra en la misma, la rede wi fi se verá sujeta a pruebas en el punto más débil que es el establecimiento de contraseñas seguras. No se pretende tratar de hackear la red ya que el objetivo principal es dar a la luz algunas vulnerabilidades que pudiera encontrar un usuario que se encuentra dentro de su propio hogar y lograr conciencia en aspectos referentes a la seguridad informática.

7.2.2 Recogida de información:

En esta fase se detalla la información recogida, se pretende tener una información completa sobre donde se realizará la prueba, esta información es útil para las fases posteriores.

Recopilación de información nivel 1: En este punto se debe tener en cuenta que al ser un laboratorio planeado se cuenta de antemano con información acerca de la red, lo que se denomina una prueba de caja blanca. La información es la siguiente:

7.2.2.1 Maquina física:

La máquina física es el equipo de cómputo que se utiliza para realizar la prueba, el cual cuenta con el Sistema operativo Windows 10 home, la conexión de red de este equipo se establecer mediante la red Wi-Fi, es decir se conecta a la red del hogar de forma inalámbrica, los equipos portátiles cuentan con adaptadores de red inalámbrica que son los que permiten este tipo de conexión, el adaptador de la máquina física tiene un número que lo identifica, este número es conocido como dirección mac (Media Access Control), que es única para cada dispositivo, en este

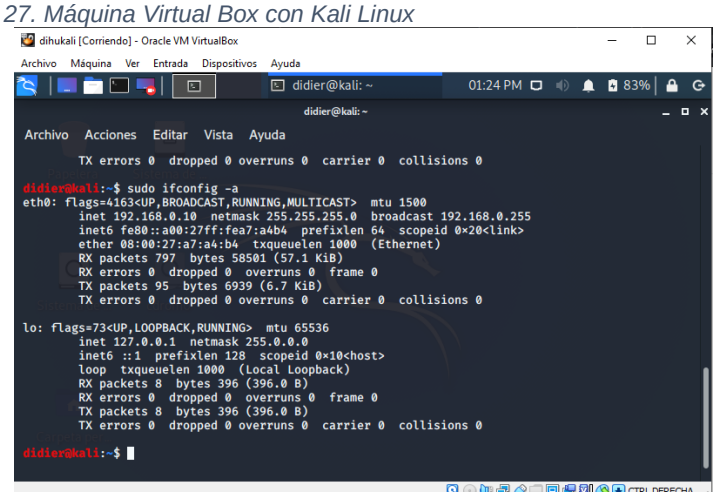
caso la mac de la tarjeta inalámbrica es la línea que dice dirección física, la cual tiene el número 2A-67-B0-75-EE-65 y la dirección ip 192.168.0.14 como lo muestra la imagen 21:

Figura 26. información de la máquina física

Fuente: Elaborado por el autor

Entonces, se tiene dos máquinas virtuales, la Figura 22 muestra la configuración de la máquina virtual donde se instaló Kali Linux, la máquina virtual al simular que es “otro equipo” asigna una también una dirección ip, esta es distinta a la que se asigna a la máquina física, es decir a la que tiene el sistema operativo Windows, la dirección asignada a la máquina virtual con Kali Linux es 192.168.0.10, así mismo la virtualización le asigna una mac como si de un adaptador de red se tratase, se puede identificar el número que tiene esta el cual es 08:00:27:A7:A4:B4, como se puede ver en la imagen:

Figura 27. Máquina Virtual Box con Kali Linux

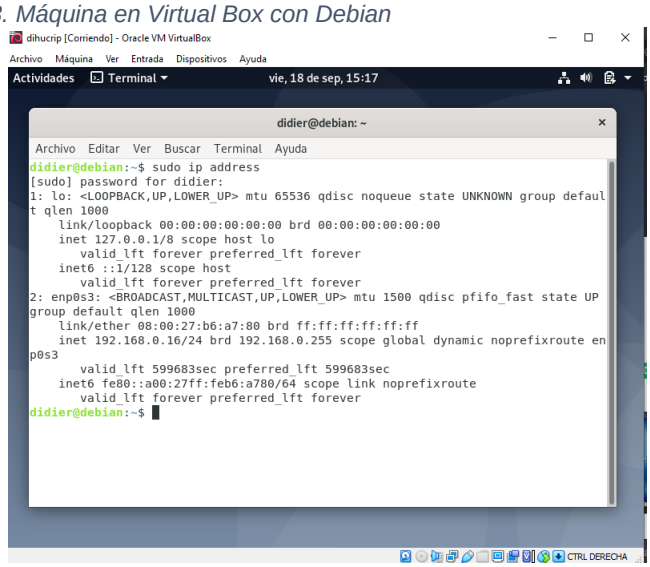


Fuente: Elaborado por el autor

7.2.2.2 Máquina Virtual con Sistema operativo Debian:

Continuando, se tiene la segunda máquina virtual, la Figura 23 muestra la configuración de la máquina virtual donde se instaló Debian, la máquina virtual al simular que es “otro computador” asigna una también una dirección ip, esta es distinta a la que se asignó a la máquina física y también a la máquina virtual Kali Linux, la dirección asignada a la máquina virtual con Debian es 192.168.0.16, así mismo la virtualización le asigna una mac , el número que es 08:00:27:B6:A7:80, como se puede ver en la imagen:

Figura 28. Máquina en Virtual Box con Debian

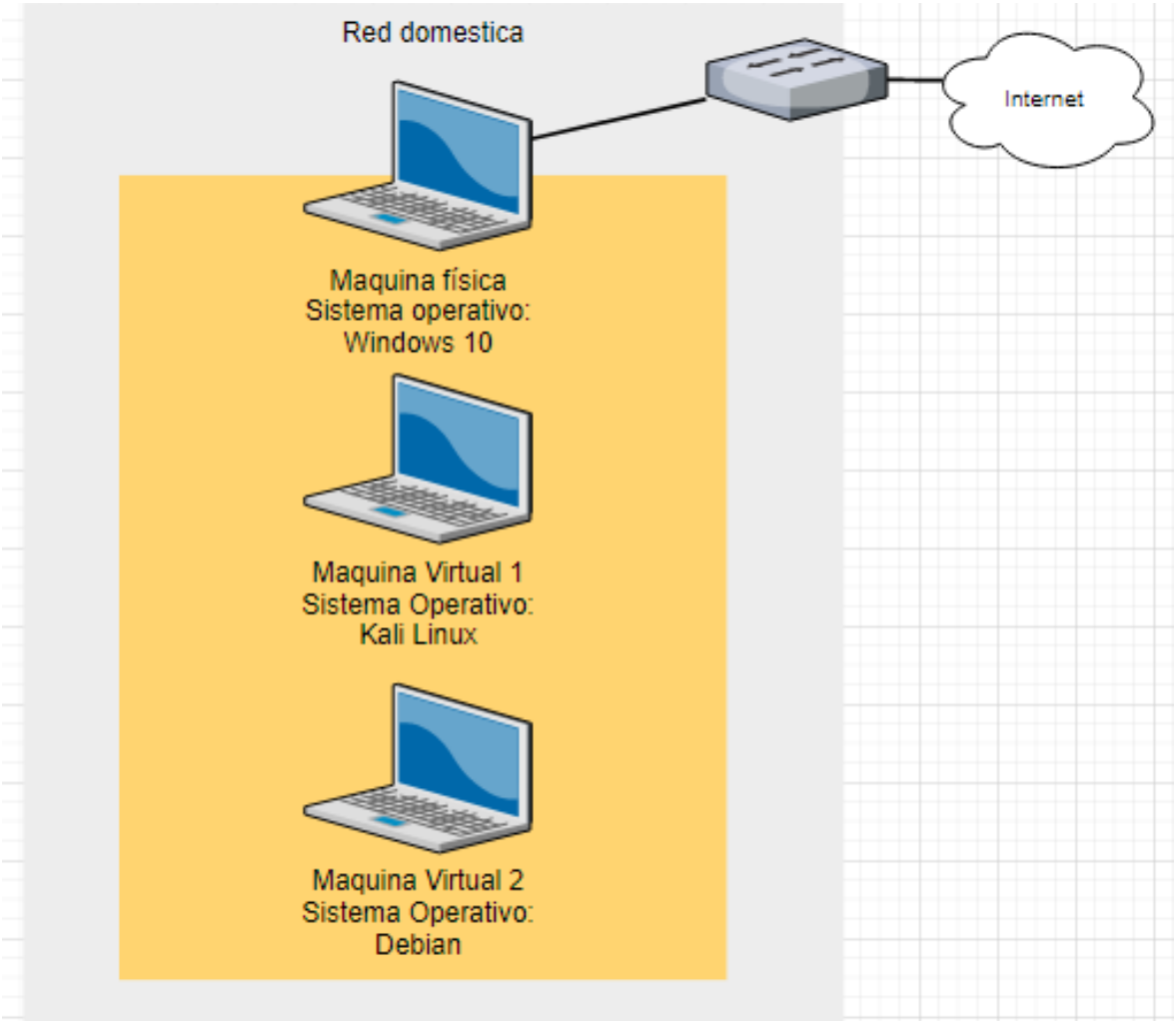


Fuente: Elaborado por el autor

7.2.2.3 Diagrama de red:

La Figura 24 muestra el diagrama de red donde se realizan las pruebas, es la forma gráfica de representar las maquinas virtuales respecto a la máquina virtual, se muestra que la máquina física hospeda las dos máquinas virtuales, es decir es hacer de cuenta que se tiene tres computadoras, cada una con un sistema operativo distinto y con su respectiva conexión de red para acceso a internet, aunque en realidad las tres acceden a internet a traves de un mismo router, que es con el que cuenta la red doméstica. En resumen, se cuenta con tres maquinas (una maquina física y dos máquinas virtuales) y se tiene tres sistemas operativos Windows 10, Kali Linux y Debian OS.

Figura 29. Diagrama de red doméstica



Fuente: Elaborado por el autor

7.3 IDENTIFICACIÓN Y ANÁLISIS DE ALGUNAS VULNERABILIDADES

7.3.1 PRUEBAS.

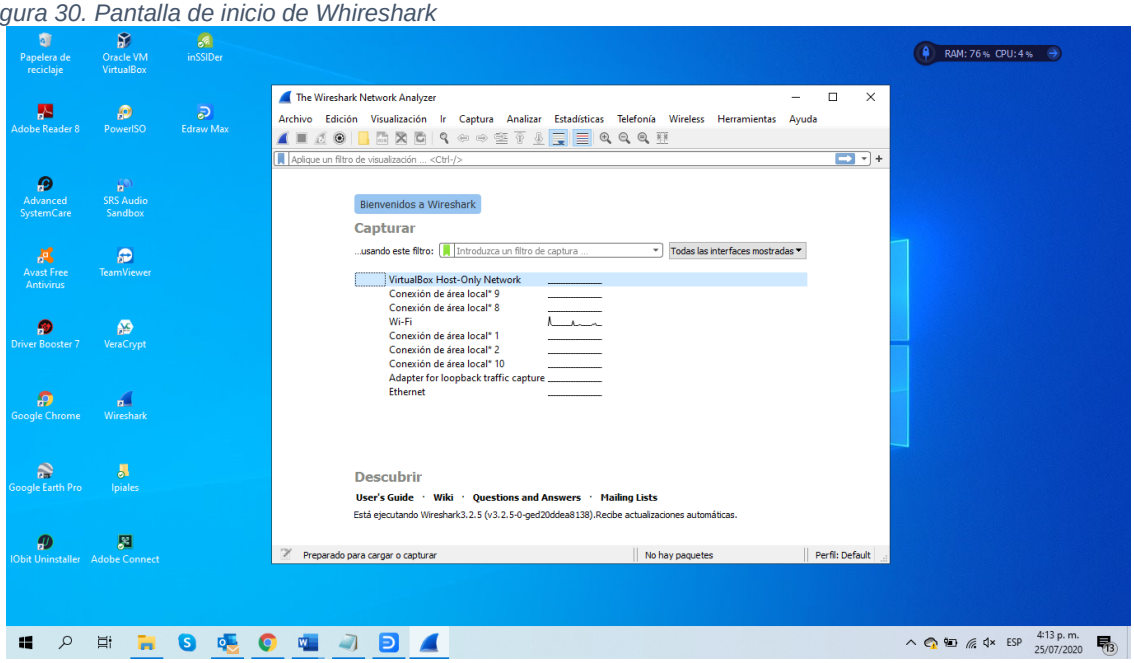
Durante esta fase se descubren las fallas de seguridad de la red doméstica y que representa una debilidad que un atacante podría aprovechar. Las pruebas que se realizan comprenden análisis de tráfico, Ataque Wi-Fi y Factor Humano, la anterior basado en la misma metodología PTES.

7.3.1.1 Análisis de Tráfico:

El análisis de tráfico es la técnica que permite la identificación del tipo de información que se envía a través de una red, comprende el reconocimiento de los protocolos de información que se encuentran dentro del tráfico de la red y con este conocimiento los ciberdelincuentes pueden perpetrar un ataque.

Para el análisis de tráfico se utiliza Whireshark, este es un software gratuito que permite el análisis de tráfico en tiempo real. Esta herramienta también permite la solución de problemas de red como latencia e incluso identificar actividad maliciosa dentro de la red. En la Figura 25 se puede ver el entorno gráfico de Whireshark:

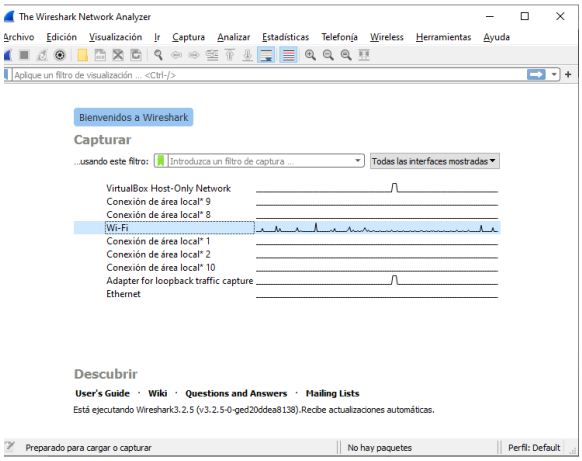
Figura 30. Pantalla de inicio de Whireshark



Fuente: El autor

Whireshark muestra las redes disponibles, así como lo muestra la Figura 26, al seleccionar una de las redes se realiza la captura del tráfico de esta, para comenzar la captura se elige la tarjeta de red que se encuentra conectada a la red donde se realiza la captura o “escuchar” como también suele conocerse este proceso:

Figura 31. Red WiFi detectada por Whireshark



Fuente: El autor

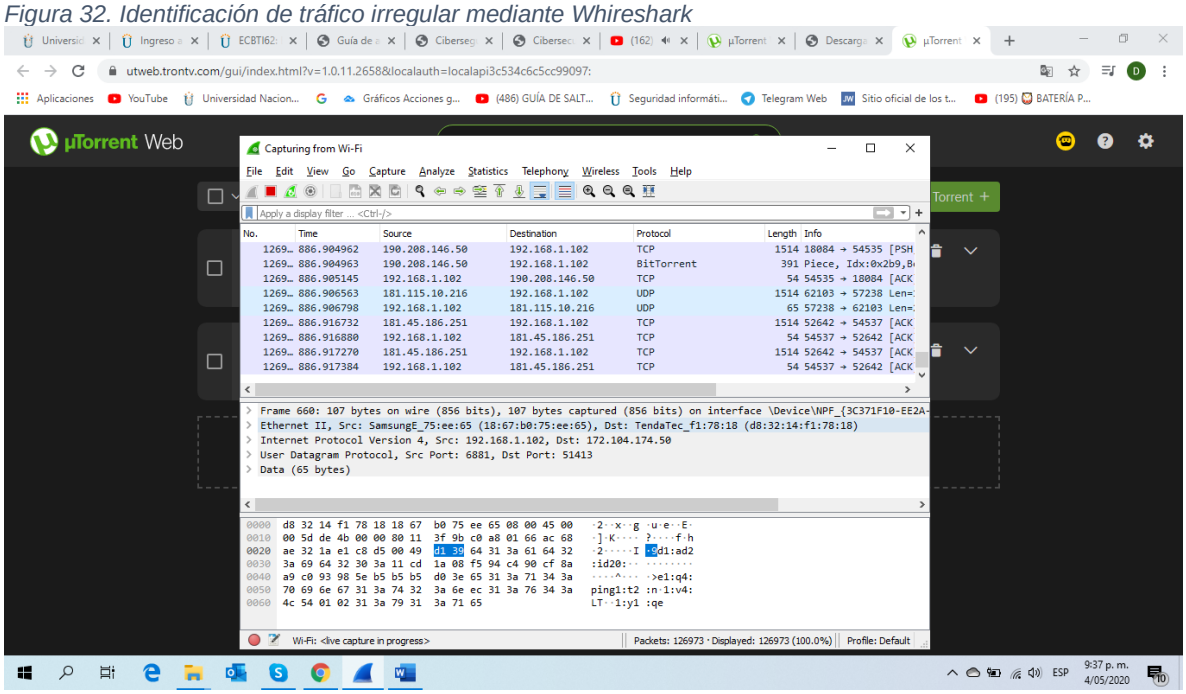
Una vez se inicia la captura dentro de la red Wi-Fi se identifica la columna “Protocolo” en Whireshark para visualizar el tráfico de los paquetes que ha pasado por la red, dentro de los cuales se encuentran paquetes del protocolo TCP (Protocolo de Control de Transmision) y el protocolo IP (Protocolo de Internet) y otros protocolos de internet como POP, SMTP, y HTTP.

En la siguiente imagen se ve paquetes del protocolo UDP (Protocolo de diagramas de usuario) resaltado en color verde, el cual es un protocolo de uso común en redes ya que este protocolo es usado por muchas aplicaciones cliente-servidor para procesos de solicitud-respuesta. También se ve un paquete con un protocolo bit Torrent, el cual es la base para intercambio de archivos entre distintos ordenadores, los usuarios descargan el archivo desde la fuente original y comparten entre si partes ya descargadas.

El protocolo Bit Torrent en si no es considerado como malicioso, pero se le ha dado un carácter de amenaza de seguridad con relación a riesgos inherentes a la

publicidad que muestran estos programas, ya que el uso u Torrent puede estar ligado al uso de Ad-ware, la Figura 27 muestra el protocolo identificado: [85]

Figura 32. Identificación de tráfico irregular mediante Whireshark

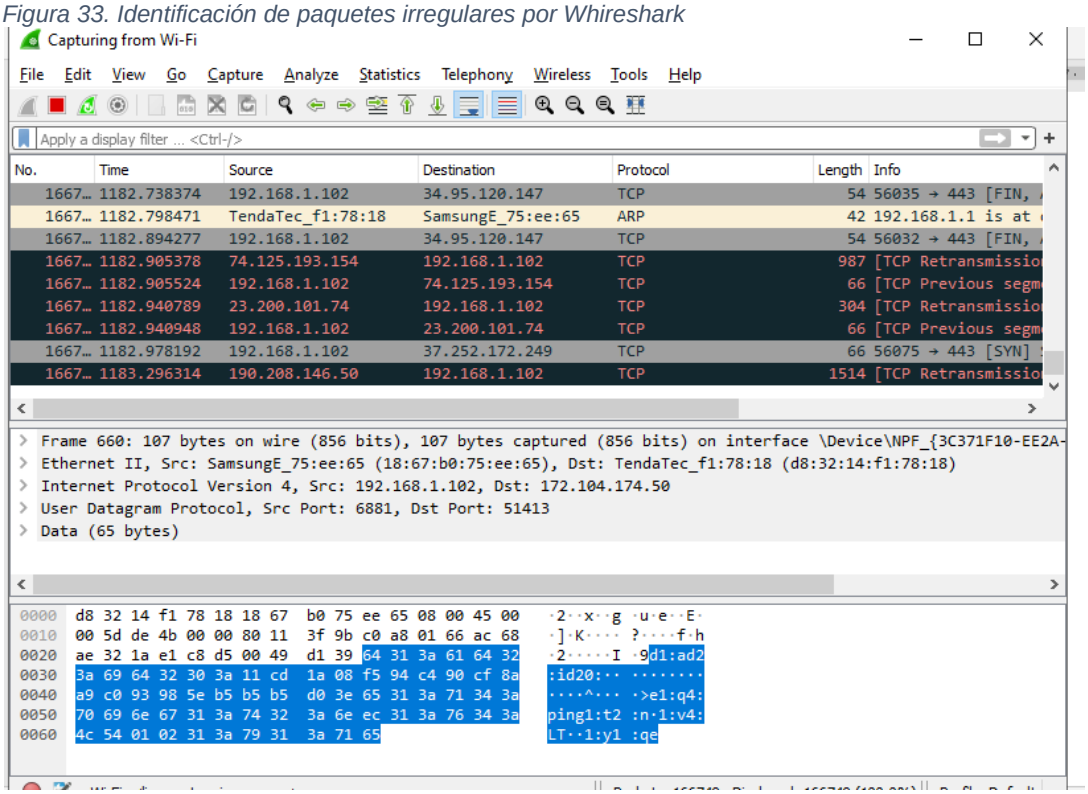


Fuente: el autor

Mediante whireshark se identifican los paquetes que viajan por la red, dentro de los cuales se encuentran algunos que no es usual encontrar dentro de una red, de la misma forma se identifica tráfico desde muchas direcciones ip distintas y muchos paquetes malos como se puede visualizar en la Figura 28 a continuación.

[85] GONZALEZ, María. XATAKA. *Qué es y cómo funciona el protocolo BitTorrent.* (En línea). [27 de 07 de 2020.] Disponible en: https://www.xatakamovil.com/conectividad/que-es-y-como-funciona-el-protocolo-bittorrent

Figura 33. Identificación de paquetes irregulares por Whireshark



Fuente: El autor

7.3.1.2 Ataque Wi-Fi

Hay disponibles ataques para los diferentes protocolos de seguridad de red inalámbrica, entre estos protocolos se encuentran: WEP, WPA2, EAP-FAST, EAP-LEP. Cada uno de estos tiene una forma de ataque la cual puede ser aprovechada por los ciberdelincuentes, usando métodos de ataque como el cracking de contraseñas wi-fi, Hotspots falsos con los cuales el usuario puede ser víctima de código malicioso. El espionaje es otra de las vulnerabilidades de las redes inalámbricas sin protección con lo cual un usuario puede exponerse a interceptación de comunicaciones, así como la modalidad de Robo de datos también puede darse si la red tiene brechas de seguridad.[86]

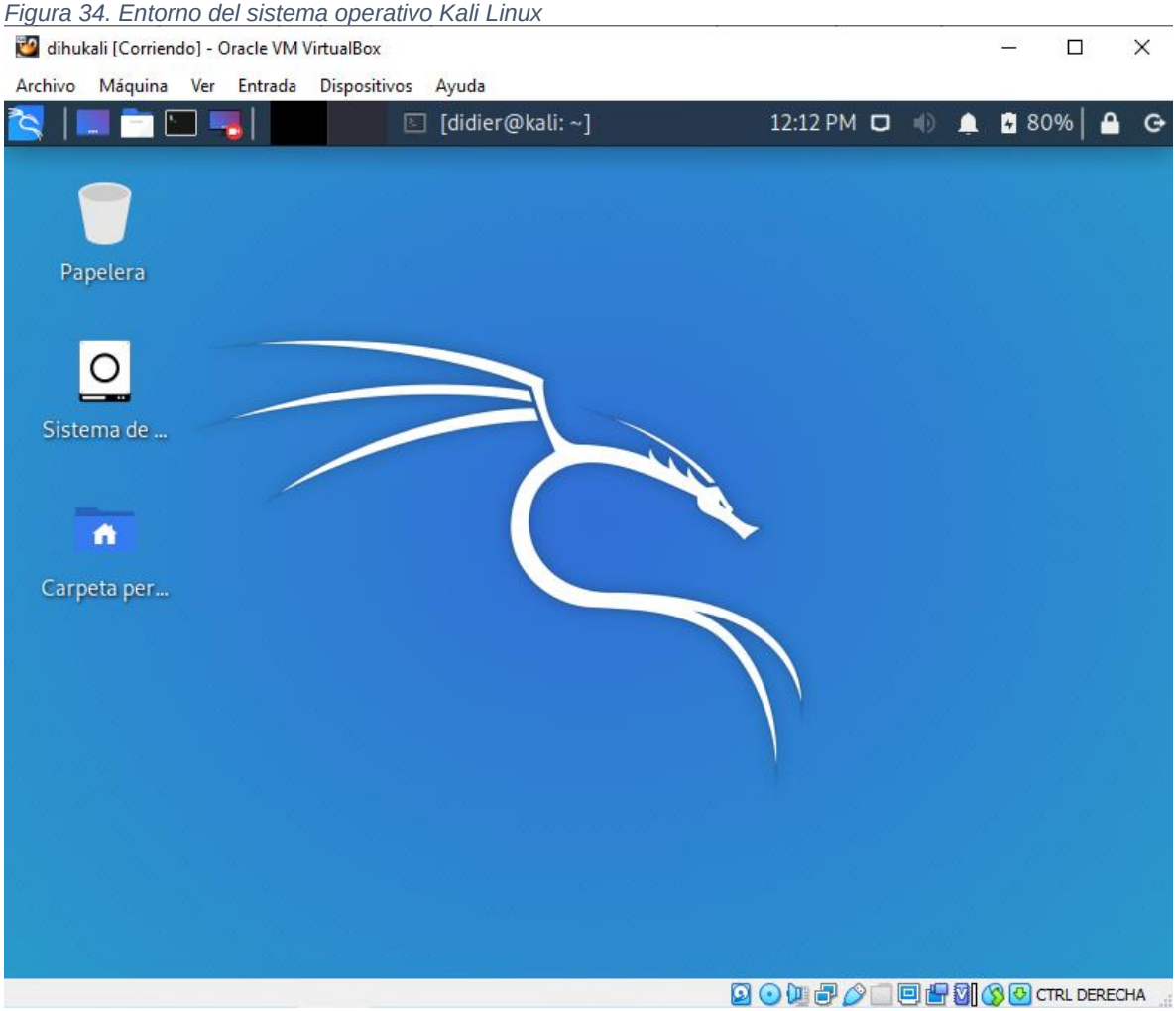
Para la prueba seguridad se usa el software Kali Linux, es de código abierto y es un importante referente para la auditoria de redes entre ellas, la seguridad de redes wi-

[86] NETWORKWORLD. Principales amenazas para la seguridad de las redes inalámbricas. [En línea] [Citado el: 27 de 07 de 2020.]. Disponible en:https://www.networkworld.es/seguridad/principales-amenazas-para-la-seguridad-de-las-redes-inalambricas.

fi. Este software cuenta con la suite aircrack-ng que proporciona lo necesario para crackear redes inalámbricas con protocolo WEP, e incluso WAP y WAP2, en la Figura 29 se aprecia como es el entorno gráfico de este software:

Entorno Kali Linux:

Figura 34. Entorno del sistema operativo Kali Linux

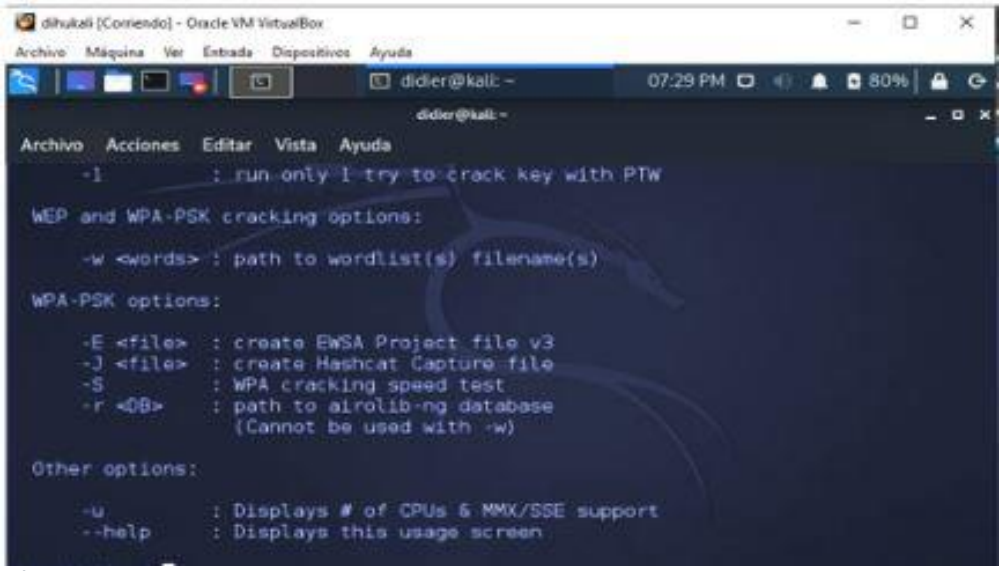


Fuente: el autor.

Por medio Kali Linux se vulnera la red inalámbrica, un método muy utilizado por los ciberdelincuentes es el llamado ataque por diccionario, el cual consiste en averiguar una contraseña por medio de la validación de todas las palabras de un diccionario, la efectividad de éste método aumenta cuando en la contraseña de la rede se utiliza una contraseña débil, en las Figuras 30 y 31 se muestra cómo se rompe la contraseña con la herramienta Aircrack, se rompió la contraseña en tan solo un

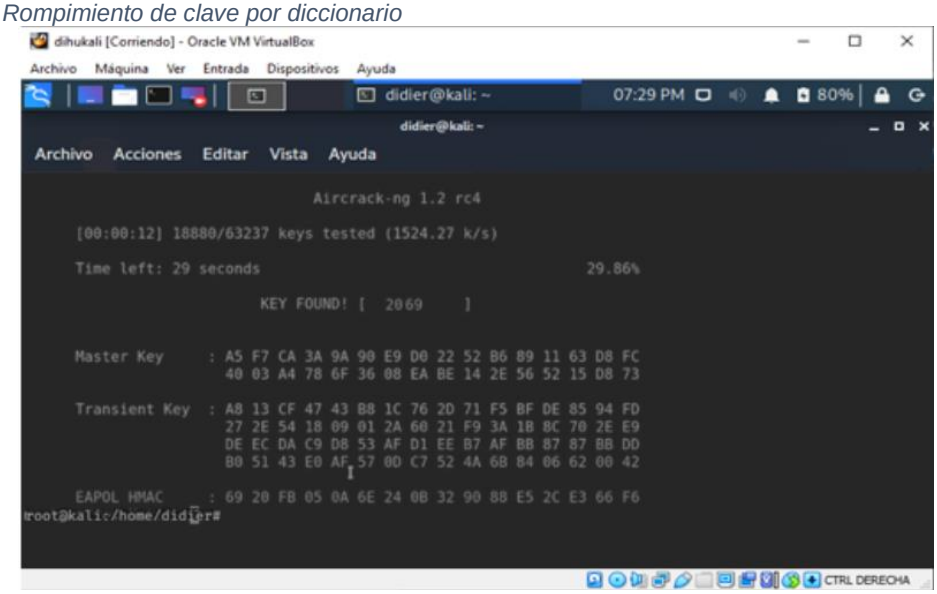
lapso de 29 segundos e indica cual es la contraseña de la red (2069), una contraseña muy débil, utilizada por muchos usuarios por la facilidad de recordación:

Figura 35. Proceso de vulneración de la red WiFi



Fuente: el autor.

Figura 36. Rompimiento de clave por diccionario



Fuente: el autor

Para esto se utiliza Kali Linux, instalado sobre el software de virtualización VirtualBox, mediante la herramienta aircrack-ng se logra el descifrado de claves, dentro de las cuales se encuentra WEB y WPA/ WPA2-PSK.

7.3.1.3 Factor Humano

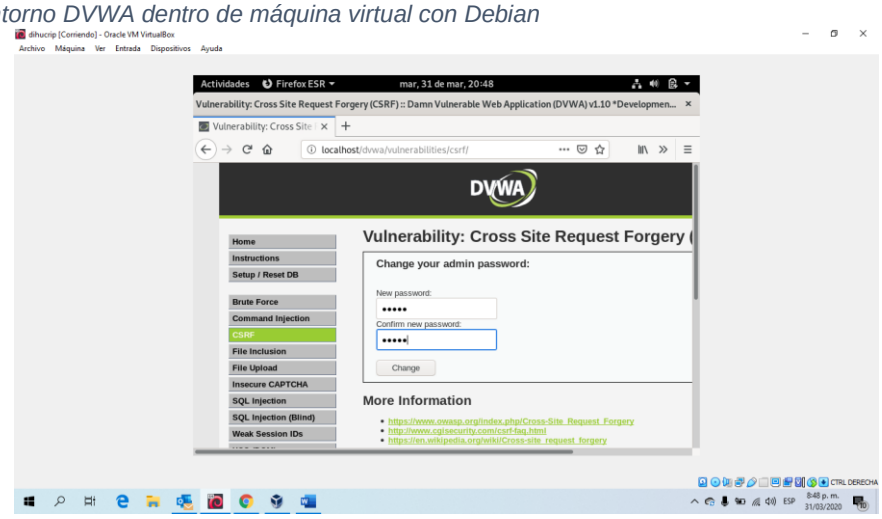
Los ataques más comunes se realizan aprovechando el factor humano, el desconocimiento de los usuarios en los temas de seguridad informática es de conocimiento de los ciberdelincuentes y no dudan en aprovechar este factor para causar daño.

De aquí la importancia de tener el conocimiento necesario para evitar caer en trampas de este tipo.

Para explotar esta vulnerabilidad se usa DVWA, que se utiliza como prueba de aplicación del usuario. Mediante la cual se puede lograr que el usuario no pueda ingresar a la aplicación por perdida de autenticación es decir el usuario perderá su contraseña de ingreso a la aplicación.

Para esta vulnerabilidad, se usa esta página (DVWA) como se ve en la Figura 32, la cual representa una aplicación web, en un caso real pudiera ser cualquier página donde el usuario ingrese con su nombre de usuario y contraseña personal, puede ser una página donde realice operaciones, consultas, contenga información personal etc.:

Figura 37. Entorno DVWA dentro de máquina virtual con Debian

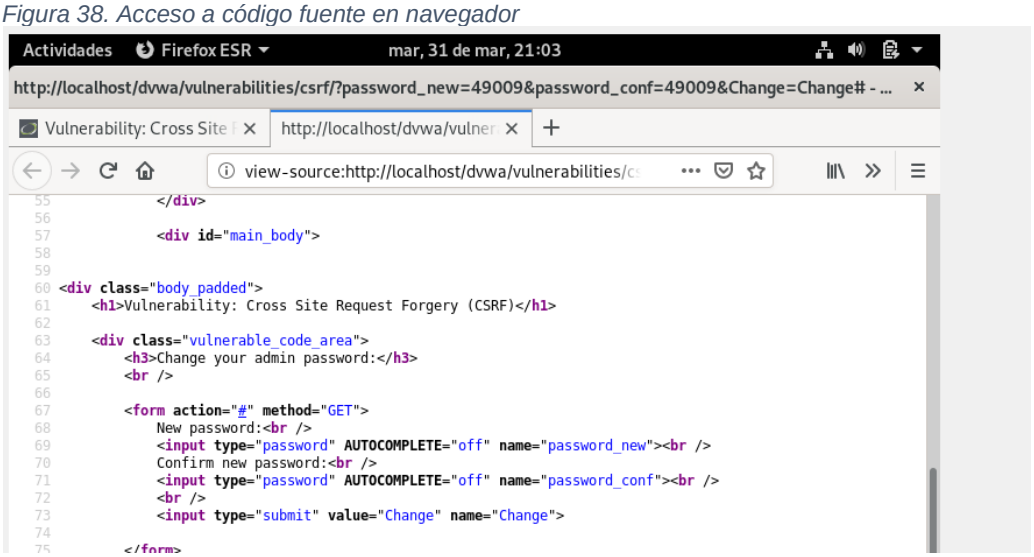


Fuente: el autor

A continuación se toma el código fuente para obtener información que sirve para crear el acceso a una página que hace un reset en la contraeña del usuario, acceder al ccódigo fuente de una página web es una opción con la que se cuenta en los

navegadores y cuenta con información que puede ser aporvechada por un ciberdelincuente, simplemente con modificar algunas líneas se puede lograr el cometido tal como lo muestra la Figura 33:

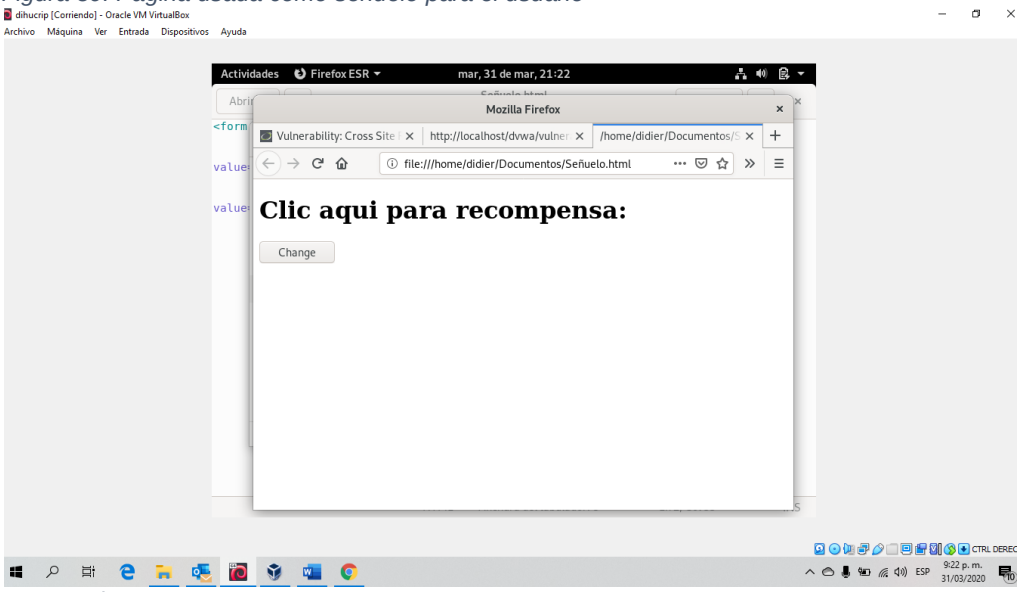
Figura 38. Acceso a código fuente en navegador



Fuente: Elaborador por el autor

Esta página es un señuelo que puede llegar al usuario por medio de correo electrónico, por medio de un mensaje con un link se le pide que ingrese a la página que promete una recompensa, y al dar clic allí el usuario perderá su contraseña de ingreso a la aplicación.

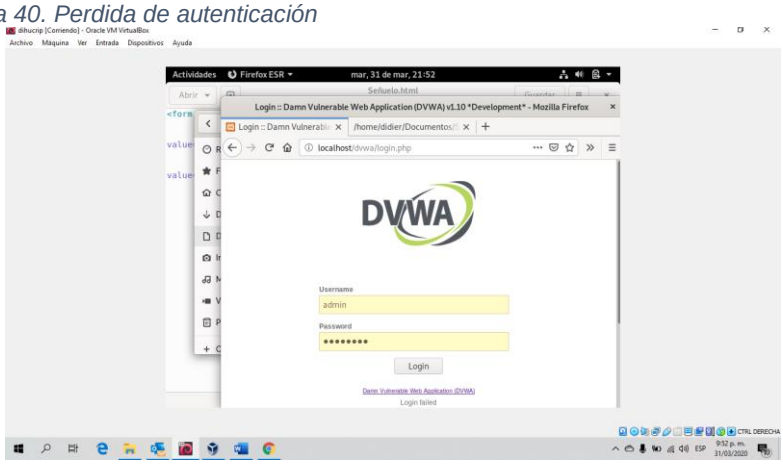
Figura 39. Página usada como señuelo para el usuario



Fuente: El autor

En la siguiente imagen se muestra como al Intentar ingresar con la contraseña el usuario ya no puede ingresar, esto se conoce como pérdida de autenticación, junto a técnicas como ingeniería social un usuario de red doméstica puede caer en una elaborada trampa.

Figura 40. Perdida de autenticación

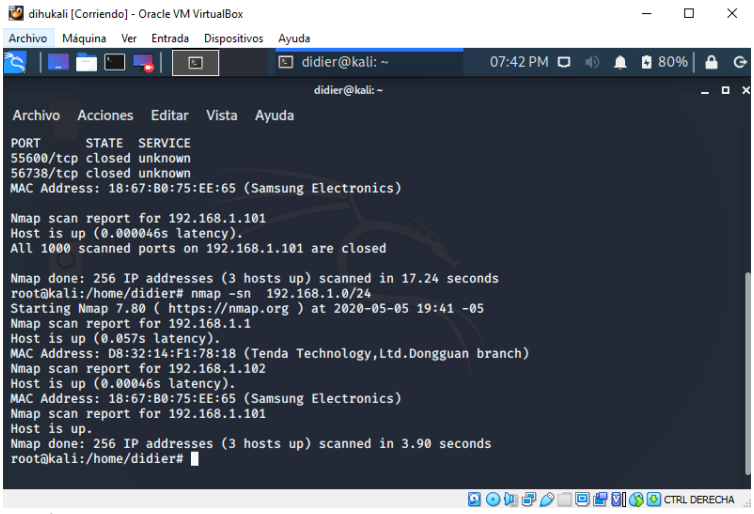


Fuente: Elaborado por el autor

7.3.1.4 Escaneo de vulnerabilidades

Escaneo de puertos: Por medio de la herramienta nmap se visualiza los equipos activos en la red doméstica. Nmap es una herramienta de software libre aplicado en la seguridad de redes, tiene la capacidad de detectar hosts y puertos abiertos, así como servicios y aplicaciones que se encuentren dentro de los mismos. En la Figura 36 se muestra el escaneo realizado, el cual contiene información donde se puede ver que hay tres equipos conectados a la red doméstica, se puede ver incluso la marca de los equipos y la dirección física de cada uno de ellos:

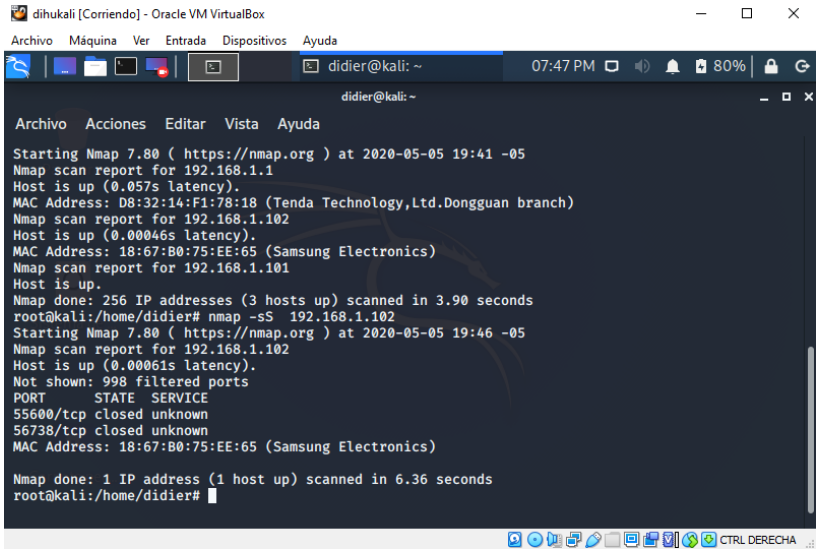
Figura 41. Escaneo de puertos con nmap



Fuente: El autor.

La herramienta permite ver también los puertos abiertos en los dispositivos de la red, en la Figura 37. se hace un escaneo de puertos y muestra la información de los puertos y el estado de estos, los puertos son como puertas que permiten la entrada y salida de mensajes entre hosts, lo más seguro es que los puertos que no se usan este cerrados.

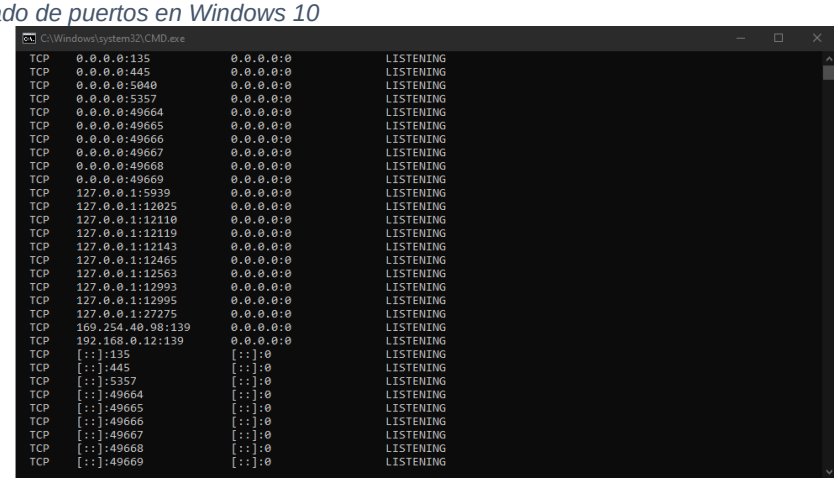
Figura 42. Nmap escaneando puertos y servicios



Fuente: El autor.

Es posible identificar los puertos que están abiertos, mediante las herramientas de netita de Windows, en la Figura 39 se puede ver una lista de los puertos que se encuentran abiertos escuchando para recibir alguna conexión, hay puertos especialmente peligrosos si están abiertos y no se usan adecuadamente, por ejemplo, el puerto 135 se encuentra en estado LISTENING (Figura 39) es decir escuchando, por este puerto puede entrar alguna conexión:

Figura 43. Listado de puertos en Windows 10



Fuente: El autor

7.4 ANÁLISIS DE LAS VULNERABILIDADES ENCONTRADAS

Luego de realizar las pruebas para identificar vulnerabilidades, se encuentra lo siguiente:

7.4.1 Debilidad en contraseñas

No se establece una contraseña segura, no tiene un mínimo de al menos 6 caracteres, no contiene combinación de mayúsculas y minúsculas.

Esta es una de las vulnerabilidades más comunes en redes domésticas, la mayoría de los usuarios suele usar contraseñas débiles principalmente por motivos como la facilidad de recordar la contraseña o por el desconocimiento de lo fácil que puede ser para los ciberdelincuentes romper una contraseña.

Una de las causas es la cantidad de contraseñas que se debe usar diariamente como usuario de la red, dado que cada vez que se navega por internet o se usa aplicaciones se debe logear y se tiene a dejar la misma para todos estos login, además que sea muy fácil de recordar para mecanizar y facilitar esta tediosa tarea.

Por esta razón las contraseñas se convierten en un punto vulnerable de seguridad informática, lo que requiere ser mitigado para mantener a salvo las cuentas y la información que contienen, es importante tener presente que si bien es un esfuerzo el correcto manejo de contraseñas; es poco en comparación con lo que representa esta vulnerabilidad.

La contraseña más débil es como: 1234, 12345678, password, qwer, asdf, por referenciar algunas, esto no representa reto alguno para los ciberdelincuentes, y no es necesario ser un experimentado para romper una de estas contraseñas en solo unos segundos, por lo que esta son las primeras en la lista de los criminales.[87]

[87] OSI. osi.es. Sabias que el 90 de las contraseñas son vulnerables? [En línea] [05 de 08 de 2020.] Disponible en: https://www.osi.es/es/actualidad/blog/2019/02/06/sabias-que-el-90-de-las-contrasenas-son-vulnerables.

7.4.2 Tráfico inusual dentro de la red

Se encuentra protocolos dentro de la red que son inusuales, protocolos de conexión p2p el cual permite compartir archivos entre varios ordenadores y se considera una fuente importante de malware.

El monitoreo de red es un importante porque es como la columna vertebral de las comunicaciones modernas. El monitoreo de la red permite identificar todo lo que está presente en la red, lo que incluye en una red doméstica routers, computadores de mesa, equipos portátiles, dispositivos móviles como celulares y tablets, impresoras, Smart tv, entre otros. Los mapas de red permiten una visualización global de la red. Mediante el monitoreo de red se puede llevar el registro del consumo de recursos y el rendimiento de esta.

Actualmente el trabajo remoto es una forma habitual de usar la red doméstica, y esto representa más que tener una conexión a internet sin más, el acceso a los recursos de la empresa se realiza mediante el trabajo remoto, usando servicios como teleconferencias que requieren baja latencia y estabilidad en la conexión.

Debido a la pandemia del Covid-19 muchas empresas han enviado sus colaboradores a trabajar desde casa, y las redes domésticas no se encuentran bien configuradas para trabajar de esta forma, si no se tiene un router bien configurado se pueden presentar problemas.[88]

Conexión de equipos fuera de la red: En ocasiones se encuentran dispositivos conectados a red si tener plena identificación de estos, lo que indica pudiese llegar a ser intrusos en la red.

Protocolos de comunicación como BitTorrent permite compartir archivos a través de la red, mediante el uso de herramientas de monitoreo de red como Whireshark, software libre, se puede identificar este tipo de protocolos. Este protocolo es utilizado por algunos tipos de adware y ransomware para transitar por la red. Uno de estos el conocido como TorrentLocker, el cual apareció en 2014 y se creó para actuar contra equipos con Windows capturando y encriptando archivos de la víctima.

[88] VELASCO, Ruben. Redes Zone. Controla el tráfico de tu red local con Network Meter. [En línea]. [06 de 08 de 2020.] Disponible en: https://www.redeszone.net/2017/01/03/controla-trafico-red-local-network-meter/.

En 2015, el cliente u Torrent, cliente de BitTorrent, sufrió el denuncio de varios usuarios que refieren que el programa sin previo aviso instala un programa potencialmente no deseado conocidos como PUP. Específicamente el programa que se instala es EpicScale, un programa de minería de bitcoins, el cual llega a consumir una gran cantidad de recursos del sistema.[89]

7.4.3 Factor humano

Los ciberdelincuentes saben que uno de los puntos débiles de la seguridad de las redes es precisamente el componente humano. Los errores que cometen los usuarios son la principal causa de las infracciones de datos, lo que conlleva a que el ataque al factor humano pueda ser vulnerado incluso en los sistemas de seguridad más complejos.

Los ataques de ingeniería social y phishing pueden conllevar a perder credenciales de usuario, y son los métodos más comunes de acceso a información privada y sensible. Hay distintas causas por las que el ser humano es el principal factor de vulnerabilidad: la percepción del valor de la información, los mitos de seguridad, la sensibilización, la actitud y los comportamientos por mencionar algunos.[90]

La ingeniería social se basa en una premisa básica: es más fácil manejar a las personas que a las máquinas. Para lo cual se utilizan técnicas psicológicas de manipulación con el ánimo de conseguir que las personas revelen información confidencial.

El medio de propagación para los ataques de ingeniería social es el correo electrónico ya que es un medio usado por muchas personas en el ámbito laboral y del hogar, además se apoyan en otros medios como llamadas telefónicas, mensajes de texto, aplicaciones de mensajería, redes sociales. Etc.

Los correos enviados en la ingeniería social son phishing, estos correos intentan tiene el propósito de convencer al usuario de que su origen es legítimo, pero tienen la intención de sacar información a la víctima., por otra parte, estos correos suelen

[89]PANDA. Panda Security.com. Que es bittorrent. [En línea] [06 de Agosto de 2020.] Disponible en: https://www.pandasecurity.com/es/security-info/bittorrent/.

[90] BURZTEIN, Sara. magazitum. Factor humano: El talón de Auiles de la Seguridad . [En línea] . [06 de Agosto de 2020.] Disponible en: https://www.magazcitum.com.mx/?p=2735#.XyyhWShKjIU.

tener archivos adjuntos con virus que pueden ir junto a contenido que parece inofensivo como puede ser videos divertidos o tiernos.

También, es común que se combinen técnicas y se haga ingeniería social en sitios públicos, donde el delincuente puede mirar por encima del hombro el computador y capturar información, de esta forma pueden conseguir nombres de usuario y contraseñas.

Ataques por medio de establecer comunicación con la víctima son usuales, el atacante puede persuadir o incluso presionar para tener acceso a la red con la excusa de tener que solucionar algún problema, se usa las emociones de las personas para convencerlas de cooperar y con ello caer en la trampa.

Cualquier dato es aprovechado por los delincuentes puede ser tan sencillo como un nombre, una fecha de nacimiento o una dirección los hackers pueden acceder a la red pasando desapercibidos. Con esto se pueden abrir camino a través del sistema y el resultado es pérdida y secuestro de información, infección del sistema con malware, rootkits, troyanos y bots. [91]

7.4.4 Puertos abiertos:

Los puertos se abren por el uso de aplicaciones, los puertos se cierra cuando se cierran los programas usados, en realidad no es necesario cerrar puertos de manera manual ya que son necesarios para la comunicación, sin embargo si hay puertos que son especialmente peligroso y representan una vulnerabilidad, el puerto 135 es compartido por servicios DCOM y MSDTC siendo estos servicios de Microsoft para comunicaciones, el bloque de puertos lo realiza el cortafuegos pero en caso de no hacerlo cualquier atacante puede aprovechar la vulnerabilidad.

La recomendación de Microsoft es bloquear los puertos TCP/IP que no se utilicen, recomendando el bloque de los puertos 135, 139,445, 593 o cualquiera otro puerto relacionado con el protocolo RCP. Se afirma que RCP sobre TCP no está diseñado para usar sobre el entorno de internet dada la hostilidad y el peligro que se encuentra en la esta red, otro protocolo más seguro en este caso es RCP sobre HTTP.

[91] KASPERSKY. Ingeniería social: definición. [En línea] [07 de Agosto de 2020.] Dispoinble en: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering.

El puerto 135 puede recibir repetidas llamadas y causar la sobrecarga de la computadora, lo que sería un ataque de denegación del servicio, uno de los virus que puede realizar esto fue el virus Blaster.

El virus Blaster es conocido también como Lovsan o Lovesn 3a1, es del tipo gusano y aprovecha la vulnerabilidad del servicio DCOM en Windows, y puede infectar varios sistemas, cuando se presentó es incidente fue necesario que Microsoft apagara sus servidores para minimizar el efecto dañino.

Los efectos de este virus generan inestabilidad en el sistema, y puede ser posible también que aparezcan avisos dentro del sistema indicando el reinicio de este.

De esta experiencia se aprendió la importancia de usar el Firewall.[92]

[92] BURGOS, Alexis. Seguridad PC. Buenos Aires. Ed. Fox Andina. 2010. 192 p ISBN 978-987-663-031-3.

8. FASE 3. MANUAL DE BUENAS PRÁCTICAS PARA EL USUARIO DE RED DOMESTICA

El manual de buenas prácticas para el usuario de red doméstica es resultado del trabajo realizado en fases anteriores y está diseñado teniendo en cuenta conceptos básicos de seguridad informática. Es una guía que permite de forma práctica conocer la forma de hacer uso adecuado de la red doméstica, así como su configuración y cuidados relacionados al tema de la seguridad informática.

El usuario final de este manual es la persona que día a día usa recursos informáticos en red desde la comodidad de su hogar, son personas que generalmente no tiene conocimientos amplios sobre estos temas, por lo que, pensando en esto, el contenido del manual contiene un lenguaje sencillo, consejos acompañados con imágenes ilustrativas que facilitan la comprensión del lector.

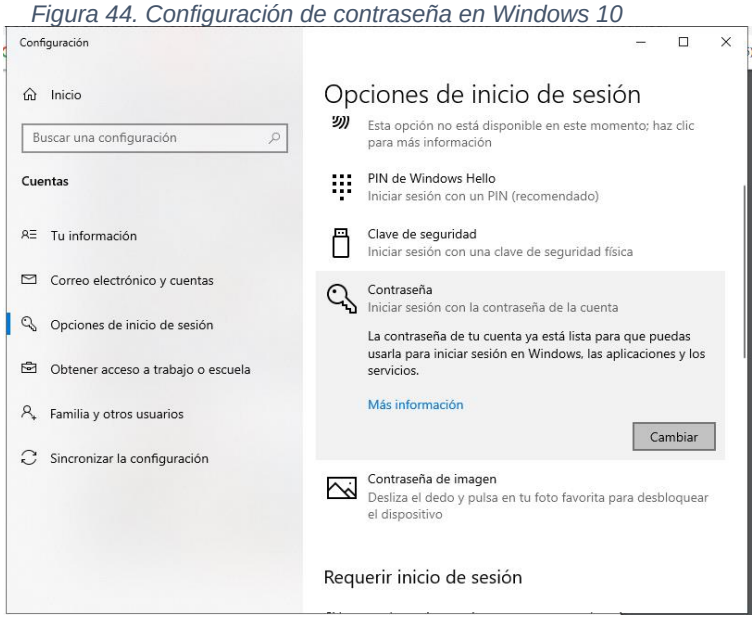
Con este fin, el manual la estructura del manual inicia con una explicación del ítem a tratar con lo cual el usuario podrá conocer el tema de forma general y le prepara para poder aplicar configuraciones de seguridad. Las configuraciones se acompañan de imágenes que permiten la mejor comprensión de cada apartado, considerando que con este apoyo visual el usuario puede sentirse motivado a seguir los pasos que le permitan realizar una configuración de seguridad dentro de su propia red doméstica.

El software que se utiliza para las configuraciones siguientes corresponden a programas de uso gratuito y se utiliza para fines didácticos, en el caso que el usuario tenga la posibilidad de adquirir software licenciado o de pago también es recomendado usarlo ya que se puede aprovechar funcionalidades adicionales y soporte de las aplicaciones, los programas escogidos para este ejercicio no obedecen a algún interés particular o especial.

8.1 ESTABLECER CONTRASEÑAS:

Es importante colocar una contraseña segura, mínimo de 6 caracteres, pero lo ideal es que sea de 8 o más, usando números, mayúsculas y minúsculas. Se puede realizar mediante del panel de control del sistema.

Figura 44. Configuración de contraseña en Windows 10

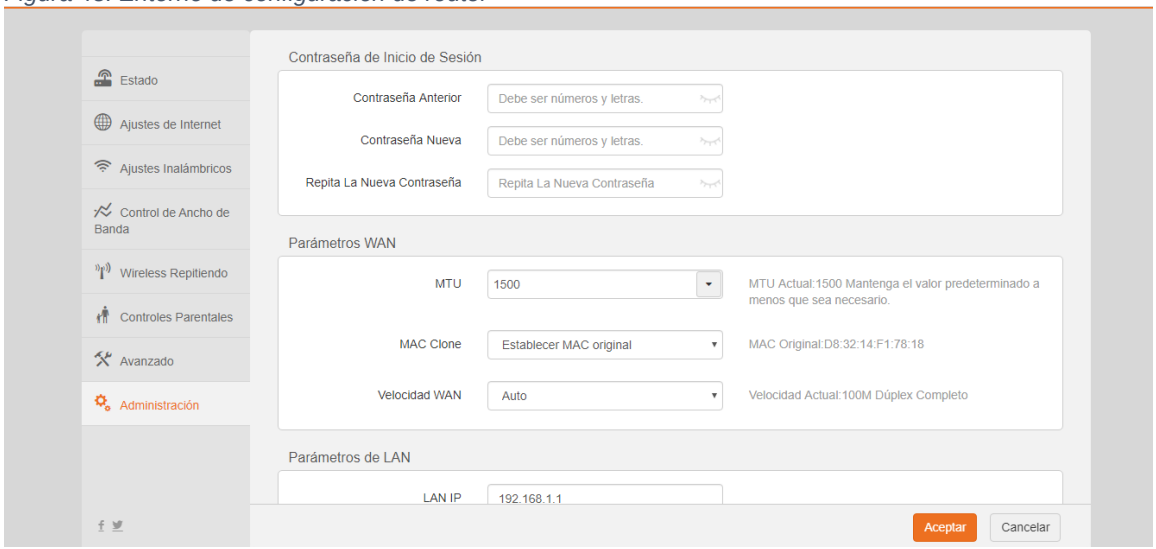


Fuente: el autor.

Para cambiar la contraseña de acceso a red Wi-Fi se ingresa al router a través del ingreso por la barra de direcciones del navegador con dirección 192.168.0.1

8.2 ACCESO A LA RED POR MAC

Figura 45. Entorno de configuración de router



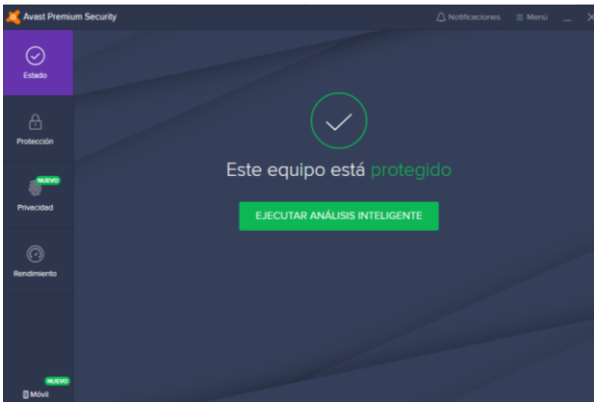
Fuente: el autor

.

8.3 ANTIVIRUS

El uso de antivirus protege el equipo de ataque como malware, troyanos, gusanos y virus en general, conviene instalarlo y configurarlo para ofrecer protección a la red. Es posible encontrar antivirus de uso gratuito y que ofrecen protección básica pero suficiente para el uso en el hogar, no obstante, se recomienda la compra de software antivirus licenciado. Para la representación de este punto se toma Avast antivirus sin obedecer a interés particular alguno:

Figura 46. Entorno de Software Antivirus

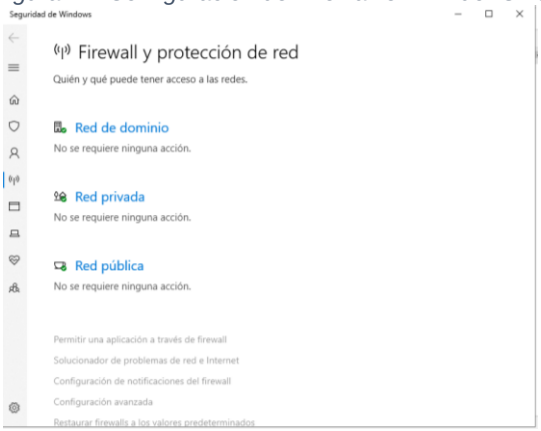


Fuente: el autor

8.4 CORTAFUEGOS

El sistema Windows trae un sistema de Firewall o cortafuegos que permite proteger el equipo de ataques externos, se puede configurar de acuerdo con la necesidad. Se ingresa a través del panel de control. La importancia de la configuración del cortafuegos para Windows quedó expuesta en la vulnerabilidad de puertos abiertos de la fase anterior.

Figura 47. Configuración de Firewall en Windows 10



Fuente: el autor

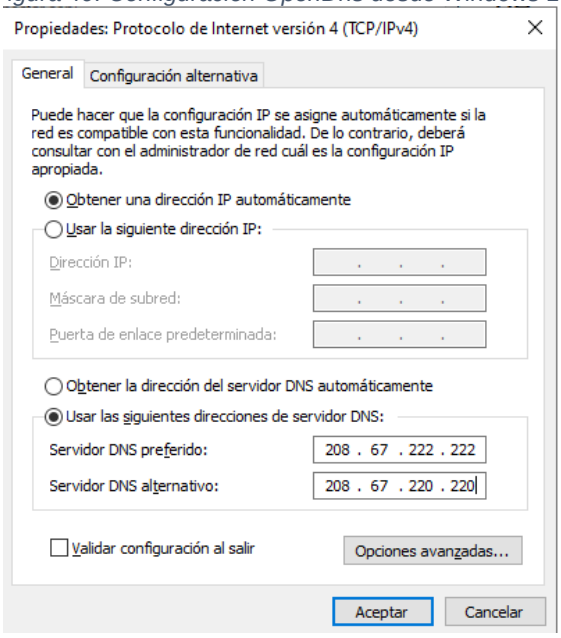
8.5 PROTECCIÓN CONTRA SPOOFING

Para proteger el sistema del spoofing se recomienda usar los dns de OpenDOS, esta es una empresa que ofrece el servicio de resolución de nombres de dominio de forma gratuita. Para esto se puede ingresar a la configuración del router o también en la configuración de red del equipo ingresando como dns primario 208.67.222.222 y dns secundario 208.67.220.220.

Figura 48. Configuración OpenDOS desde el router

Fuente: el autor

Figura 49. Configuración OpenDns desde Windows 10



Fuente: el autor.

8.6 ACTUALIZACIÓN DEL SISTEMA

Para proteger el sistema de malware es importante mantener actualizado el sistema mediante Windows update, aplicación a la cual se llega mediante el panel de control.

Figura 50. Windows 10 actualizando

Fuente: el autor.

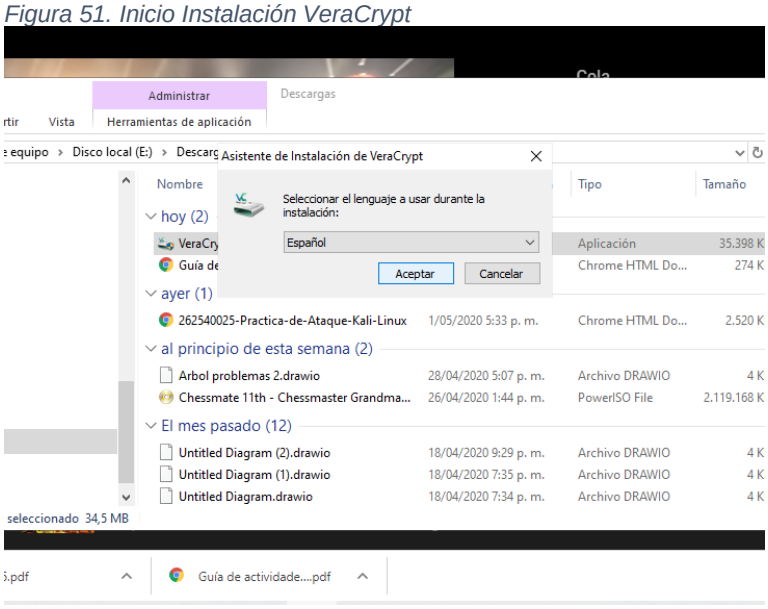
8.7 CIFRAR INFORMACIÓN

Uno de los puntos más importantes dentro de la seguridad informática es el resguardo de la información que se tiene dentro del equipo. Para esto se cuenta con herramientas especializadas en el cifrado de las unidades del equipo, por ejemplo, el software Veracrypt permite cifrar la unidad de disco duro entre otras.

8.7.1 Instalación y cifrado de disco con Veracrypt

Se descarga el software de la página oficial y empieza la instalación. Se selecciona el lenguaje:

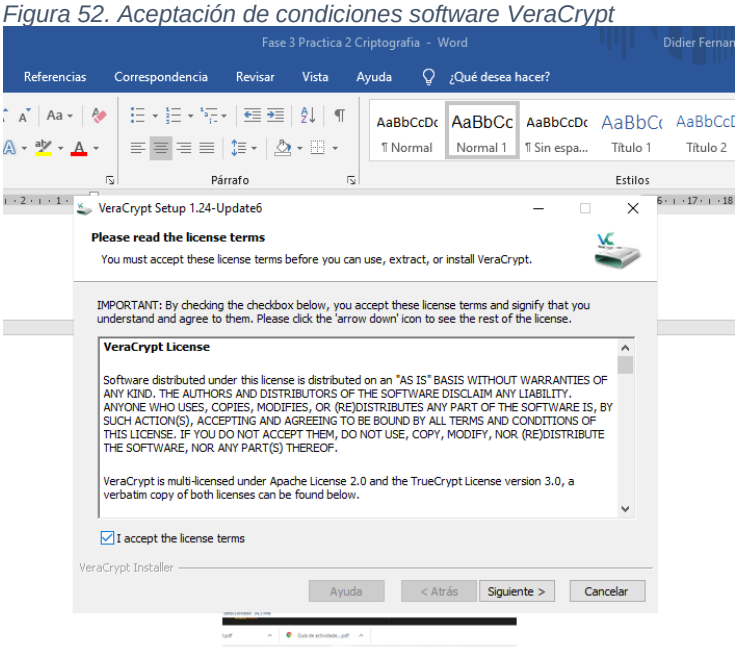
Figura 51. Inicio Instalación VeraCrypt



Fuente: el autor

Se acepta condiciones de uso del software:

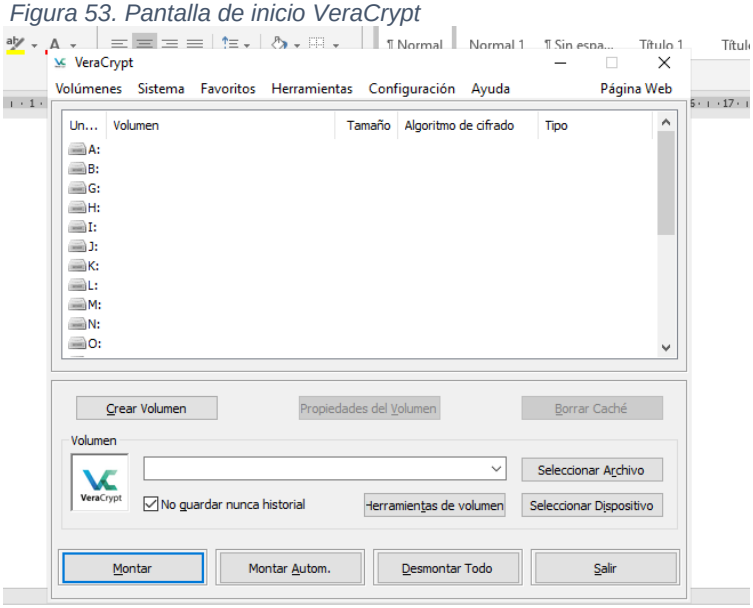
Figura 52. Aceptación de condiciones software VeraCrypt



Fuente: el autor

Inicio de la aplicación:

Figura 53. Pantalla de inicio VeraCrypt



Fuente: el autor

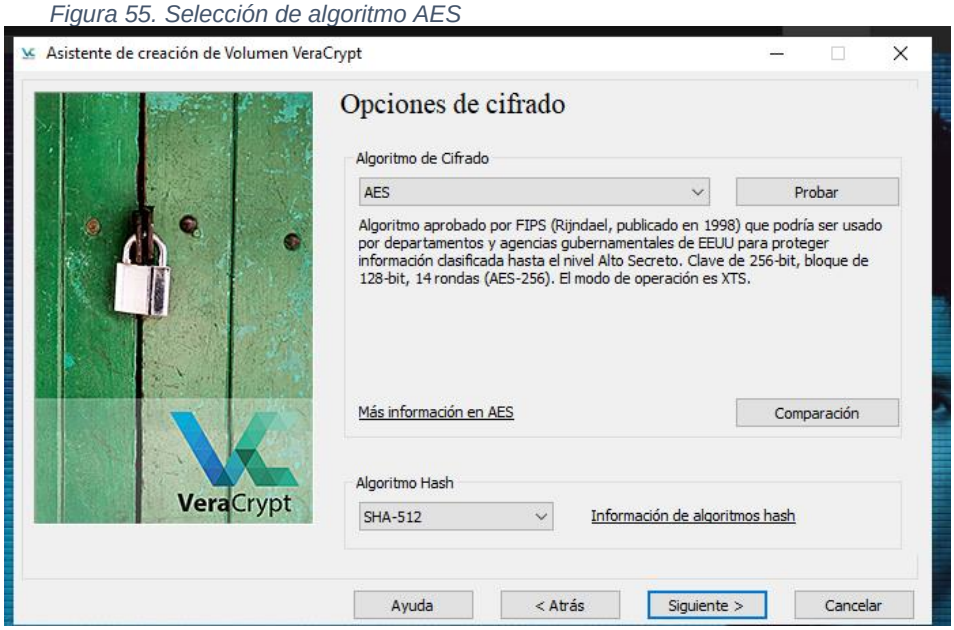
Se selecciona crear volumen:

Figura 54. Crear volumen en VeraCrypt

Fuente: el autor

Selección algoritmo AES:

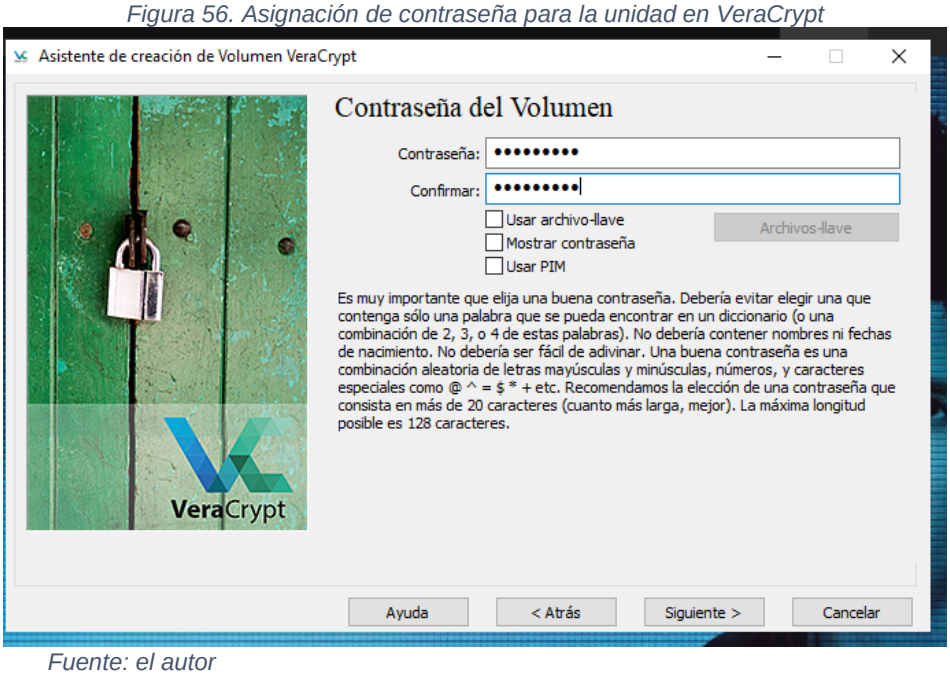
Figura 55. Selección de algoritmo AES



Fuente: el autor

Asignación de contraseña:

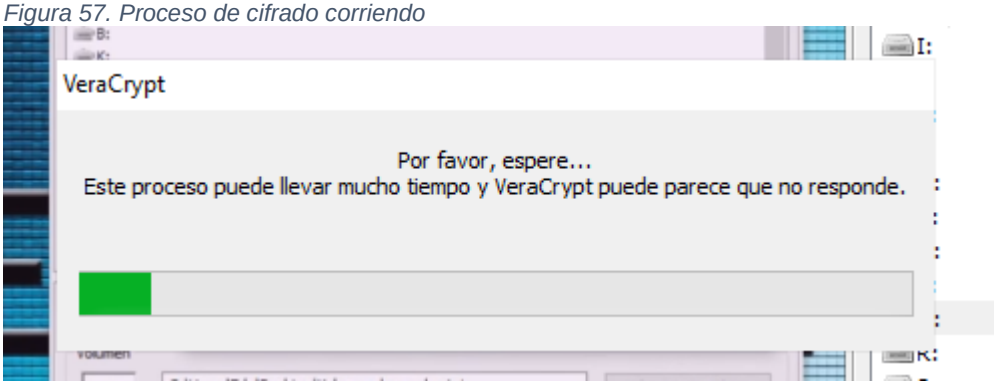
Figura 56. Asignación de contraseña para la unidad en VeraCrypt



Fuente: el autor

Montaje de la unidad:

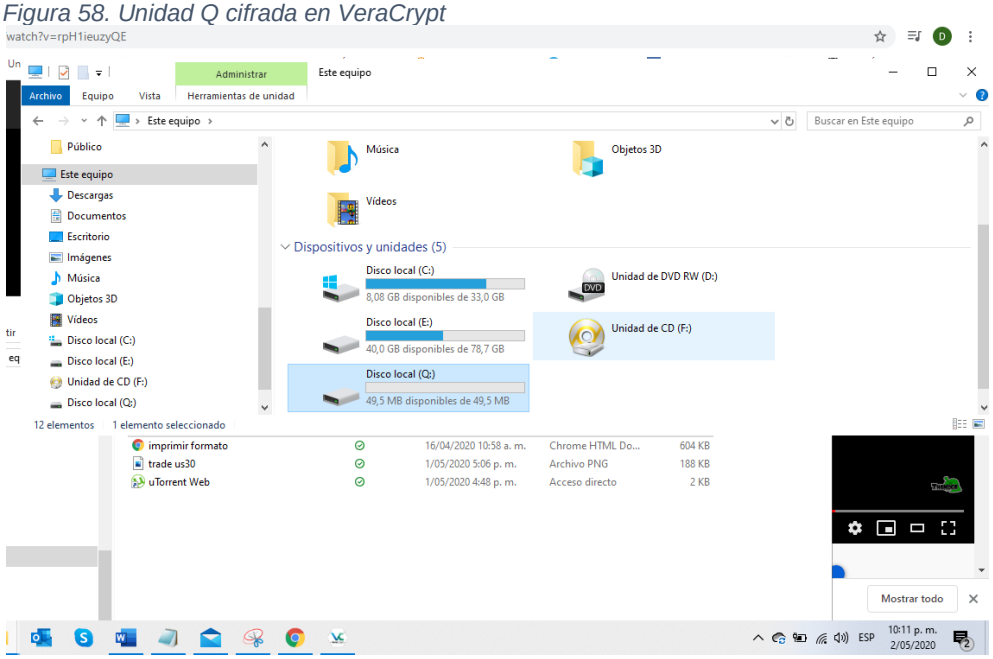
Figura 57. Proceso de cifrado corriendo



Fuente: el autor

Se ha creado el volumen Q para guardar los archivos de forma segura:

Figura 58. Unidad Q cifrada en VeraCrypt



Fuente: el autor

8.8 VPN

Una red vpn (red privada virtual) crea un túnel entre el dispositivo usado y el servidor, con la ventaja que la información que por allí transita va codificada, esto

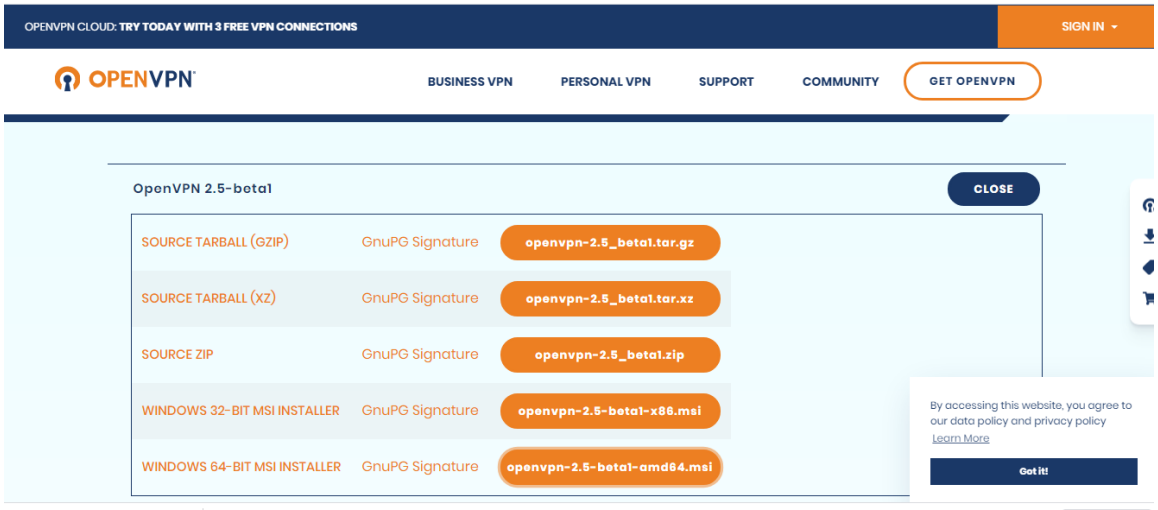
significa que, aunque sea capturada información no puede ser legible por estar codificada.

Como alternativas para implementar esta solución de seguridad se cuenta con software de uso libre como lo es Openvpn de Linux.

Este servicio de vpn ofrece conectividad de muy buenas prestaciones en redes wi-fi, como ventaja tiene la simplificación de la conexión vpn con el objetivo de hacerlo más accesible a personas que no cuentan con grandes conocimientos en informática.

Entre tantas opciones de configuración y uso de red vpn, a continuación, se ofrece la configuración de vpn con Openvpn:
Lo primero es descargar la aplicación cliente de OpenVpn disponible en la página oficial https://openvpn.net/community-downloads/:

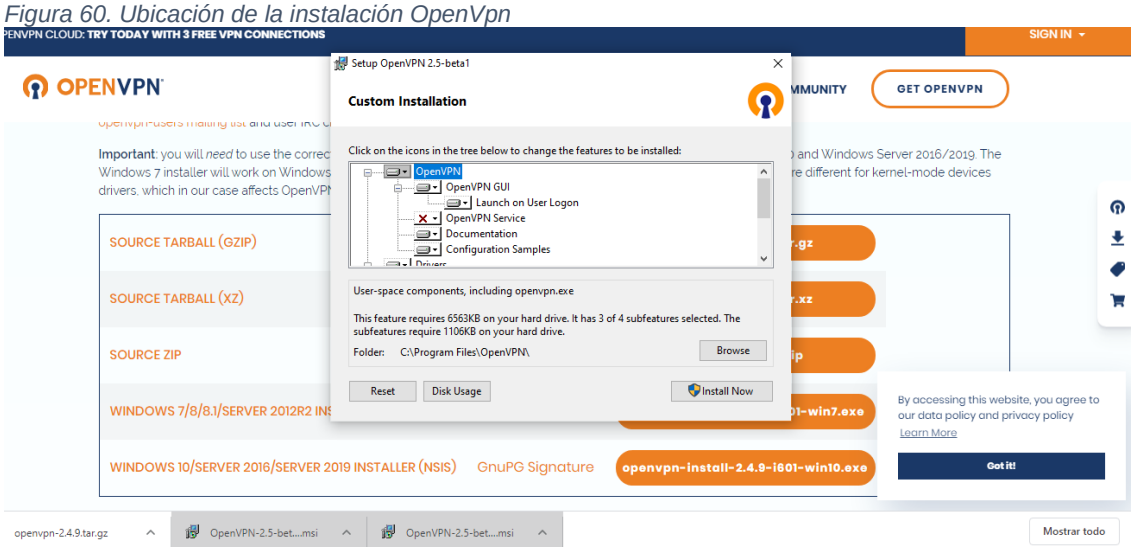
Figura 59. Página Oficial de OpenVpn



Fuente: Elaborado por el autor

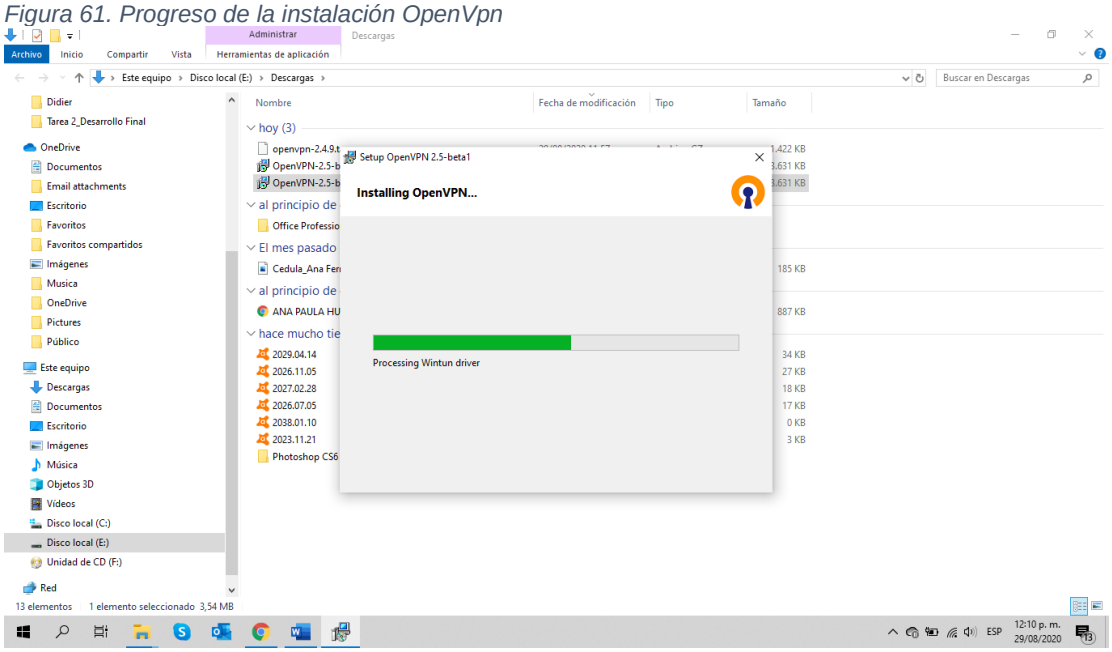
Al descargar el archivo de instalación, se ejecuta y se selecciona la ubicación donde se instala:

Figura 60. Ubicación de la instalación OpenVpn



Fuente: Elaborado por el autor

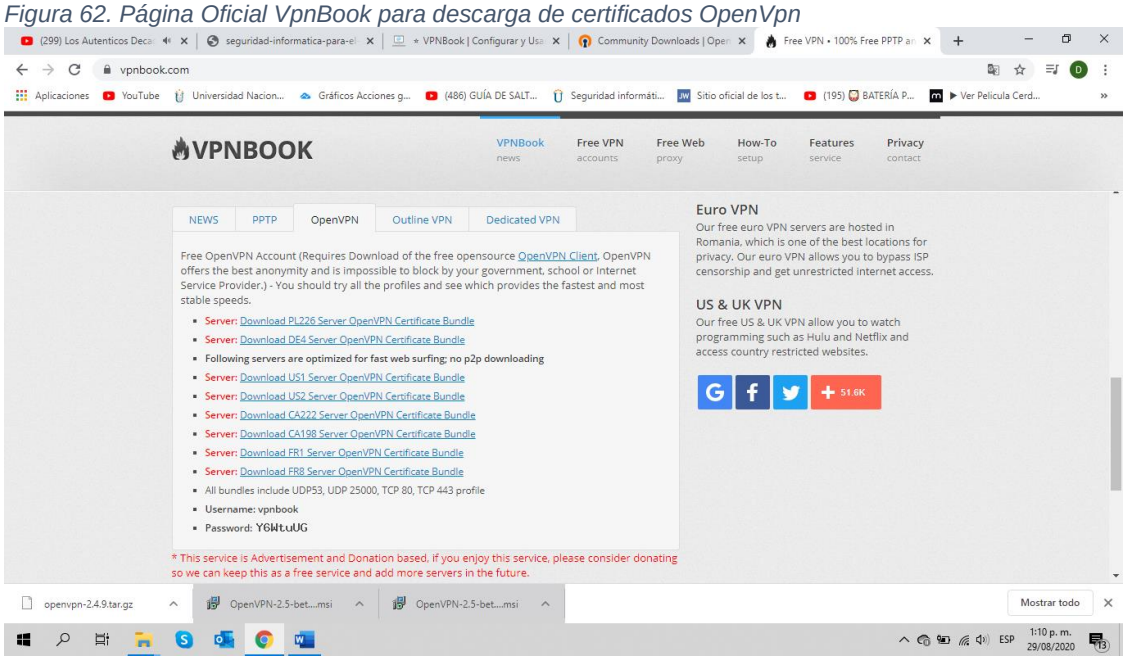
Figura 61. Progreso de la instalación OpenVpn



Fuente: Elaborado por el autor

Una vez instalado el cliente, se debe descargar los ceritificados de la página vpnbook:

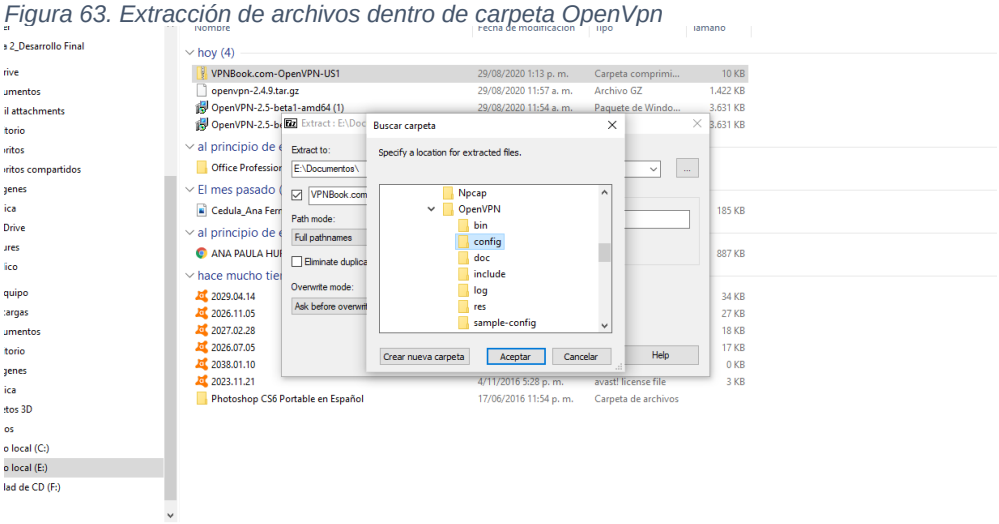
Figura 62. Página Oficial VpnBook para descarga de certificados OpenVpn



Fuente: Elaborado por el autor

Una vez se ha descargado el paquete de certificados en formato .zip se debe extraer en la carpeta de instalación de openvnp, a continuación, se muestra la ubicación:

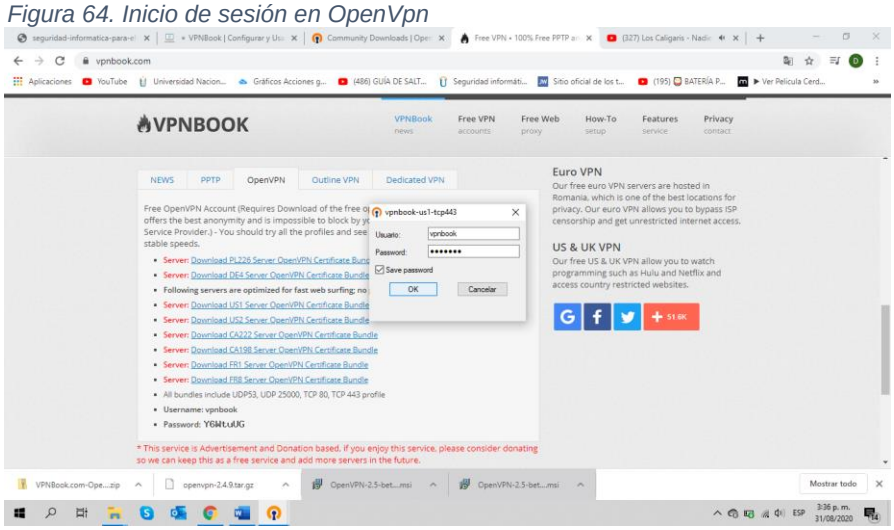
Figura 63. Extracción de archivos dentro de carpeta OpenVpn



Fuente: Elaborado por el autor

El siguiente paso es abrir la aplicación OpenVpn, lo que se puede realizar desde el menú de inicio, y al ejecutarla pide usuario y contraseña, datos que se encuentra en la misma página de vpnbook

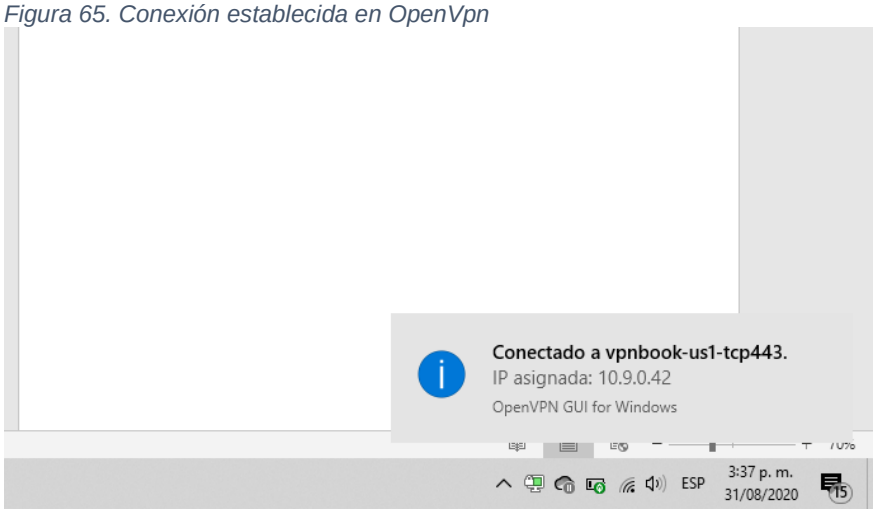
Figura 64. Inicio de sesión en OpenVpn



Fuente: Elaborado por el autor

Al conectarse a la vpn se presenta una notificación en sesión Windows que permite advertir que se está conectado a vpn, lo que significa que ahora los datos que se transmiten están protegidos:

Figura 65. Conexión establecida en OpenVpn



Fuente: El autor

9. RECOMENDACIONES DE SEGURIDAD INFORMÁTICA EN REDES DOMÉSTICAS

9.1 IMPORTANCIA DE LA SEGURIDAD EN REDES

Con el crecimiento de las redes, crece también el riesgo de que estas sean utilizadas de forma inapropiada o sin autorización, la seguridad en redes se encarga de velar por los pilares de la seguridad de la información: confidencialidad, disponibilidad e integridad de la información de los peligros que pueden existir en la red tales como virus, spam, gusanos, troyanos, ataques etc.

Actualmente la seguridad de la información va más allá de usar un antivirus, ya que con los sofisticados ataques actuales es difícil que solo el antivirus logre prevenir los ataques a los sistemas informáticos, porque ahora es necesario tomar otras medidas de seguridad que involucran no solo al encargado de la seguridad sino a varias partes que deben tener en cuenta detalles como no revelar información por internet, cambiar contraseñas, tener cuidado con los correos electrónicos, mantener actualizaciones y otras.

Las vías para atacar los sistemas informáticos se han ampliado llegando incluso a desarrollar mecanismos para atacar dispositivos específicos como lectores USB desarrollado Malware como el llamado Conficker que se ejecuta automáticamente al conectar la llave al USB.[93]

9.2 ASEGURAMIENTO DE REDES

Para poder asegurar una red es importante identificar los puntos de entrada en los sistemas informáticos actuales, estos puntos de entrada pueden ser aplicaciones que se usan comúnmente en las computadoras tales como aplicaciones de correo, el acceso a internet por medio de las páginas web, dado lo anterior es necesario aplicar algunas restricciones con el fin de reducir riesgos dentro de la red, dentro de las medidas que se pueden tomar hay un principio básico que es el restringir dentro de lo posible el sistema a modo lectura acompañado de permisos y restricciones de acceso a los usuario del sistema.

[93] MANKY, Derek. “Fortificar los sistemas TI para atajar la explosión de ciberdelincuencia”. {En línea}. {Consultado el 26 de marzo de 2020} disponible en: (https://cso.computerworld.es/cibercrimen/fortificar-los-sistemas-ti-para-atajar-la-explosion-de-ciberdelincuencia)

Es importante igualmente aplicar medidas para controlar el acceso a internet para evitar el ingreso de virus por este medio. Para lo cual resulta útil tener en cuenta lo siguiente:

9.2.1 Configuración de redes con WPA y WPA2

Los algoritmos para seguridad en redes inalámbricas se considera que empezaron cerca de los años 90 y han tenido cambios a través del tiempo lo que hace que sean mejores y más seguros, con el fin de proteger las redes domésticas se ha creado los protocolos WEP, WPA y WPA2 que, aunque tiene en mismos propósitos son diferentes entre sí.

Estos protocolos permiten que las parte no deseadas se conecten a una red inalámbrica y además encriptan los datos enviados. El protocolo WEP fue desarrollado a finales de los 90 con el fin de ofrecer la misma seguridad que las redes cableadas, aun así, no se lograba una seguridad total y tenía baches de seguridad, conocida por ser fácil de romper ya en contraparte difícil de configurar. Aun hoy es un protocolo que ha sido dejado de lado por sus mismos problemas de seguridad.

WPA2: En 2004 se introdujo el protocolo basado en el estándar 802.11i, y este protocolo represento un significativo avance ya que incluyó el AES (Advance Encryption Standard) la cual encripta la información de índole secreto y se encuentra disponible para redes domésticas, aun así las opciones de ataque a este tipo de redes se presenta constantemente ye el riesgo sigue siendo alto, aunque el intentar el acceso no autorizado a una red con estos protocolos puede representar una tarea de varias horas.[94]

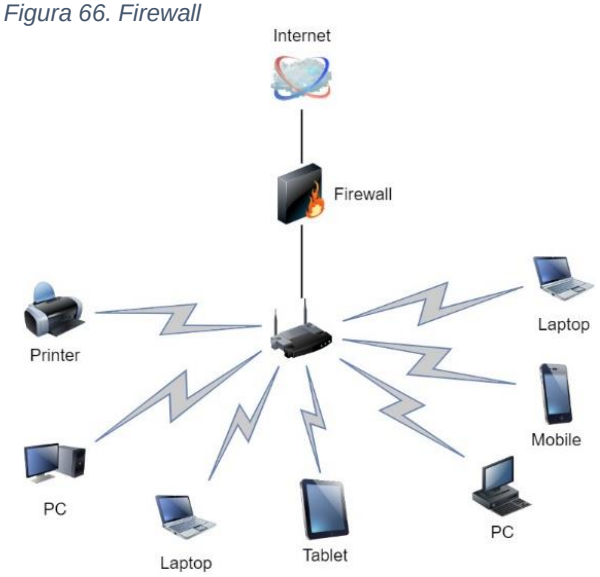
Actualmente los router soportan varios protocolos de seguridad, WPA2 es segura, pero tiene la desventaja de necesitar un hardware más potente pero los proveedores realizan el esfuerzo para proveer del equipamiento necesario para poder implementar este protocolo de seguridad, es recomendable usar WPA2 por encima de WPA, aunque también puede representar una baja en la velocidad de la red. WPA2 tiene la ventaja de aumentar la seguridad de la red estableciendo contraseñas hasta de 63 caracteres, una contraseña fuerte es una buena forma de evitar ataques ya que representa un mayor esfuerzo para el atacante.

[94] ANDREU, Fernando. Redes Wlan Fundamentos y Aplicaciones de Seguridad.: Ed. Marcombo, Barcelona. 2006. 160 p. ISBN 84-267-1405--6.

Actualmente contamos también con el protocolo de seguridad WPA3, es el protocolo de nueva generación que protege las conexiones de red inalámbricas. Una de las principales características de este protocolo es que protege contra los ataques de diccionario mediante el intercambio de claves, además cuenta con reenvío secreto lo que significa que el tráfico permanece encriptado aun cruzando las distintas puertas.

9.2.2 Firewalls:

Figura 66. Firewall



Fuente: Drawio

El Firewall es un componente o un sistema de componentes que se encuentran dentro de una red y que consta de políticas de seguridad que establece la organización con el fin de conservar la seguridad de la información.

Es uno de los elementos más utilizados para protección de redes y sistemas informáticos, está diseñado para proteger una red de intrusos y accesos no autorizados. Un Firewall es Gateway o puerta bloqueada que se abre solo para dejar pasar los paquetes de información que hayan pasado ciertos filtros. Los Firewall son utilizados mayormente por grandes organizaciones.[95]

El Firewall puede constar de varios dispositivos y se ubica en medio de dos redes, contiene información sobre las políticas de seguridad establecidas, protegiendo una

[95] KOMAR, Brian. et al. 2003. Firewalls for dummies. Segunda edición. New York : Wiley Publixhing Inc., 2003. pág. 428 p. ISBN 0-7645-4048-3.

red segura como lo puede ser una red corporativa de una red de riesgo como lo es internet.

El uso de Firewall busca cumplir los siguientes objetivos:

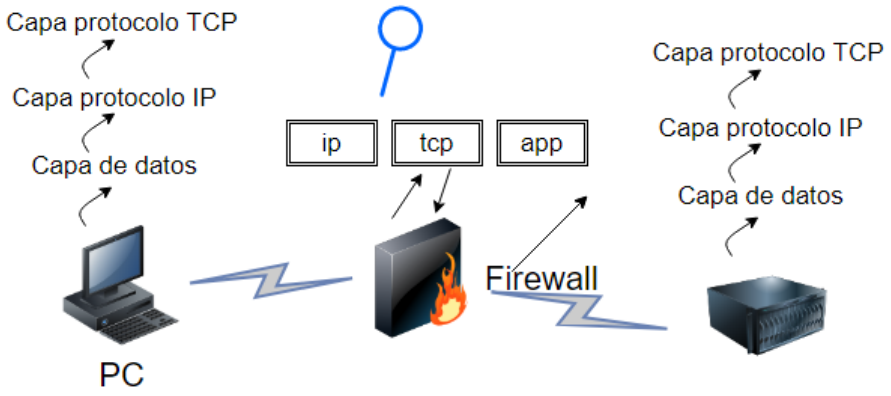
- El tráfico que pasa de fuera hacia adentro y viceversa debe pasar por el Firewall.
- Solo puede pasar el tráfico que este permitido por las políticas de seguridad.

El Firewall solo puede proteger solo el perímetro comprendido por la red, si se presenta un ataque dentro de la red no puede ser impedido, si el firewall logra ser vulnerado se pierde la protección del total de la red. Teniendo en cuenta que la información debe pasar por el Firewall, es una buena práctica dar seguridad adicional encriptando los datos que transitan por la red. [96]

9.2.3 Tipos de Firewall

Filtrado de paquetes: Los Firewall de filtrado de paquetes trabajan sobre el nivel de Transporte y Nivel de Red del modelo OSI dado el funcionamiento y estructura de este tipo de Firewall, son económicos y su desempeño se considera bueno y no es percibido por el usuario.

Figura 67. Firewall de cifrado de paquetes



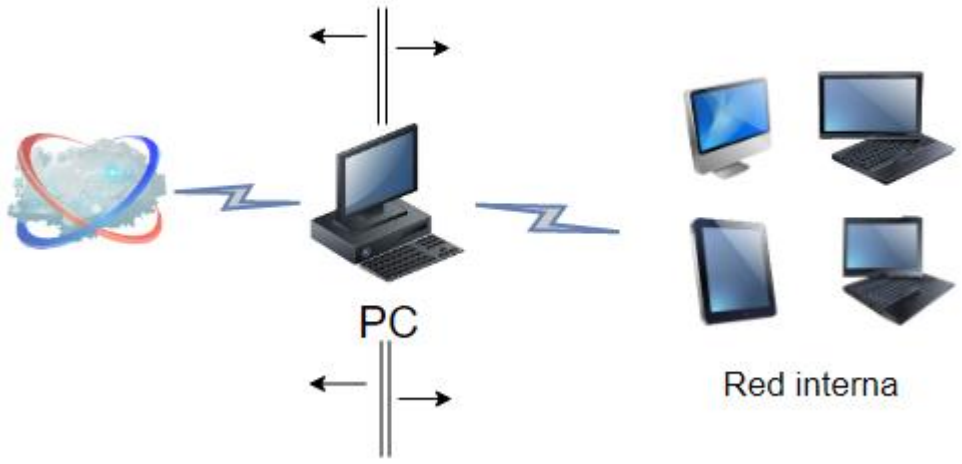
Fuente: Huawei.com

[96]RIOS, Julio. "Seguridad Informática".{En Línea} {10 de Abril de 2020} (https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.html.)

Dual-Homed Host: Estos dispositivos se caracterizan por estar conectados perímetro interior y también al perímetro exterior, y no permite el paso de IP (IP-Forwarding desactivado).

Un usuario en el perímetro interior que desee una conexión exterior se conectará primero al Firewall, el proxy atenderá la petición, y de acuerdo a la configuración de seguridad y hará de puente entre el exterior y el usuario al interior utilizando dos conexiones: una que parte desde la máquina del perímetro interior y va hasta el Firewall y otra conexión que va desde el Firewall hasta la maquina host del servicio exterior.[97]

Figura 68. Dual-Homed



Fuente: Elaborado por el autor

Screened Subnet: Consta de aislar la maquina más atacada y vulnerable del Firewall, siendo el Nodo Bastion. Se establece una DMZ o zona desmilitarizada de forma que si el atacante logra la intrusión no consiga el control total de la subred protegida. [98]

Proxy-Gateway de aplicaciones:
El filtrado de paquetes puede contar con debilidades, para contrarrestarlas, se ha creado por parte de desarrolladores software de aplicación capaz de filtrar las

[97] KOMAR, Brian. et al. Firewalls for dummies. Segunda edición. New York : Wiley Publixhing Inc., 2003. 428 p. ISBN 0-7645-4048-3.

[98] KOMAR, Brian. et al. Firewalls for dummies. Segunda edición. New York : Wiley Publixhing Inc., 2003. 428 p. ISBN 0-7645-4048-3.

conexiones, esto se conoce como servidor Proxy el cual se ejecuta en una máquina que se llama Bastion Host o Gateway de aplicación.[99]

Screened Host: Es la combinación de un Host Bastión con un Router, y utiliza el filtrado de paquetes como primera barrera de seguridad. Se permite solo un número reducido de servicios, en el Choke se filtran los paquetes peligrosos y se ejecuta el Proxy de aplicaciones. El Screened host puede asegurar los equipos de la red interna.[100]

Figura 69. Screened Host

Fuente: Elaborado por el autor.

Si bien el Firewall es un método de protección efectivo, también tiene sus desventajas, por ejemplo, protege solo capas bajas del modelo OSI, no tiene la posibilidad de proteger las más altas como presentación y aplicación, así mismo está fuera del Firewall el poder esconder la topología de red de la red privada por lo que puede representar una vulnerabilidad al contar con esta información, si las políticas de seguridad llegan a ser complejas puede no soportarlas,

El Gateway conocido también como puerta de enlace, es un dispositivo tipo ordenador configurado para interconectar redes con protocolos y arquitectura diferente en todos los niveles de comunicación, traduciendo la información del protocolo de una red a la red receptora.[101]

---

[99] Ibid., p 303.
[100] Ibid., p 174.

[101] ECURED. Puerta de Enlace. [En línea]. Disponible en: https://www.ecured.cu/Puerta_de_enlace.

9.3 MECANISMOS ANTE RIESGOS DE SEGURIDAD

Los mecanismos de seguridad informática se componen de técnicas y herramientas que permiten disminuir el riesgo en la exposición de la confidencialidad, disponibilidad e integridad de la información.

9.3.1 Autenticación:

Este mecanismo busca la identificación del usuario del sistema, por ejemplo, al ingresar a un equipo, una red o una base de datos. Es posible la autenticación de las siguientes formas:

- Lo que uno saber, por ejemplo, contraseñas
- Lo que uno tiene, por ejemplo, un token
- Lo que uno es, por ejemplo, huella digital y biometría

Es común utilizar uno o más métodos de autenticación, lo que trae como ventaja que la autenticación de un usuario se haga de la forma correcta y que el usuario autorizado realmente sea quien intenta acceder al sistema. Esta decisión, de usar uno o más o cuales usar se determina por el valor que se le da a la información que se busca proteger, la organización en consideración a esto lo determinará. Una vez se ha realizado la autenticación cada usuario dispone de unos roles o niveles de acceso a la información.[102]

El uso de contraseñas es ampliamente usado actualmente, pero muchas veces no se hace de la forma correcta, el éxito de este método está en gran parte determinado por el usuario, ya que al usar contraseñas fuertes y difíciles de adivinar o romper será igualmente más difícil para un atacante vulnerar el sistema de autenticación.

Las contraseñas deben ser en todo caso confidenciales y es responsabilidad del dueño resguardarla y que esta no se transferida de ninguna forma, por lo anterior es una mala práctica anotarla en papeles y prestarla a otra persona. Las contraseñas seguras deben tener un conjunto de caracteres lo suficientemente amplio como para evitar ser adivinada, junto con la incorporación de números y

[102] AGUILERA, Purificación. Seguridad Informática. Madrid: Ed. Editex, 2010. ISBN 978-84-9771-657-4.

signos, minúsculas y mayúsculas, así como el cambio de contraseña de forma constante.

9.3.2 Autorización:

El proceso de autorización determina el cómo, cuándo y dónde un usuario tiene acceso a recursos corporativos. Los recursos se deben organizar en niveles y de acuerdo con el nivel se le concede un grado de autorización, lo anterior basado en la importancia o valor de la información.

Para autorizar el uso de recursos se suele usar formularios y contraseñas, y es importante llevar un registro para controlar las autorizaciones, las cuales solo se conceden a quienes por el desarrollo de sus actividades en la organización lo requieran, en caso contrario siempre el acceso será denegado.[103]

9.3.3 Administración:

Elimina, mantiene y define el tipo de autorización de los usuarios de los sistemas. Es una actividad de gran dinamismo que requiere actualización constante, esto debido a la constate evolución d ellos sistemas y los riesgos que día a día aparecen en la red. Para esta tarea se utiliza software incorporado den los mismos sistemas operativos, o también se puede utilizar software específico para tal fin.

9.3.4 Auditoria y registro:

La auditoría es la vigilancia de los servicios de producción valiéndose del análisis de información. El registro por su parte el registro es un mecanismo que almacena los intentos de vulnerar un sistema con el fin de poder analizarlo posteriormente. La característica en común de estos dos procesos es que requieren de un análisis posterior, existen métodos manuales y automatizados para realizar estas tareas y la frecuencia con la cual se hace depende del nivel de riesgo y o crítico de la información.[104]

---

[103] AGUILERA, Purificación. Seguridad Informática. Madrid : Ed. Editex, 2010. ISBN 978-84-9771-657-4.

[104] MIFSUD, Elvira. "Listas de Control de Acceso" {En Línea} {30 de Mazo de 2020} disponible: http://recursostic.educacion.es/observatorio/web/ca/software/servidores/1065-listas-de-control-de-acceso-acl?start=3.

9.3.5 Código de detección de modificación:

Este mecanismo consiste en una suma que se agrega a los datos que se quieren transmitir, el receptor efectúa la comprobación por medio de la recepción de la suma junto a los datos. La suma es implementada por métodos criptográficos y debe arrojar el mismo resultado tanto en el emisor como en el receptor.

9.3.6 Código de autenticación del mensaje:

Similar al anterior, cuando el receptor realiza la comprobación puede estar seguro de la veracidad del emisor mediante una suma cifrada al enviar el mensaje.

9.3.7 Firma digital:

Consiste en una función relacionada a un documento con clave privada del firmante, por lo que la firma depende exclusivamente del mensaje y del emisor del mismo. Se utiliza para para servicios de no repudio debido a la certeza que tiene el receptor sobre el emisor del mensaje.[105]

9.3.8 Numero de secuencias de mensaje:

A cada paquete de transmisión en la que puede llegar a ser dividido se le asigna un número que poder ser cifrado o no cifrado, este número identifica el paquete por medio de una secuencia de bits, el receptor verifica que esta secuencia corresponde a los paquetes que está recibiendo, este proceso permite identificar la inserción o sustracción de paquetes dentro del mensaje.

9.3.9 Cifrado:

El cifrado impide que usuarios o procesos puedan entender la información transmitida transformándola para que sea ilegible. Por medio de técnicas de cifrado

[105] BORJA, Lázaro. Certificación de la firma digital.Primera edición. Madrid: Ed. Forem, 2005. pág. 77. ISBN 84-933150-5-2.

la seguridad de la información se logra por la protección cifrada junto a otros mecanismos de seguridad.[106]

9.3.10 Relleno de tráfico:

Consiste en enviar datos falsos junto a los datos verdaderos, con el fin de engañar a quien pueda estar monitoreando la red y analizando el tráfico haciendo difícil discriminar entre información útil y la que no lo es.

9.3.11 Certificación:

La certificación la realiza un tercero, un agente de confianza, el cual certifica la integridad, frecuencia y secuencia de los datos, así como del receptor y del emisor de estos. [107]

[106] AGUILERA, Purificación. Seguridad Informática. Madrid : Ed. Editex, 2010. 240 p. ISBN 978-84-9771-657-4.

[107]SUAREZ, Rodrigo." Mecanismos de Seguridad Informática". {En línea} {19 de Abril de 2020} disponible en:. (http://blogs.acatlan.unam.mx/lasc/2016/04/19/mecanismos-de-seguridad-informatica/.)

10. CONCLUSIONES

- Las personas como usuarios de los sistemas informáticos son el componente más importante, pero a la vez más vulnerable de los mismos, debido a que por desconocimiento pueden incurrir en faltas a normas básicas de seguridad informática, lo que puede tener como consecuencias la vulneración de la red doméstica y la exposición de esta a ciberdelincuentes.

- El grado de conciencia que tenga el usuario respecto a la seguridad de la información representa en gran medida el nivel de seguridad de un sistema de seguridad en las organizaciones, mediante pruebas de pentesting se logra identificar brechas de seguridad dentro de la red doméstica, tal como el uso de contraseñas débiles, siendo esto, la puerta de entrada a riesgos mayores.

- La tecnología de defensa de un sistema va mucho más allá de simplemente el uso de antivirus, firewall y vpn´s, detrás de todo esto se debe contar con una completa conciencia partiendo del conocimiento del usuario de tecnología lo que se convierte en el primer escudo de defensa contra ataques a redes domésticas.

11. RECOMENDACIONES

Es importante mantener actualizado el sistema operativo, así como, todos los softwares con que cuenta el equipo informático, resaltando que uno de los componentes más utilizados y por lo tanto más vulnerable es el navegador web, por lo cual, se debe mantener actualizado.

El uso de antivirus es un método sencillo para protegerse de múltiples problemas de seguridad, todos los usuarios de internet navegan en diferentes sitios y descargan archivos, examinar estos, con el antivirus puede evitar graves daños en el sistema.

Se recomienda habilitar el firewall de Windows o con el que cuente instalado en su equipo personal, así como, revisar que se encuentre actualizado.

Un método efectivo de seguridad informática es el uso de contraseñas fuertes y seguras, compuestas por mínimo 8 caracteres, combinando letras, números y caracteres especiales. De igual forma es importante actualizar la contraseña recurrentemente para evitar fallas de seguridad.

Es importante tener especial cuidado al navegar por la web, para identificar las páginas seguras, más aún si se realizan transacciones y compras, en este caso es importante que la página cuente con certificado digital confiable.

El correo electrónico es uno de los medios más utilizados por los ciberdelincuentes para realizar estafas, es importante cuidar la información que se maneja a través de él, así como, evitar el ingreso a enlaces desconocidos y la descarga de archivos sospechosos.

Mantenerse informado y actualizado en temas de seguridad informática es la primera defensa ante riesgos informáticos, el usuario es el blanco principal de muchos ciberataques.

12. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación del mismo; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de seguridad informática en redes domésticas, puedan acceder al documento.

BIBLIOGRAFÍA

ACIS Asociacion Colombiana de Ingenieros de Sistemas. (2020). Seguridad y Ciberseguridad. (155).

AGUADO, David Prudencio**.** Seguridad Informáticva para el Hogar. Como asegurar nuestra red. Madrid. Bubok Publishing, 2012. 93 p. ISBN: 8468604674

AGUIERRE, Sebastian. Vivir en el poblado. El teletrabajo durante la cuarentena en Colombia: ¿cómo hacen vigilancia las ARL?. (En linea) (19 de Mayo de 2020). Disponible en https://vivirenelpoblado.com/teletrabajo-en-cuarentena-vigilancia-arl/

AGUILERA, Purificación. Seguridad Informática. Madrid : Ed. Editex, 2010. 240 p. ISBN 978-84-9771-657-4

ALEXANDER, Alberto G. (s.f). Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El Enfoque ISO 27001:2005. (En linea) (10 de Mayo de 2020) Disponible en: (http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf.)

ANDREU, Fernando. Redes Wlan Fundamentos y Aplicaciones de Seguridad.: Ed. Marcombo, Barcelona. 2006. 160 p. ISBN 84-267-1405--6

AVAST, Avast Blog. [En línea]. [16 de mayo de 2017] Disponible en: (https://blog.avast.com/es/predicciones-para-2019-el-internet-de-las-cosas-vulnerables).

BACA, Gabriel. Introducción a la Seguridad Informática. México. 2016. Grupo Editorial Patria.

BACH, Mario. "Seguridad Informática VI". {En línea}. {22 de Febrero de 2020} Disponible en: (http://2bconsmario.blogspot.com/2017/10/seguridad-informatica-vi.html.)

BANKIA. (2020). Bankia. Obtenido de http://www.bfatenedoradeacciones.com/en/retail-banking/security/cybersecurity-glossaryBan

BARCELÓ, Miquel. Una historia de la informática. Barcelona. 2008. Ed. UOC

BARREN, Daniel,et al**.** SSH, The Secure Shell, The Definitive Guide. Serverwide Configuration Segunda edición. California USA . Ed.OReilly Media, 2005. 645 p. ISBN: 0-596-00895-3

BORJA, Lázaro. Certificación de la firma digital.Primera edición. Madrid: Ed. Forem, 2005. 77 p. ISBN 84-933150-5-2.

BURGOS, Alexis. Seguridad PC. Ed. Fox Andina. pág. 192. Buenos Aires. ISBN 978-987-663-031-3.

BURZTEIN, Sara. Magazitum. Factor humano: El talón de Aquiles de la Seguridad (En línea) (10 de octubre de 2014). (06 de agosto de 2020). Disponible en https://www.magazcitum.com.mx/?p=2735#.XyyhWShKjIU

BUSTAMANTE, Rubén. Seguridad en Redes. Hidalgo. 2005. Universidad Autónoma del Estado de Hidalgo.

CANALDA, Victor. "Proyecto tecnológico" {En línea}{16 de Mayo de 2017}. disponible en: (https://blogdevictorcanalda.blogspot.com/2017/05/.)

CANO, Jeimy J. Pautas y Recomendaciones para elaborar Políticas de Seguridad Informática (PSI). (En linea) (26 de Mayo de 2020). Disponible en: (http://www.derechotecnologico.com/estrado/estrado004.html.)

CARBALLAR, Jose Antonio. Wi-Fi lo que necesita conocer. Para que sirve Wi-Fi. Madrid. RC Libros. 2010. 211 p. ISBN: 978-84-937769-0-9

CEGARRA, Jose. ”Metodología de la investigación científica y tecnológica”, España: Ediciones Días de Santos, S.A., 1° edición. 2004.

CHICANO, Esther. Auditoría de Seguridad Informática. Málaga. IC Editorial, 2014. ISBN 978-84-16433-23-0.

CONSEJO ARGENTINO DE RELACIONES INTERNACIONALES (CARI). Ciberdefensa: los riesgos que plantea. (En linea) (3 de Marzo de 2020).Disponible en: (http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf)

CORLETTI, Alejandro. ANÁLISIS DE ISO-27001:2005. (En línea) (16 de Septiembre de 2020) Disponible en: http://documentos.shellsec.net/otros/analisis_iso27001_shellsec.net.pdf

COURSE TECHNOLOGY. 2004. Diccionario de Informatica E Internet: Computer and Internet Technology Definitions in Spanish. Montreal : Ed. Cengage Learning, 2004. 221 p. ISBN 9780619267889.

CUNHA, Daniel. Películas, compras y videojuegos en Internet: los riesgos de seguridad durante los días de cuarentena. welivesecurity eset. {En línea}. {Citado el: 25 de Abril de 2020} disponible en: (https://www.welivesecurity.com/la-

es/2020/03/26/peliculas-compras-videojuegos-internet-riesgos-seguridad-dias-cuarentena/.)

DEFINICIÓN ABC. Definición de infraestructura. (En línea). (04 de febrero de 2020) Disponible en: (URL: http://www.definicionabc.com/general/infraestructura.php)

DE LUIS, Erik. La seguridad de los menores en internet. Barcelona : Editorial UOC, 2017. ISBN 978-84-9116-963-5.

DIAZ, Gabriel. Procesos y Herramientas para la seguridad en redes. Madrid : Uned Publicaciones, 2014. ISBN 978-84-362-6838-6.

DIAZ, Jhonathan. "Tantas ip como granos de arena". {En línea} {09 de Abril de 2020} disponible en: (http://usuariosinfinitosipv6.blogspot.com/2015/04/todos-somos-un-numero-en-la-red-mundial.html.)

DESONGLES, J. y Moya, . “Conocimientos básicos de Informática”, España: Editorial Mad, S.L., 1° edición.

DOCUMETOP. documentop.com. guía de seguridad (ccn-stic-401) glosario y ... - CCN-CERT - CNI - DOCUMENTOP.COM. (En línea) (2 de septiembre de 2015) (Recuperado 4 de abril de 2020) Disponible en: Obtenido de https://documentop.com/guia-de-seguridad-ccn-stic-401-glosario-y-ccn-cert-cni_5a02e7b01723dd12f3e3eecd.html

ECURED. Puerta de Enlace. (En línea). (Recuperado 24 de marzo de 2020). Disponible en: https://www.ecured.cu/Puerta_de_enlace

ERNEST & YOUNG**.** El Diario Exterior. "La seguridad informática en las empresas no es la prioridad, a pesar de los ataques". {En linea} { 20 de Febrero 2020} disponible en: (https://www.eldiarioexterior.com/articulo.asp?idarticulo=2356.)

ESPIÑEIRA, Sheldon y Asociados. ISO 27000: orden a la seguridad. (En línea) (Recuperado 16 de agosto de 2020). Disponible en: (http://www.pcnews.com/detalle.asp?sid=&id=10&Ida=2544.)

FERNANDEZ, Henry. Análisis de la seguridad del sitio web del Ministerio del Trabajo aplicando pruebas de Pentesting en la sede principal de la ciudad de Bogotá. (En línea) (2 de Julio de 2019). Repository.unad.edu.co. Obtenido de https://repository.unad.edu.co/handle/10596/27059

FISHER, Royal**.** Seguridad en los sistemas informáticos. De máxima prioridad a la seguridad. Madrid : Ediciones Diaz y Santos. 1988. 262 p. ISBN: 0-13-464727-0

GOMEZ, Alvaro. Enciclopedia de la Seguridad informática. 2a Edicón. Madrid : Ra-Ma, 2014. 830 p. ISBN 978-84-9964-038-5.

GONZALEZ, Jesus. 2017. Softaones.es. Tutorial de Virtual Box para emular sistemas operativos. [En línea] 06 de Marzo de 2017. [Citado el: 04 de 08 de 2020.] Disponible en: https://www.softzone.es/manuales-software-2/tutorial-de-virtualbox/.

GONZALEZ, María. Xataka. Qué es y cómo funciona el protocolo BitTorrent. [En línea] 05 de Abril de 2011. [Citado el: 27 de 07 de 2020.] Disponible en: https://www.xataka.com/

GUZMAN, Camilo, et al. Protocolos para la mitigación de ciberataques en el hogar. Trabajo de Grado Especialísta en Seguridad de la Información. Bogotá : Universidad Católiaca de Colombia. Facultad de Ingeniería. 2017. 79 p

HERNANDEZ, Joel. esemanal. Historia y evolución de las redes. [En línea] (18 de Abril de 2008). (16 de Abril de 2020) Disponible en https://esemanal.mx/2008/04/historia_y_evolucion_de_las_redes_/.

HOSTINGER. (4 de 04 de 2020). Tutoriales Hostinger. Obtenido de ¿Qué Es El Protocolo SSH Y Cómo Funciona?: https://www.hostinger.es/tutoriales/que-es-ssh

HUIDOBRO, Jose Manuel. Manual de Domótica. Redes (datos, control, multimedia y comunicaciones). España : Creaciones Copyrigth S.L, 2010. 206 p. ISBN 976-84-92779-37-6

IPV6.MX.Fundamentos IPv4. {En línea} {10 de Abril e 2020} disponible en: (http://www.ipv6.mx/index.php/informacion/fundamentos/ipv4.)

IOS. tecnologia de la informacion. tecnicas de seguridad. sistemas de gestion de la seguridad de la informacion sgsi. ginebra iso. 2005

INTERNATIONAL Telecommunication Union (ITU). Decisiones destacadas de Guadalajara, Ciberseguridad, (En linea) (06 de Abril de 2020) Disponible en: (https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx)

JUNESTRAND, Stefan, PASSARET, Xvier y VASQUEZ, Daniel. Domótica y hogar digital. Integracion de sistemas del hogar digital. Madrid : Thomson Ediciones S.A, 2005. 174 p. ISBN: 84-283-2981-9

KASPERSKY LAB, Kaspersky LAB. [En línea]. [Recuperado 04 de abril de 2020] Disponible: (https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.

KIO NETWORKS. Protocolos de comunicación de redes. (En línea) (Recuperado 11 de septiembre de 2020). Disponible en https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes#:~:text=Los%20protocolos%20para%20la%20transmisi%C3%B3n,son%20POP%2C%20SMTP%20y%20HTTP.

KOMAR, Brian. et al. Firewalls for dummies. Segunda edición. New York : Wiley Publixhing Inc., 2003. 428 p. ISBN 0-7645-4048-3.

LAZARO, Francisco. Introducción a la informática Forense. Madrid : Editorial RA-MA, 2014. ISBN 978-84-9964-209-3.

LEÓN, Mario. Diccionario de informática Telecomunicaciones y ciencias afines. Madrid : Ed. Babel, 2004.1348 p. ISBN 84-7989-626-4.

LOPEZ, Maar.Issuu. Glosario de seguridad informática. [En línea] (2 de Febrero de 2018). (3 de Mayo de 2019) Disponible en https://issuu.com/maarlopez/docs/glosario_de_seguridad_inform__tica.

LINARES, Samuel. Presentación titulada “Implementando la Ciberseguridad desde la realidad: Perspectiva desde Europa, América y Medio Oriente”. (En línea). (13 de Julio de 2020) Disponible en: (https://www.cci-es.org/documents/10694/0/IV+Congreso+ línea)

LÓPEZ, Agustín y Ruiz, Javier. (s.f). ISO 27000. (En línea). (Recuperado 16 de agosto de 2020) Disponible en: (http://www.iso27000.es/es/download/doc_iso27000_all.pdf)

MAGERIT. (s.f.). Metodología de Análisis y Gestión de Riesgos de Sistemas de Información. Libro 2.

MANKY, Derek. “Fortificar los sistemas TI para atajar la explosión de ciberdelincuencia”. {En línea}. {Recuperado 26 de marzo de 2020} disponible en: (https://cso.computerworld.es/cibercrimen/fortificar-los-sistemas-ti-para-atajar-la-explosion-de-ciberdelincuencia)

MARQUÉS, Guillermo. IPSec Redes Privadas Virtuales. s.l. : Ed. Lulu, 2016. 66 p. ISBN 9781329824195.

MENDILLO, Vincenzo. Seguridad en Informática y Comunicaciones: Una necesidad de la era moderna. UCV. (En línea). (Recuperado 18 de septiembre de 2020) Disponible en: (http://www.iso27000.es/es/download/doc_sgsi_all.pdf)

MIFSUD, Elvira. "Observatorio Tecnológico. Listas de Control de Acceso". {En línea} {12 de Abril de 2020} disponible en:.

(http://recursostic.educacion.es/observatorio/web/ca/software/servidores/1065-listas-de-control-de-acceso-acl?start=3.)

NETWORKWORLD. networkworld. (En línea) Principales amenazas para la seguridad de las redes inalámbricas. (18 de 01 de 2016). (Recuperado el 27 de Julio de 2020) Disponible en: https://www.networkworld.es/seguridad/principales-amenazas-para-la-seguridad-de-las-redes-inalambricas

OJEDA, Daniel. El Espectador. [En línea]. (Recuperado 04 de abril de 2020) Disponible en: (https://www.elespectador.com/tecnologia/cuidado-estos-son-los-ataques-informaticosque-seran-protagonistas-en-2019-articulo-834202.)

OSI. osi.es. de Sabias que el 90% de las contraseñas son vulnerables. (En línea) (02 de 06 de 2019). (Recuperado el 05 de agosto de 2020 https://www.osi.es/es/actualidad/blog/2019/02/06/sabias-que-el-90-de-las-contrasenas-son-vulnerables

OVALLE, Anggie Katherine. Uso de herramientas informáticas para descubrir vulnerabilidades en las redes wifi domesticas. Trabajo de Grado Especialista en Seguridad informática. Bogotá : Universidad Católica de Colombia. Facultad de Ingeniería. 2019. 64 p.

PACHECO, Federico. Hackers al descubierto. s.l. : Creative Andina Corp, 2010. 421p.

PANDA. (s.f.). Panda Security.com. de Que es bittorrent, (En línea) (Recuperado el 06 de agosto de 2020), https://www.pandasecurity.com/es/security-info/bittorrent/

PARDO, Ezequiel. Microinformática de gestión. Oviedo : Publicaciones Universidad de Oviedo, 1993. 373 p. ISBN 84-7468-788-8.

PILLAJO, José. Importancia del estudio del control para los sistemas cyber-físicos. (En línea) (Recuperado 15 de mayo de 2020). Disponible en: http://carlospillajo.info/wpcontent/uploads/sites/1369/2014/12/Importancia-del-estudio-de-control-para-los-CPS_RevCP.pdf

PNTIC,MEC,ES. (s.f.). Descargas.pntic.mec.es. Obtenido de Mecanismos básicos de seguridad ciber Informática: Disponible en http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/mecanismos_bsicos_de_seguridad.

POLICIA NACIONAL. Centro cibernético policial. Obtenido de Amenazas del cibercrimen en Colombia 2016-2017: (marzo de 2017) (Recuperado el 05 de marzo de 2020) Disponible en;

https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

RAZQUIN, Rafael. Seguridad informática básica para profesionales. (En linea) (Recuperado 25 de Abril de 2020) Disponible en: (http://www.herrerodigital.com/blog/seguridad-informatica-basica-para-profesionales)

REMER, Red. (s.f.). Proteccioncivil.org. (En línea) (Recuperado 6 de abril de 2020) Disponible en: http://www.proteccioncivil.org/catalogo/carpeta02/carpeta24/vademecum19/vdm02516.htm

RIOS, Julio. Seguridad Informática".{En Línea} {10 de Abril de 2020} (https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.html.)

ROMERO, Martha, *et al*. Introduccion a la seguridad informatica y análisis de vulnerabilidades. Introducción a la Seguridad Informática. Alicante. Editorial Area de Innovación y desarrollo. 2018. 123 p.. ISBN: 978-84-949306-1-4

RUBEN, A. (03 de 04 de 2016). Computer Hoy. Recuperado el 04 de 08 de 2020, de Que es Kali Linux y que puedes hacer con el: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671

RUBEN, Andres. Computer Hoy. Que es Kali Linux y que puedes hacer con el. [En línea] (03 de 04 de 2016). [Recuperado el 04 de Agosto de 2020.] Disponible en: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671.

RUIZ, Enrique. Sistemas integrados y hogar digital. España. 2020. Ediciones Parainfo S.A.

SALDANA, Gabriel. Kaspersky Lab Daily. [En línea]. [Recuperado 20 de febrero de 2020] Disponible en: (https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataquesciberneticos-en-america-latina/13266/.)

SAAVEDRA, Gabriel Andres. Seguridad en redes inalambricas domesticas. Monografía para Ingeniero de Sistemas. Bogota. Universidad Libre de Colombia. Facultad de Ingeniería de Sistemas. 2011. 59 p.

SILES, Roberto. Análisis de seguridad de la familia de protocolos tcp/ip. Santiago: catatonia. 2001.

STALLINGS, William. Fundamentos se Seguridad en Redes Aplicaciones y Estándares. Seguridad en los sistemas. Segunda edición Madrid. Pearsons Education. 2004. 432 p. ISBN: 84-205-4002-1
STEL, Enrique. Seguridad y ciberdefensa del espacio. Buenos Aires : Ed. Dunken, 2014. 192 p. ISBN 9789870271871.

SUAREZ, Rodrigo." Mecanismos de Seguridad Informática". {En línea} {Recuperado 19 de Abril de 2020} Disponible en:. (http://blogs.acatlan.unam.mx/lasc/2016/04/19/mecanismos-de-seguridad-informatica/.)

TANENBAUM, Andrew. Redes de computadoras. Uso de las redes de computadoras. Cuarta edición. Mexico : Prentice Hall, 2003. 869 p. ISBN: 970-26-0162-2

TECNÓSFERA, El Tiempo. [En línea]. [23 de agosto 2017.] [Consultado el 26 de marzo de 2020]. Disponible en (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/mas-de-la-mitad-de-loshogares-en-colombia-cuenta-con-acceso-a-internet-122714)

TORRES, Katia. La ONU y los Delitos Informaticos. {En línea} {Recuperado 23 de Febrero de 2020}. Disponible en: (https://prezi.com/i9pr2hukxiyu/la-onu-y-los-delitos-informaticos/.)

UNIVERSIDAD VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme? | VIU. (En línea) (Recuperado 04 de abril de 2020) Disponible en: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

VELASCO, R. (03 de enero de 2017). Redes Zona. Recuperado el 06 de 08 de 2020, de Controla el tráfico de tu red local con Network Meter: https://www.redeszone.net/2017/01/03/controla-trafico-red-local-network-meter/

VELASCO, Ruben. Redes Zone. Controla el tráfico de tu red local con Network Meter. [En línea] (03 de Enero de 2017). [Citado el: 06 de Agosto de 2020.] Disponible en: https://www.redeszone.net/2017/01/03/controla-trafico-red-local-network-meter/.

VERIZON. Español, verizon, com. Obtenido de Resumen de Redes Domesticas. (En línea) (Recuperado 11 de septiembre de 2020). Disponible en: https://espanol.verizon.com/support/residential/internet/home-network/overview#:~:text=Hay%20dos%20tipos%20de%20redes,con%20cables%20o%20dispositivos%20inal%C3%A1mbricos.

WIKI.IES. Wiki, ies. Haria Informática. Obtenido de Características y componentes de las redes locales. (En línea) (Recuperado 6 de octubre de 2019) Disponible en:

https://smr.iesharia.org/wiki/doku.php/rde:ut1:caracteristicas#caracteristicas_de_las_redes_locales