PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

CARRERA DE:

INGENIERÍA EN TECNOLOGIAS DE LA INFORMACIÓN

Trabajo de Titulación

Tema:

ANÁLISIS DE VULNERABILIDADES EN DISPOSITIVOS IOT EN LA RED DE UN NEGOCIO DE LA PARROQUIA DE MACHACHI

AUTOR:

Emily Rea

QUITO, JUNIO 2024

DEDICATORIA

El trabajo de titulación se lo dedico a Hugo René Quinteros, el ser más especial en mi vida, que ha sido mi mayor apoyo y fuerza día a día. Aunque ya no se encuentre entre nosotros, siempre ha sido mi guía cada día de mi vida, ya que, de no ser por él, todo mi trayecto a lo largo de esta etapa universitaria no hubiera sido posible. Sé que, estés donde estés, mi querido viejito, nunca te olvidaré, porque fuiste y serás siempre mi padre, mi fuerza y mi fortaleza. Por tu constante apoyo día tras día hasta tu último aliento, este trabajo es para ti y por ti.

AGRADECIMIENTO

Agradezco principalmente a mi madre, quien ha sido siempre mi apoyo incondicional, así como a mi familia materna, hermanos y a mi papi Javy, quienes han creído en mí. Gracias por sus elogios y consejos en cada momento necesario.

Asimismo, extiendo mi agradecimiento a mis compañeros de carrera, Freddy Pijal, Adrián Bastidas y Marilin Ilbay, quienes no me dejaron decaer en los momentos más difíciles de la carrera. Les agradezco por su constante ayuda y por ver una salida cuando todo parecía perdido. A cada persona que formó parte de mi etapa universitaria, les estoy profundamente agradecido.

Además, quiero expresar mi gratitud a cada docente que ha sido mi mentor a lo largo de mi crecimiento educativo, especialmente a los de la Pontificia Universidad Católica del Ecuador. En particular, agradezco a mi tutora de tesis, la ingeniera Beatriz Campos, quien no me dejó rendirme en ningún momento. Sin su apoyo, no habría logrado culminar este proyecto.

Igualmente, agradezco a Esteban Acuña, Verónica Rivera, José Cabrera, Jazmín Herrera, Ricardo Albán y Michael Rodríguez, quienes han sido mi apoyo en mis últimos semestres. Han creído en mí y me han impulsado constantemente a culminar esta etapa y obtener mi título universitario.

Por último, quiero agradecer el apoyo económico brindado en los primeros semestres por el Sr. Roberto Rea. Aunque eventualmente tuve que buscar otras formas para poder culminar mis estudios debido a la falta de apoyo y compromiso ante una promesa, siempre reconoceré que la herencia más grande es el estudio, ya que me permitirá alcanzar todo lo que algún día soñé.

RESUMEN

El presente trabajo de tesis se enfoca en la identificación de vulnerabilidades presentes en los dispositivos IoT (Internet de las Cosas) conectados a redes locales, específicamente en entornos comunitarios. El presente trabajo se aplicó dentro de la red de un negocio el cual cuenta con dispositivos IoT comunes en la mayoría de los establecimientos e incluso hogares; se ha realizado un exhaustivo análisis de las vulnerabilidades que tienen estos instrumentos. Es importante tomar en cuenta que, al compartir una red con los clientes del negocio, permite identificar la necesidad de crear conciencia en los propietarios sobre la pérdida de datos y riesgos en general que podrían experimentar si no se toman medidas preventivas.

Para generar conciencia en los propietarios sobre el riesgo al que están expuestos sus dispositivos IoT, se realizó un ataque controlado, en el cual se pretende suplantar la red del negocio, desconectar a los dispositivos y a su vez actuar como un "man in the middle".

En base a la información recolectada, se presentan diversas soluciones y medidas de seguridad que pueden implementarse para prevenir ataques cibernéticos hacia los dispositivos en red, tales como: mantenerlos actualizados, cambio de credenciales predeterminadas, deshabilitar servicios fuera de uso y puertos de red innecesarios, configuración de firewalls en los equipos, instalación de sistemas SOC, entre otras. Este estudio pretende contribuir al conocimiento sobre la seguridad en entornos IoT, instruir a los usuarios sobre los riesgos potenciales y proporcionar pautas prácticas para la protección de dispositivos conectados a redes locales.

1. Contenido

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO I - DEFINICIÓN DEL TRABAJO

1.1. Justificación

En la actualidad, la mayoría de los lugares comerciales cuenta con al menos un dispositivo IoT conectado a una red pública o privada; sin embargo, su constante uso evita que el usuario común detecte las amenazas potenciales en la práctica. Es fundamental generar conciencia entre las personas sobre los riesgos asociados a la falta de precauciones en la seguridad de los datos, no solo en los equipos que proveen el servicio, sino en una amplia gama de dispositivos, como por ejemplo computadoras, celulares, Smart TVs, relojes inteligentes, electrodomésticos, entre otros. A menudo, no se toman las medidas adecuadas para proteger estos equipos de posibles ataques cibernéticos.

Muchas personas asumen erróneamente que al tener una red privada están exentas de ser blanco de robos de información o ataques cibernéticos, como los ataques de denegación de servicio (DDoS), el phishing, poniendo en riesgo datos personales o la ingeniería social. No obstante, la realidad es que no es necesario tener una gran empresa, ni tener datos altamente sensibles para convertirse en víctima de ciberdelincuentes. Por lo tanto, este proyecto busca concienciar a las personas y proporcionar herramientas para crear una red mucho más segura.

Aunque muchas empresas se esfuerzan por concienciar sobre la importancia de prevenir los ciberataques a través de correos electrónicos y otros medios comúnmente usados, estas medidas no siempre se aplican debido a la falta de interés o conocimiento. De hecho, la mayoría de los ciberataques con más riesgos suelen ocurrir al conectarse a una red privada que pertenece a un lugar comercial, además sus clasificaciones son diversas, uno de estos ataques es el “Man in the Middle”, consiste en que un ciberdelincuente se haga pasar por un servidor o una página web válida para que, de esta manera, robe credenciales o información importante.

Es fundamental comprender que, al conectarse a redes en lugares comerciales, los riesgos de robo de información aumentan, ya que se desconoce qué personas se encuentran

conectas a las mismas. Por tanto, no se puede garantizar que los datos no sufran algún tipo de vulneración, principalmente porque no se conoce el verdadero propósito que tienen las personas usuarias de la red.

El personal de los locales comerciales no es consciente del peligro que pueden tener sus clientes al estar conectados dentro de la misma red, por lo que es importante realizar una buena configuración dentro del servicio para que sus sistemas, datos y dispositivos no se encuentren en riesgo, logrando así mantener una buena seguridad en este entorno. Es importante identificar qué dispositivos de esta red son propios del lugar y cuál es su nivel de seguridad para que, de esta manera, sus dispositivos IoT no se encuentren expuestos a personas malintencionadas.

1.2. Planteamiento del problema

En la actualidad, los dispositivos IoT han revolucionado en numerosos aspectos de la vida cotidiana, ofreciendo comodidad y eficiencia en diversas tareas. Sin embargo, la seguridad de los usuarios no ha sido prioritaria para algunos de los creadores de estos dispositivos. Se ha observado que muchas de las vulnerabilidades presentes en estos dispositivos son el resultado de la falta de actualizaciones, contraseñas débiles, ignorar las políticas de seguridad y sistemas de autenticación poco seguros. Esta situación plantea un grave problema, ya que compromete la confidencialidad de los datos personales que transitan y son almacenados en estos dispositivos.

Se han reportado casos alarmantes, especialmente en cámaras de seguridad, donde la falta de medidas de seguridad adecuadas ha dado paso a intrusiones no autorizadas. Esto pone de manifiesto la importancia de contar con una red segura para proteger la privacidad de los usuarios y prevenir posibles incidentes Ciber-delictivos. Cabe mencionar que los proveedores son responsables de brindar seguridad a los usuarios que contratan sus servicios, en este caso los dueños de los locales comerciales. En varias ocasiones, también es importante mantener medidas de seguridad en algunos de los dispositivos más comunes, mucho más cuando se tiene un negocio, ya que se debe brindar la mayor seguridad posible a nivel físico, y tecnológico.

Otro problema común radica en la falta de conocimiento por parte de los usuarios sobre las vulnerabilidades a las que están expuestos al utilizar dispositivos IoT en sus redes. Es fundamental tomar conciencia de que el robo de datos y la usurpación de identidad son amenazas latentes, así como la posibilidad de que los datos personales sean utilizados de manera indebida. Estas prácticas se han vuelto cada vez más comunes debido a la conveniencia y la facilidad de manejo que ofrecen estos dispositivos.

1.3. Objetivos

1.3.1. Objetivo general

Realizar un análisis de vulnerabilidades en dispositivos IoT en la red de un negocio de la parroquia Machachi, que ayude a identificar posibles riesgos de seguridad que puedan comprometer la integridad de la red y la información manejada por el negocio.

1.3.2. Objetivos específicos

1. Identificar los dispositivos IoT conectados a la red, utilizando una matriz de observación.

2. Utilizar herramientas de escaneo y penetración disponibles en la distribución del sistema operativo Kali linux, para determinar los dispositivos IoT vulnerables dentro de la red local.

3. Analizar los resultados obtenidos para identificar las vulnerabilidades más críticas en los dispositivos IoT.

4. Realizar un ataque cibernético controlado, simulando un posible escenario de riesgo en el que podría estar expuesta la red del negocio.

5. Proponer soluciones viables para mitigar los riesgos a los que están expuestos los dispositivos IoT en la red.

1.4. Alcance

En el marco del presente trabajo de integración curricular, se procederá a identificar los dispositivos IoT conectados a la red local del negocio, del caso de uso del presente trabajo, mediante una matriz de observación con información de cada dispositivo.

Se evaluará vulnerabilidades presentes en los dispositivos IoT de la red, considerando aspectos relacionados con el hardware, para identificar posibles amenazas para la seguridad y la privacidad de los usuarios.

Se analizarán las buenas prácticas de seguridad vigentes en entornos comerciales para evaluar las implicaciones derivadas de la proliferación de dispositivos IoT y proponer medidas de seguridad, como configuraciones adecuadas en cada dispositivo para evitar posibles amenazas.

CAPÍTULO II- MARCO CONCEPTUAL Y TEÓRICO

2.1. Marco conceptual

El avance tecnológico ha alcanzado un nivel en el que la mayoría de las personas posee al menos un dispositivo inteligente, ya sea un Smart tv, un teléfono celular, una Tablet o un ordenador. Esta tendencia muestra un evidente crecimiento exponencial en los últimos años de los dispositivos u otros elementos del internet de las cosas (IoT). Sin embargo, esta proliferación de dispositivos conectados a redes domésticas, comerciales e industriales han planteado desafíos significativos en términos de seguridad.

Cuando se habla sobre el internet de las cosas (IoT) se hace referencia al ecosistema de dispositivos que se conectan entre si e intercambian datos en redes cableadas o inalámbricas. Este tipo de dispositivos incluyen Smartphones, ordenadores, electrodomésticos inteligentes o cualquier otro con características similares. (Canle, 2022)

Muchos de estos dispositivos son vulnerables a ataques cibernéticos por su diseño y configuración deficientes, lo que preocupa la privacidad de los datos y la seguridad. Dado que muchos de estos dispositivos contienen información personal sensible, se convierten en objetivos atractivos para los ciberdelincuentes.

Numerosos estudios y análisis han corroborado que los dispositivos IoT son susceptibles a una variedad de vulnerabilidades, como contraseñas débiles, falta de actualizaciones de seguridad, configuraciones por defecto inseguras y la carencia de mecanismos de autenticación robustos. Estos riesgos representan una amenaza seria para la seguridad a nivel individual como a nivel de red.

Por consiguiente, el análisis de vulnerabilidades en dispositivos de este tipo se ha convertido en un área de investigación crucial. Esta labor permite encontrar, comprender y mitigar las vulnerabilidades presentes en los dispositivos, garantizando la seguridad y la privacidad de los usuarios, así como la integridad de las redes en las que operan.

2.2. Marco Teórico

2.2.1. Seguridad de la información

Proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción de los recursos informáticos de una organización, es decir que administren el riesgo para garantizar el correcto funcionamiento ininterrumpido de esos recursos. (Voutssas, 2010)

2.2.2. Análisis de vulnerabilidades y pruebas de seguridad

Proceso que nos ayudará a detectar las vulnerabilidades existentes en los sistemas de nuestra empresa, muy probablemente a tiempo antes de que puedan materializarse. Este se encarga de detectar, listar, analizar y priorizar las vulnerabilidades. (Cruz, 2021)

2.2.3. Internet de las cosas (IoT)

Proceso que permite conectar los elementos físicos cotidianos al internet: desde los objetos domésticos comunes, como las bombillas de luz, hasta los recursos para la atención de la salud, como los dispositivos médicos; las prendas y los accesorios personales inteligentes; e incluso los sistemas de las ciudades inteligentes. (Red Hat, 2023)

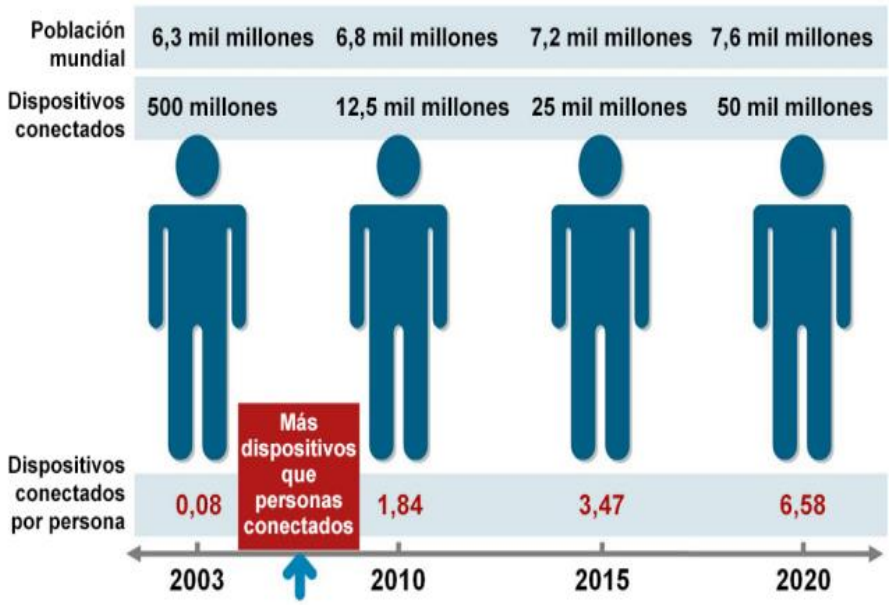
2.2.3.1. Definición y evolución de internet de las cosas (IoT)

Las raíces de idc se pueden remontar al Instituto de Tecnología de Massachusetts (MIT), hasta llegar al trabajo del auto-id center. Este grupo, fundado en 1999, realizaba investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y las tecnologías de sensores emergentes. Los laboratorios de investigación estaban conformados por siete universidades

ubicadas en cuatro continentes, seleccionadas por auto-id center para diseñar la arquitectura de idc. (cisco, 2011)

El crecimiento explosivo de los smartphones y las tablet pc elevó a 12,5 mil millones en 2010 la cantidad de dispositivos conectados a internet, en tanto que la población mundial aumentó a 6,8 mil millones, por lo que el número de dispositivos conectados por persona es superior a 1 (1,84 para ser exactos) por primera vez en la historia. (Cisco, 2011)

Figura 1.
Internet de las cosas "nació" entre los años 2008 y 2009



Nota. Este grafico muestra los resultados de un estudio realizado para saber que cantidad de dispositivos se encontraban conectados al internet entre 2003 y 2008. Adaptado de internet de las cosas cómo la próxima evolución de internet lo cambia todo (p. 3), por d. Evans,2011, cisco Internet Business Solutions Group (IBSG)

Es así como el concepto de combinar las computadoras y las redes para controlar y monitorear diferentes dispositivos ha existido desde épocas pasadas. A finales de la década de 1970 ya se encontraban en el mercado sistemas disponibles que permitían monitorear medidores conectados a redes eléctricas de forma remota a través de líneas telefónicas. En la década de los 90, los avances de las tecnologías inalámbricas brindaron una solución en la difusión corporativa

e industrial “maquina a máquina” (m2m) con el fin de monitorear y operar diferentes equipos. La comunicación m2m es el paso siguiente de la conexión de uno a uno o conexión de una máquina a otra; en la actualidad el termino m2m se refiere a la comunicación entre maquinas remotas para el intercambio de información. El objetivo principal es recopilar los datos que son transmitidos por la red, además, usa secuencias de eventos para ejecutar acciones de forma automática entre las maquinas que están conectadas; sirve como base para la inteligencia artificial y el internet de las cosas. (Rose et al., 2015)

El internet de las cosas en la actualidad es considerado como una verdadera revolución tecnológica, en especial en el área de las comunicaciones. Se trata de una red inteligente entre dispositivos que permiten el intercambio de información y comunicación entre ellos, capaces de procesar y gestionar órdenes que son programadas y monitoreadas por las personas (Espina Suárez & Gómez Hormaza, 2021).

Los dispositivos IoT han dejado de ser un mercado minorista; la tendencia de tener todos los dispositivos interconectados en conjunto con el bajo costo en la fabricación de las tecnologías impulsa a gran medida su popularidad. Además, se visualiza que en los próximos años este hecho vaya en incremento de la mano con la implementación del espacio de direcciones ipv6 y el despliegue de la nueva tecnología 5g en todas las redes móviles (Meneghello, Calore, Zucchetto, Polese, & Zanella, 2019).

De forma básica, se tienen tres capas: capa perceptiva, capa de red, capa de procesamiento y capa de aplicación. Cada capa tiene su función particular y, por lo tanto, cada una conlleva sus propias amenazas. Sin embargo, son dependientes la una de la otra, y si se quiere decir que una capa es segura, las otras también deben serlo.

Capa perceptiva: es conocida como la capa de sensores y, como su nombre lo indica, es la encargada de detectar, capturar y recopilar datos por medio de diversos sensores como lo son gps, rfid, zigbee, etc.

Capa de red: se encarga de la transmisión confiable de los datos; ocurre el enrutamiento y/o reenvío de información a través de internet, y, al igual que la capa de red de TCP/IP, también puede tener amenazas de seguridad comunes como lo son: espionaje de información, daño en la confidencialidad o integridad de los datos, ataque dos, man-in-the-middle, invasión de virus, entre otros.

Capa de procesamiento: se encarga de obtener los datos de la capa de red y realizar una toma de decisiones inteligente y control basado en la computación en la nube y las tecnologías de minería de datos. La información en la capa de procesamiento puede garantizar la interoperabilidad y la escalabilidad.

Capa de aplicación: es la más diversa y compleja de las capas IoT. Dado que existen una gran cantidad de fabricantes y productos, no hay un estándar en la creación de las aplicaciones. Esta capa es la que permite acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos; no actúa directamente con el usuario ya que suele interactuar con programas que facilitan la interacción y terminan siendo intuitivos.

2.2.3.2. Importancia de la seguridad en dispositivos IoT.

Debido a la gran cantidad de dispositivos IoT conectados a la red, los ciberdelincuentes han desarrollado una brecha de ataque cada vez más extensa, basta con encontrar alguna vulnerabilidad en un dispositivo para cometer algún tipo de delito informático al poner en evidencia información delicada y confidencial de los usuarios (Arias Silva, 2019).

Existen varias razones, por la cual, los riesgos de seguridad del internet de las cosas en la actualidad suponen el reto más importante para los usuarios y fabricantes:

- El número de dispositivos IoT crece de manera exponencial y los fabricantes de dispositivos instalan sensores IoT en todos los aparatos electrónicos, coches, bombillas, tomacorrientes, refrigeradores, entre otros electrodomésticos. Estos sensores permiten a

los dispositivos conectarse a internet para comunicarse con los sistemas informáticos para su control y programación.

- Los dispositivos IoT, además de proporcionarnos numerosas y novedosas funciones y capacidades, introducen posibles vulnerabilidades de seguridad. Por esta razón, la tecnología IoT tiene que ser sometida periódicamente a mantenimiento y protección a medida que se detectan nuevas amenazas.
- Muchos dispositivos no incluyen funciones de seguridad; la velocidad con la que los fabricantes sacan nuevos dispositivos al mercado provoca que dejen de lado el desarrollo de una interfaz de seguridad, y aunque los propios dispositivos son cada vez más sofisticados, a menudo no existen sistemas de seguridad IoT subyacentes para protegerlos.
- Inclusive si los dispositivos IoT incluyeran funciones de seguridad, los usuarios generalmente no dedican el tiempo suficiente para configurarlos y mantenerlos adecuadamente. Su fácil configuración y puesta en marcha hace que la gente se preocupe más por el ver que su dispositivo funcione sin novedad que configurar las funciones de seguridad o tal vez no saben cuánto afecta la seguridad a la privacidad de sus datos.

Como se pude apreciar, la aplicabilidad en este campo es ilimitada, lo que provoca que exista una feroz competencia entre las empresas de tecnología por quién lanza más rápido al mercado un dispositivo IoT. Este desarrollo prematuro de productos hace que se cometa errores en la implementación de la seguridad, en los casos en los que se implementa (Molina García, 2006).

Protección de datos en los dispositivos IoT: en los últimos años los dispositivos inteligentes han llevado la recopilación de datos a niveles que nunca se pensaba, lo que se ha convertido como la principal preocupación la privacidad del IoT. Por ejemplo, algunos altavoces y/o televisores graban conversaciones mientras ejecutan y escuchan órdenes; incluso han intentado obtener datos por medio de vías judiciales durante alguna investigación al pensar que un pequeño altavoz habría grabado una conversación incriminadora. Por otra parte, algunos distribuidores han tenido que retirar juguetes al descubrir que un osito o un artefacto graba voces de los niños y los envía al fabricante.

Patiño y Sánchez, (2021) plantean lo siguiente: los dispositivos IoT recopilan toda clase de datos del usuario, como distribución de horarios, hábitos de las personas, entre otras. Un estudio comprobó que, de 81 dispositivos de consumo IoT comunes 72 enviaban datos a terceros distintos del fabricante original. Eso no significa que se deba apagar cualquier tipo de conexión, los dispositivos necesitan por lo menos un punto de acceso a datos para realizar las funciones por las que lo compraron, sin embargo, cabe la posibilidad que el usuario tenga un mínimo control sobre el acceso del dispositivo.

2.2.3.3. Tipos de amenazas y vulnerabilidades en dispositivos IoT

Amenazas de malware: Como los dispositivos IoT no cuentan en su mayoría con medidas de seguridad, a los ciberdelincuentes no les resulta difícil acceder al sistema. Así como sucede con los equipos comunes como PCs, o teléfonos móviles, los dispositivos IoT son vías para una infección de malware. Algunos ciberdelincuentes han utilizado malware para transformar dispositivos IoT en medios para propagación de más malware, o para contribuir en ataques distribuidos de negación de servicio o simplemente un malware que permita el bloqueo del dispositivo.

Dispositivos secuestrados: las cámaras de seguridad que cuentan con escasa seguridad son foco principal de los ciberdelincuentes que buscan secuestrar dispositivos IoT. En varias ocasiones, se reciben advertencias falsas sobre misiles balísticos y amenazas de secuestros de menores de edad. Otros incidentes populares son voces que surgen de la cámara o desde otro dispositivo IoT conectado a la red, así como también, el control de dispositivos sensores que permiten regular la temperatura o controlar ciertos aspectos del hogar. Algunas de las situaciones son resultados de un mal comportamiento del usuario al realizar la configuración de la seguridad sin usar contraseñas robustas o la utilización de las mismas credenciales de acceso en todos los sitios. Los ciberdelincuentes tras robar estas contraseñas obtienen acceso a las aplicaciones que administran los dispositivos inteligentes; si sucede algo como esto, son muy pocas las aplicaciones que avisan si un tercero comienza a utilizar los dispositivos de la red.

Intrusión: Una vez que el ciberdelincuente ha logrado entrar en un dispositivo de Internet de las Cosas, o ya ha ingresado en la red a través de uno de estos dispositivos, recopilan datos privados sobre sus clientes y negocios, los cuales pueden llegar a ser vendidos.

Según López, (2022) menciona lo siguiente: los vectores de ataques más comunes utilizados por los ciberdelincuentes en los dispositivos IoT son:

- **Ataque de fuerza bruta:** Para obtener contraseñas, descubrir puertos abiertos (por ejemplo, al usar la aplicación telnet), o incluso el login y password de uno de los nodos para acceder a la red.
- **Ataque de negación de servicio (DDoS):** ataques que inhabilitan el sistema y le impiden realizar su función. Si un atacante conoce o adivina una secuencia de acciones (por ejemplo, una secuencia de voltajes en su módulo de alimentación) en un sensor que provoca que deje de tomar muestras; esto va a impedir que el sistema al que pertenece ese sensor realice su función. Por ejemplo, en un sistema de ayuda a la conducción en un vehículo en el que se toman muestras a través de una cámara que captura las imágenes de señales del tráfico. Si se inhabilita dicha cámara o se provoca un malfuncionamiento, el sistema de ayuda a la conducción no opera correctamente, incluso puede informar mal de señales con la velocidad máxima incorrecta, esto ocasiona que el conductor incremente la velocidad del vehículo en una zona que está limitada a menor velocidad, lo cual, llega a provocar que el conductor cometa una infracción y se vea obligado a pagar una multa por exceso de velocidad.

- **Acceso a uno de los nodos de la red:** El atacante, consciente de que la seguridad desde el exterior es probablemente más robusta que desde el interior, logra encontrar un punto o un nodo más débil con menos protección, acceder a dicho nodo para entrar en la red y una vez dentro realizar el ataque al nodo o al subsistema que desee. En este tipo de ataques, también, emplea uno de estos nodos, como una etapa más (trampolín) para cubrir el rastro del atacante, que perpetra un ciberataque a otro sistema y necesita ocultar su identidad y evitar que su IP sea rastreada al usar conexiones sucesivas a varios nodos de distintas redes.

En base a la investigación realizada por Patiño y Sánchez, (2021) mencionan lo siguiente: existen amenazas de seguridad en cada una de las capas descritas, amenazas en la captura de datos (capa perceptiva), en la transmisión de datos (capa de red), en el procesamiento de datos (capa de procesamiento) y por último en la aplicación. A continuación, se describen estas amenazas en cada una de esas capas.

- **Capa perceptiva:** La capa perceptiva puede realizar la percepción integral de la información. Los equipos de red sensores, como la identificación de radio frecuencias, los códigos bidimensionales y sensores, se usan para tecnologías integrales de detención, capturas y medición para recopilar y capturar información de cualquier momento y lugar, los dispositivos más vulnerables en esta capa evidenciamos los RFID, GPS y sensores, juntos a otros equipos en la protección integral de la capa perceptiva, una de las grandes amenazas que se evidencia en esta capa es la trasmisión de la información entre los nodos, se pueden involucrar nodos no autorizados y desviar esta trasmisión, en esta capa se realizan inspecciones de seguridad y autenticación periódica, se debe de construir un mecanismo de trasmisión seguro para la información en los nodos, así garantizar una información veraz.
- **Capa de red:** La función principal de la capa de red puede lograr una transmisión confiable de la información e información de datos segura, la transmisión a través de redes de comunicación móvil, redes informáticas y redes inalámbricas Las principales tecnologías de transmisión en la capa de transmisión incluyen: tecnología de cable a larga distancia, tecnología de comunicación inalámbrica y tecnología de comunicación de red, las amenazas que vemos en esta capa se da en el proceso de transmisión de datos, la capa de red se ve afectada por la propagación de información falsa de enrutamiento, reenvío selectivo / no reenvío, ataques de agujeros negros. Esto afectan los datos que no pueden ser transmitido de manera eficiente al destino e incluso puede dañar la red.

- **Capa de procesamiento:** La principal función de la capa de red es desarrollar el procesamiento inteligente de información para analizar y procesar los datos e información masiva. El propósito de esta práctica radica en la toma de decisiones y un control inteligentes; basado en la computación de la nube la información de datos en la capa de procesamiento puede garantizar la interoperabilidad y la escalabilidad, para reducir amenazas al momento del procesamiento y así elegir la información con una máxima seguridad, este procedimiento hace que la información de datos proporcione un entorno seguro y servicios eficientes.
- **Capa de aplicación:** La información procesada por la capa de procesamiento se transmite a la capa de aplicación. Esta información es heterogénea. Cuando se procesa una gran cantidad de datos variados en la plataforma de la nube, se debe establecer un sistema unificado y una plataforma de sistema para mejorar la seguridad de la computación en la nube en la capa de aplicación. Estos ataques se dan en el acceso y autenticación de la red de la nube, la información de datos debe fortalecer el acceso y la gestión de autorizaciones; tomándolo en cuenta, se puede reforzar la protección de varios tipos de información de datos.

2.2.3.4. Seguridad en el diseño y desarrollo de dispositivos IoT

Red Hat (2022) define los siguientes aspectos:

- **Utilice un solo panel de control:** obtenga información sobre todos los dispositivos del IoT en su red desde un mismo lugar.
- **Controle el acceso:** permita que solamente los dispositivos del IoT autorizados se unan a la red y limite su acceso.
- **Supervise la red:** conozca en detalle las actividades que son "normales", para poder detectar los comportamientos extraños que requieran una investigación profunda.
- **Automatice las respuestas:** disminuya el tiempo de exposición a las amenazas con las respuestas automáticas. Si descubre que un dispositivo conectado presenta puntos vulnerables durante la supervisión, las medidas automáticas para contener y solucionar el problema reducirán el riesgo de comprometer la seguridad.

2.2.4. Herramientas y técnicas de análisis de vulnerabilidades.

El análisis de vulnerabilidades es el estudio profundo de un sujeto u objeto o situación, teniendo como meta el conocimiento de sus fundamentos, principios y motivos, así como su creación y demás cosas enlazadas.

2.2.4.1. Nessus

Una de las principales herramientas que se utilizará es nessus. Arboledas, (2013) define que nessus es un programa de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio, nessusd, que realiza el escaneo en el sistema objeto, y nessus, el cliente que muestra el avance e informa sobre el estado de los escaneos. En operación normal, nessus comienza escaneando los puertos con nmap para buscar puertos abiertos y después intentar varios exploits para atacarlo. Opcionalmente, los resultados del escaneo pueden ser exportados como informes en varios formatos, como texto plano, xml, html y latex. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

Esta herramienta ayudará a identificar las vulnerabilidades presentes dentro de cada dispositivo que se encuentre conectado a la red. El reconocimiento de estas a su vez aportará fundamentalmente a identificar cuáles son los puertos, protocolos, entre otros elementos involucrados en el proceso. De esta manera, será posible buscar herramientas o configuraciones que permitan una menor vulnerabilidad y de igual manera evitar que se presenten ataques mediante estas brechas de seguridad.

Esta herramienta es usada normalmente al realizar auditorías informáticas o cuando el sistema se encuentra en un proceso de creación de parches, los cuales ayudan en gran escala a reconocer qué métodos se deberían usar para mitigar vulnerabilidades. De esta forma, se logrará que los determinados dispositivos IoT sean mucho más seguros y no se conviertan en un riesgo para el negocio involucrado y así, evitar pérdidas económicas.

2.2.4.2. Nmap

Nmap, (s.f.) Menciona que: Nmap (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes ip "crudos" («raw», n. Del t.) En formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, así como docenas de otras características. Aunque generalmente se utiliza nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

2.2.4.3. Wireshark

Es un analizador de protocolos de red, llamado analizador de paquetes, diseñado para proporcionar visibilidad del tráfico que se produce en una red o entre máquinas. Permite mirar desde el interior de la red y examinar los detalles del tráfico inalámbrico y por cable a varios niveles: desde la información a nivel de conexión hasta los bits que hacen un determinado paquete y los datos que contiene. (Abba, 2023)

2.2.4.4. Kali linux

> Sistema operativo gratuito orientado a la seguridad informática y a las pruebas de penetración, cuenta con diversas herramientas clasificadas para que el pentester tenga a su disponibilidad toda una suite en donde realizar toda clase de testeo interno y externo. (parra, 2020)

2.2.5. Seguridad cibernética y prácticas de seguridad en dispositivos conectados

Según la definición de elastic, (s.f) tenemos lo siguiente: la ciberseguridad es la práctica de proteger redes, sistemas, dispositivos y otra información confidencial de ataques deliberados y uso no autorizado. Es un esfuerzo holístico que requiere alineación entre tu gente, tus procesos y tus tecnologías. Con el fin de proteger los activos, los empleados, los clientes y los usuarios de una organización, los expertos en ciberseguridad de hoy utilizan una variedad de estrategias para proteger sus datos. En un mundo cada vez más digital, proteger la ciberseguridad es de suma importancia para garantizar lo siguiente:

- **Privacidad y seguridad personal:** la ciberseguridad protege la privacidad y la seguridad personal al evitar que los hackers exploten la información de identificación, directa o indirectamente.
- **Protección de activos financieros y propiedad intelectual:** una ciberseguridad deficiente puede permitir que los ciberdelincuentes roben información comercial confidencial, como secretos comerciales, diseños de productos y otra información patentada.
- **Preservación de las operaciones comerciales:** los ciberataques pueden interrumpir el funcionamiento normal de una organización, al interrumpir los servicios y causar pérdidas de gran alcance.
- **Integridad reputacional:** una filtración de datos u otro incidente de ciberseguridad puede dañar la reputación de una organización, lo que dificulta atraer y retener clientes, inversionistas y empleados.
- **Resiliencia y confiabilidad de la infraestructura crítica:** los ciberataques hacia los sistemas de infraestructura crítica, sistemas de energía, transporte y agua, pueden afectar la seguridad de las personas y el funcionamiento de la sociedad.
- **Garantía legal y de cumplimiento:** una ciberseguridad deficiente puede ocasionar el incumplimiento de las normas de privacidad de datos, lo que genera problemas normativos, sanciones financieras y otras consecuencias.

2.2.6. Conciencia de seguridad y educación del usuario

La educación y la concienciación en seguridad cibernética son fundamentales en la sociedad actual. La protección de la información personal, el uso responsable de internet, la

prevención del ciberacoso y la conciencia sobre el impacto de acciones en línea son aspectos clave de la seguridad cibernética. Al promover una cultura de seguridad cibernética y brindar a las personas los conocimientos y las habilidades necesarias, se puede crear un entorno en línea más seguro y protegido para todos. La educación y la concienciación en seguridad cibernética deben ser una prioridad tanto para adultos como para jóvenes, ya que todos están conectados en este mundo digital en constante evolución. (Herrero, 2023)

2.2.7. Tipos de ataques

2.2.7.1. Exploit

Tipo de ataque que aprovecha las vulnerabilidades de aplicaciones, redes o hardware para obtener el control de un sistema o robar los datos que están en la red. Cuando en un software existen errores de programación los intrusos pueden utilizan estas debilidades para controlar o infectar un sistema. (Olaya, 2021)

2.2.7.2. Denegación de servicio (DDoS)

El objetivo de este ataque es inhabilitar un sistema, una aplicación o una red bloqueando los servicios que ofrece, de esta manera impide que los usuarios legítimos puedan tener acceso. Es causado por la saturación de los puertos con flujo de información, esto genera la sobrecarga de los servidores e imposibilita que presten los servicios. (Olaya, 2021)

2.2.7.3. Ingeniería social (Social Engineering)

Acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Estas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo. (Medina, 2015)

2.2.7.4. Pruebas de Penetración (penetration testing)

Las pruebas de penetración están enfocadas en intentar explotar dichas vulnerabilidades con el objetivo de descubrir qué tan críticas son y hasta dónde podría afectar a la organización si un ciberdelincuente llegara a realizar un ataque. (Cruz, 2021)

2.2.8. Protección de datos

Práctica que consiste en proteger la información digital contra el acceso no autorizado, la corrupción o el robo durante todo su ciclo de vida. Es un concepto que comprende todos los aspectos de la seguridad de la información, desde la seguridad física del hardware y los dispositivos de almacenamiento hasta los controles administrativos y de acceso, así como la seguridad lógica de las aplicaciones de software. También incluye las políticas y los procedimientos de la organización. (IBM, s.f.)

2.2.8.1. Medidas para protección de datos

Estrategias y procesos de seguridad que ayudan a proteger datos confidenciales frente a corrupción, vulneración y pérdida. Las amenazas a datos confidenciales incluyen incidentes de vulneración y pérdida de datos. (Microsoft, s.f.)

2.2.8.2. Políticas de privacidad

Declaración que las empresas tienen en su sitio web que informa a los usuarios sobre la recopilación, el procesamiento, la protección y el uso de sus datos privados. (Trevino, Cutler & Guccione, 2023)

2.2.8.3. Control de accesos

Elemento esencial de seguridad que determina quién puede acceder a ciertos datos, aplicaciones y recursos, y en qué circunstancias. De la misma forma que las claves y listas de invitados con aprobación previa protegen los espacios físicos, las directivas de control de acceso protegen los espacios digitales. (Microsoft, s.f.)

2.2.9. Seguridad informática

Medidas, herramientas y controles preventivos que deben considerar las personas, organizaciones y tecnologías para proteger la información, para preservar la confidencialidad, autenticidad e integridad de los datos. (Olaya, 2021)

2.2.9.1. Seguridad de red

Área de la ciberseguridad que se centra en la protección de las redes informáticas frente a las ciber amenazas. Tiene tres objetivos principales: impedir el acceso no autorizado a los recursos de la red, detectar y neutralizar los ciberataques y las violaciones de la seguridad en curso, y garantizar que los usuarios autorizados tengan un acceso seguro a los recursos de la red que necesitan, cuando los necesitan. (IBM, s.f.)

2.2.9.2. Vulnerabilidad

Es una debilidad en el software o sistema de configuración que puede ser explotada. Las vulnerabilidades pueden venir de muchas formas, pero más a menudo están asociados con parches faltantes. (Medina, 2015)

2.2.9.3. Riesgo

Los riesgos informáticos son problemas, que pueden afectar a los sistemas de información o a los equipos informáticos. Si no se tienen las medidas adecuadas para precautelar los datos y la información, dichos riesgos se pueden presentar por vulnerabilidades y amenazas

en un futuro, por lo que se pueden clasificar en: riesgos de integridad, de acceso, de relación, de utilidad, de infraestructura. (Solarte, 2015)

2.2.9.4. Ciberataques

Los ciberataques son intentos de robar, exponer, alterar, deshabilitar o destruir los activos de otra persona a través del acceso no autorizado a los sistemas informáticos. (IBM, s.f.)

2.2.9.5. Amenazas

Posibilidad de que pueda llegar a ocurrir cualquier evento que atente contra la seguridad de la información, se genera una amenaza cuando se saca provecho de una vulnerabilidad en un sistema y puede generarse a través de ingeniería social o cuando no se da una correcta capacitación y concientización de los usuarios (Martínez, 2018).

2.2.9.6. Ataques Informáticos

Aprovechamiento de las vulnerabilidades del software o hardware para ingresar con el objetivo de destruir, exponer, alterar, inhabilitar un sistema informático o la información que almacena o la red. Además, puede definirse como un intento organizado por varias o una sola persona para causar daños a un sistema informático o una red. Un ataque usualmente puede ser provocado por delincuentes informáticos que realizan espionaje, suplantación de identidad entre otros (Ecured, s.f).

2.2.9.7. Autenticación

Proceso de verificar la identidad de alguien o algo. La autentificación suele tener lugar mediante la comprobación de una contraseña, un token de hardware o algún otro dato que demuestre la identidad. (Cloudflare, s.f.)

2.2.9.8. Autorización

Los permisos que un usuario tiene en cualquier concepto, según el rol que cumple en cualquier lugar, con acceso a información o actividades especificar dentro de un lugar.

2.2.9.9. Protocolos de red

Un protocolo de red hace referencia a normativas y criterios que fijan como deben comunicarse entre sí los distintos componentes de un sistema informático. (Limones, 2021)

2.2.10. Privacidad y confidencialidad

Según Gómez, (2023) menciona que la confidencialidad de la información es el principio que garantiza que los datos personales o la información sensible no sea divulgada a terceros; es decir, que solo puede ser conocida por el emisor y el receptor.

El acuerdo de confidencialidad obliga a que dicho tipo de información sea protegida para evitar que las personas no autorizadas puedan tener acceso a ella. Este principio se aplica en las bases de datos de las empresas, las relaciones de las compañías con sus empleados y clientes, los datos médicos, en el ámbito jurídico, entre otros escenarios.

Por otro lado, la National Cybersecurity Alliance, (2022) menciona que: la intimidad es un derecho: generalmente se entiende como el derecho a no ser observado o molestado por otros. Esto incluye el derecho a que cierta información no sea observada.

Además, es importante tener presente lo descrito por la National Cybersecurity Alliance, (2022) en el que menciona que la privacidad de los datos se ha convertido en una cuestión definitoria de nuestra era digital. Aunque no te importe demasiado, miles de empresas de todo el mundo pagan mucho dinero por conocerte a través de estos datos.

Sus datos en línea pueden clasificarse de ciertas maneras. En primer lugar, hay información personal como su nombre, fecha de nacimiento y número de la seguridad social. También hay información importante sobre usted, como su historial médico y los números de su tarjeta de crédito.

Una vez comprendidos estos dos conceptos relevantes, se puede entender que la privacidad y la confidencialidad de los datos son sumamente importantes. En una era de transformación digital, muchas personas desconocen cómo proteger sus datos personales, lo que puede representar un problema significativo para las empresas. Si no se aplican controles adecuados y no se utilizan herramientas y dispositivos de seguridad dentro de la red empresarial, los datos críticos pueden quedar expuestos a cibercriminales.

2.2.11. Transparencia y responsabilidad

La transparencia cobra especial relevancia en un mundo digital donde el flujo e intercambio de información es continuo y, con frecuencia, sobre todo en el caso de la publicidad en línea, existe la dificultad de conocer el lugar en el que las páginas web ubican los datos de los usuarios, a su vez, existe la dificultad de saber por quién y con qué finalidad se están recogiendo esos datos (considerando 58 rgpd). La transparencia permitirá que las personas estén debidamente informadas en este aspecto. (cuevas, 2018)

Es importante comprender que la transparencia es fundamental dentro del tratamiento de datos personales, es de alta responsabilidad el dar a conocer que se hace con los datos, si no se toman las medidas precautelares necesarias, se puede causar una vulneración de los datos, teniendo así un mal uso de los datos personales expuestos.

2.2.12. Ley de protección de datos personales

La protección de datos personales surge como un mecanismo jurídico para proteger el derecho a la vida privada de las personas en la era de las tecnologías de la información. Sus

objetivos principales son: definir a los datos personales; determinar quién es el responsable del tratamiento de datos; regular cuestiones esenciales del tratamiento de datos, tales como la conservación, el acceso, la seguridad, la confidencialidad; y determinar el nivel de protección adecuado para la transferencia de datos personales a otros países. (Enríquez, 2017)

En base a la ley orgánica de protección de datos personales, (2021) se tienen los siguientes artículos a considerar:

CAPÍTULO III: METODOLOGÍA APLICADA

3.1. Diseño de investigación

En primera instancia se aplicará una investigación documental – bibliográfica, llamada investigación teórica que permite analizar diferentes fuentes, que ayudarán a sustentar los conceptos puntuales del marco conceptual y teórico Se investigarán todos los temas relacionados a ciberseguridad, vulnerabilidades, ataques, hacking ético, entre otros temas relacionados al trabajo.

Adicionalmente, se empleará una investigación aplicada tecnológica, para poner en práctica herramientas para analizar las vulnerabilidades en los dispositivos IoT que se encuentran dentro de la red del lugar comercial, del caso de estudio de este trabajo y proponer mejores practicas para proteger la información del negocio y de los clientes. Esta etapa se realizará acudiendo físicamente a la empresa, para revisar vulnerabilidades en los dispositivos IoT, utilizando las herramientas disponibles en el sistema operativo Kali Linux.

3.2. Matriz de observación

Se ha diseñado una matriz de observación para recolectar la información principal de los dispositivos IoT de la empresa del caso de uso del presenta trabajo, con datos como:

- Fabricante del dispositivo,
- Modelo
- Tipo
- IP

En la primera visita se obtuvo la siguiente información:

Tabla 1.
Dispositivos IoT en red

Fabricante	Modelo	Tipo	Dirección ip
Xiaomi	Poco x5 5g	Móvil	192.168.1.200
Lg	Webos 2.0 pro-smart tv	Tv	192.168.1.249
Tv	Tv box 4k mxq pro	Tv box	192.168.1.132
Tcl	S5400a	Tv	192.168.1.115
	Desktop	Pc	192.168.1.169
Hp	Hp notebook - 15-bs662tu	Pc	192.168.1.221

En la matriz se describen los dispositivos IoT que tiene el negocio del caso de estudio, con los datos del fabricante, el modelo, tipo de dispositivo y la dirección IP. De los dispositivos de esta lista se analizaran uno a uno las vulnerabilidades.

3.3. Proceso de hacking ético

Para el presente trabajo de titulación se llevará a cabo un proceso de hacking ético en base al artículo "hacking ético: una herramienta para la seguridad informática" realizado por Edwin Medina, en el cual nos propone una serie de etapas que se deben llevar a cabo en el hacking ético como una herramienta para prevenir y reparar posibles vulnerabilidades de los dispositivos. Pasos por realizar:

Alcance de la prueba: en esta etapa se define cuáles son los activos que se van a evaluar. Se realiza una evaluación de los riesgos que se pueden llegar a tener, se define la fecha, hora y duración que tendrá la prueba, se definirá que actividades se usaran y que herramientas que usaran para poder lograr con el objetivo definido.

Descubrimiento y enumeración: aquí se define que tipo de estrategia se usará, si se realizara mediante un reconocimiento pasivo o un reconocimiento activo por el cual se determinará qué métodos se usarán para obtener la recolección de información necesaria.

Algunas de las herramientas utilizadas para hacer este descubrimiento y enumeración son: whols, nslookup, maltego, arin (american registry of internet numbers), traceroute, smart/whois, sam spade, entre otras. (Engebretson, 2011)

Mapeo de vulnerabilidades: aquí se encentrarán todas las vulnerabilidades que el proceso arrojará como resultado al realizar la ejecución de la herramienta en cuestión.

Ingeniería social: este término hace referencia a todas las formas en la que una persona puede obtener información de otra mediante técnicas psicológicas. Su objetivo es la obtención de información de valor, con la cual se puede realizar la suplantación de identidad, a la vez que permitiría obtener credenciales para diferentes sistemas. Según el artículo anteriormente mencionado, nos da como dato lo siguiente:

Algunas herramientas utilizadas en la ingeniería social son: vigilancia, pishing, suplantación de identidad, llamada telefónica, correo electrónico, sms, entre otras.

Explotación: esta etapa es en la cual se realiza el ingreso a la infraestructura y se logra escalar al punto de controlar las máquinas y poder ejecutar los cambios que se quieran realizar, al igual que recolectar toda la información que sirva como pruebas para el levantamiento de los reportes. Todo este procedimiento se lo debe realizar con el permiso del usuario administrador ya que, de lo contrario, se lo consideraría acto ilegal.

Documentación y reporte: en esta sección se presentan todos los resultados obtenidos, se realizan las observaciones y recomendaciones para las vulnerabilidades que se han encontrado, ya que el objetivo principal de este proceso es evitar perdida de datos, intrusiones y mejoras en la seguridad de la red y los sistemas que se tiene, en cada uno de los activos que se encontraron dentro de la red.

3.4. Consentimiento informado

El consentimiento informado es el proceso mediante el cual se comunica a todos los involucrados los detalles del estudio, incluidos los procedimientos, riesgos y beneficios. Es fundamental especificar claramente el propósito del estudio, los métodos utilizados, su duración y las medidas de confidencialidad para proteger la identidad de los participantes. Además, se deben respetar los derechos de los involucrados conforme a la ley de protección de datos.

Justamente para iniciar este trabajo se recibió de los propietarios de la empresa de estudio, la aceptación voluntaria para aplicar los procedimientos expuestos.

CAPÍTULO IV: EJECUCIÓN DE HERRAMIENTAS PARA EL ANÁLISIS DE VULNERABILIDADES EN DISPOSITIVOS IOT

4.1. Introducción

En el presente capítulo se realizará el análisis de vulnerabilidades en cada dispositivo de la red, con uso de las herramientas anteriormente mencionados, como son:

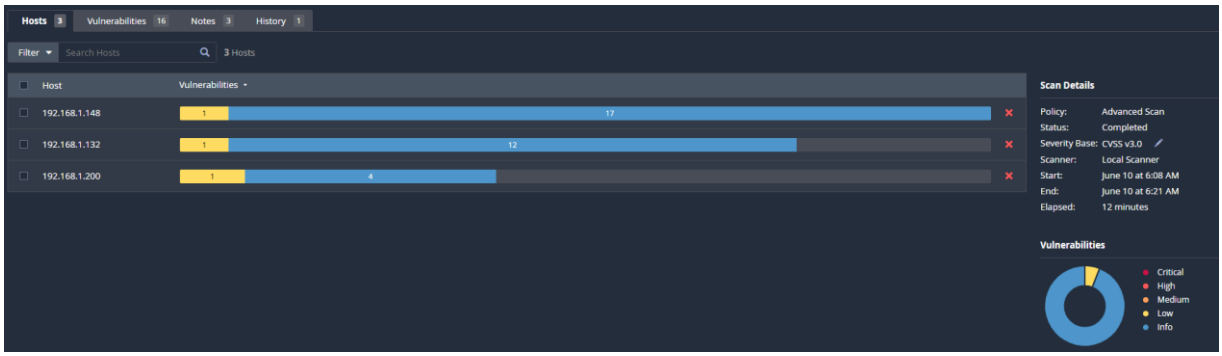
- Nessus
- Wireshark
- Nmap
- Kali linux

El fin del uso de estas herramientas, es identificar las posibles vulnerabilidades existentes, para analizar y categorizar las vulnerabilidades, en base a los resultados que estos nos presentan.

4.2. Ejecución de herramientas para identificar vulnerabilidades en dispositivos IoT.

Figura 2.

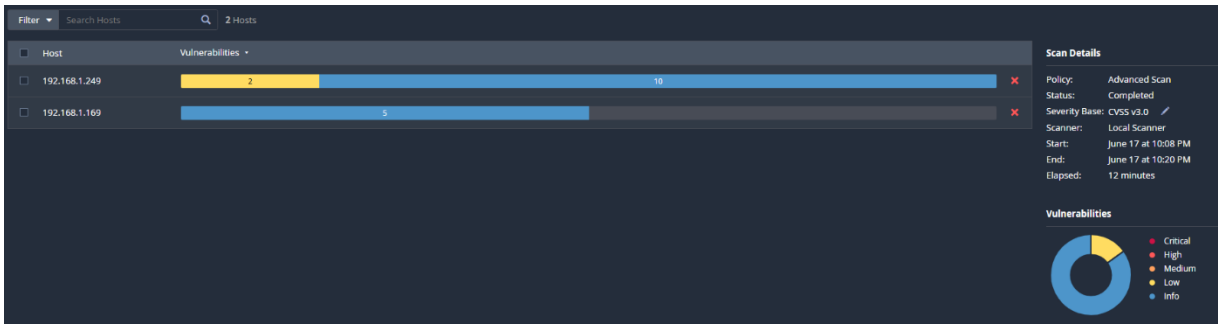
Análisis de vulnerabilidades con la herramienta Nessus



Instalada la herramienta Nessus en una PC del negocio, se ejecuta dentro de la red del negocio. En la figura 2 se visualizan los hosts que se encuentran con vulnerabilidades de todo tipo, criticas, de nivel alto, mediano y bajo.

Figura 3.

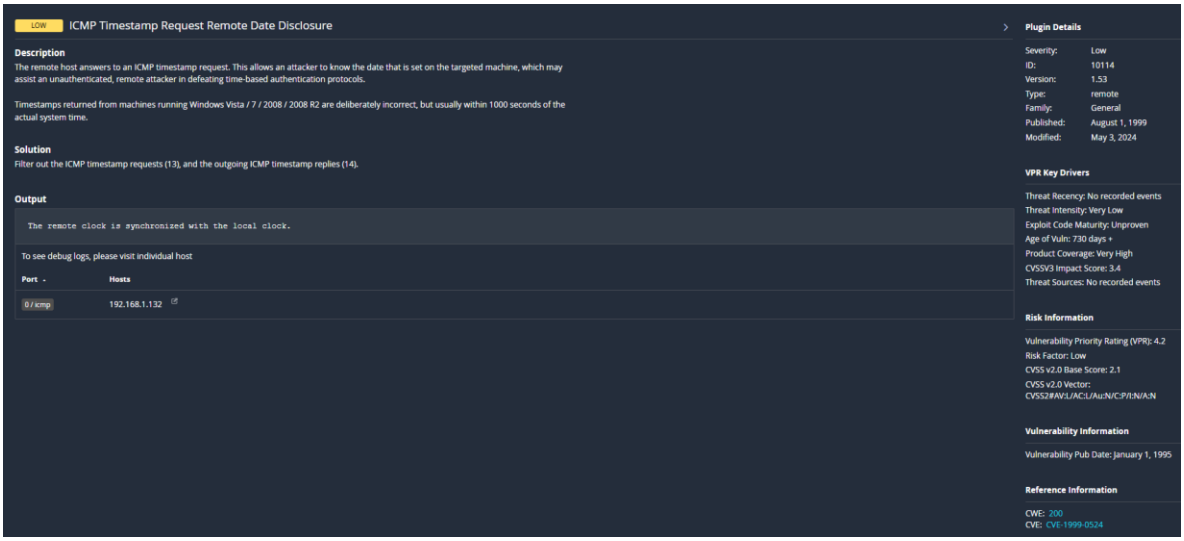
Análisis de vulnerabilidades con la herramienta Nessus



En la figura 3 se visualizan las vulnerabilidades encontradas en los hosts, PC y TV LG, que son vulnerabilidades de todo tipo, criticas, de nivel alto, mediano y bajo.

Figura 4.

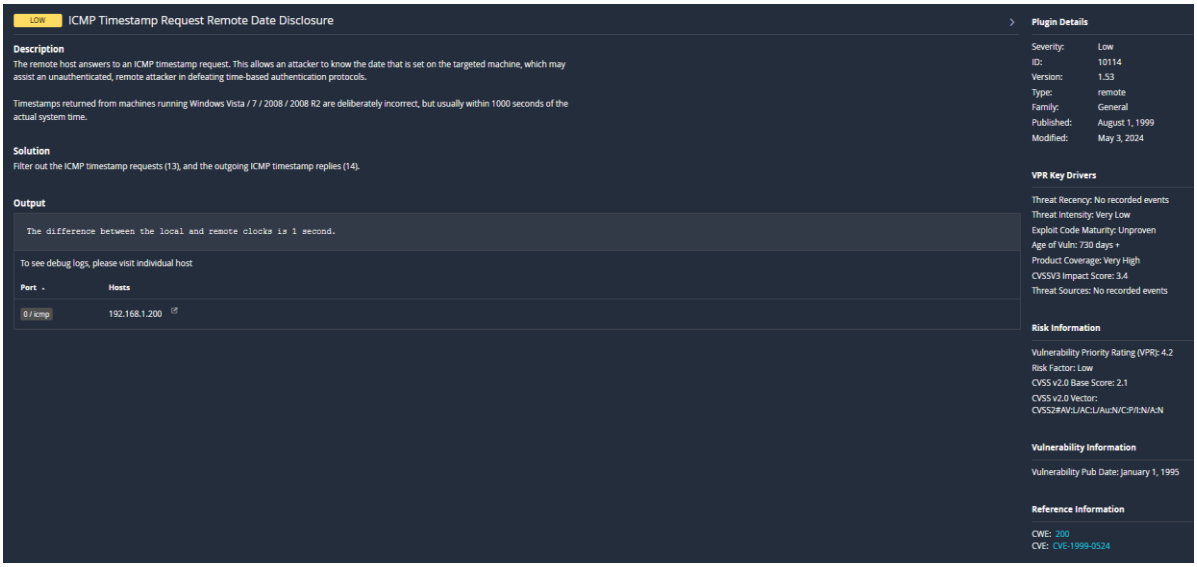
Análisis de vulnerabilidades con la herramienta Nessus – TV Box*nota.*



En la figura 4, se visualiza que, a más de la descripción de la vulnerabilidad encontrada, se despliega su solución e identifica el puerto en el que se presenta la vulnerabilidad en el dispositivo TV Boxnota.

Figura 5.

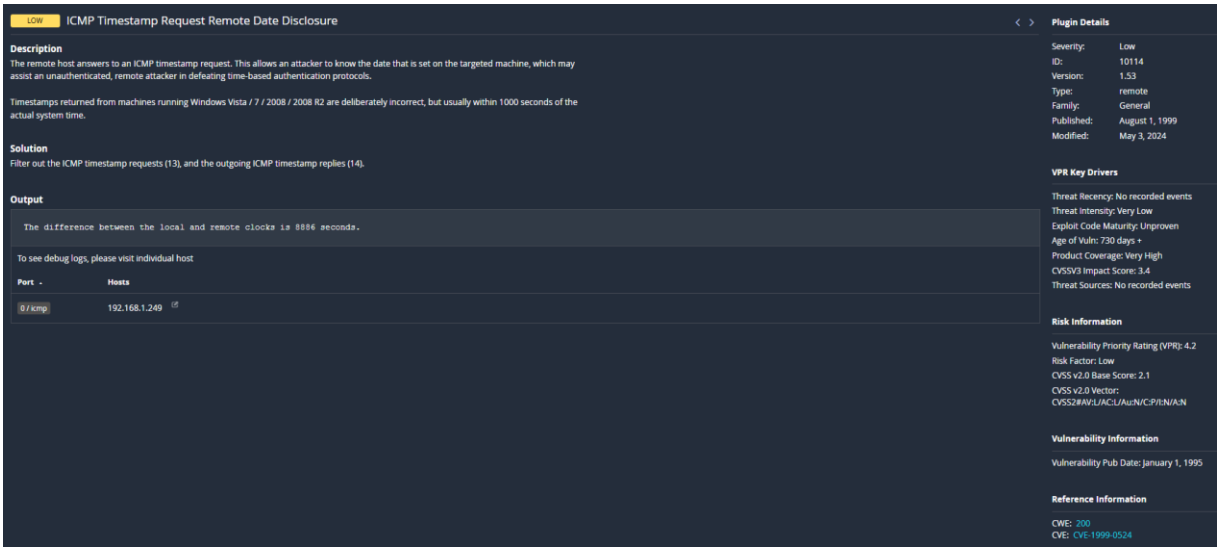
Análisis de vulnerabilidades con la herramienta nessus – Celular



En la figura 5, se visualiza que, a más de la descripción de la vulnerabilidad encontrada, se despliega su solución e identifica el puerto en el que se presenta la vulnerabilidad en el Celular.

Figura 4.

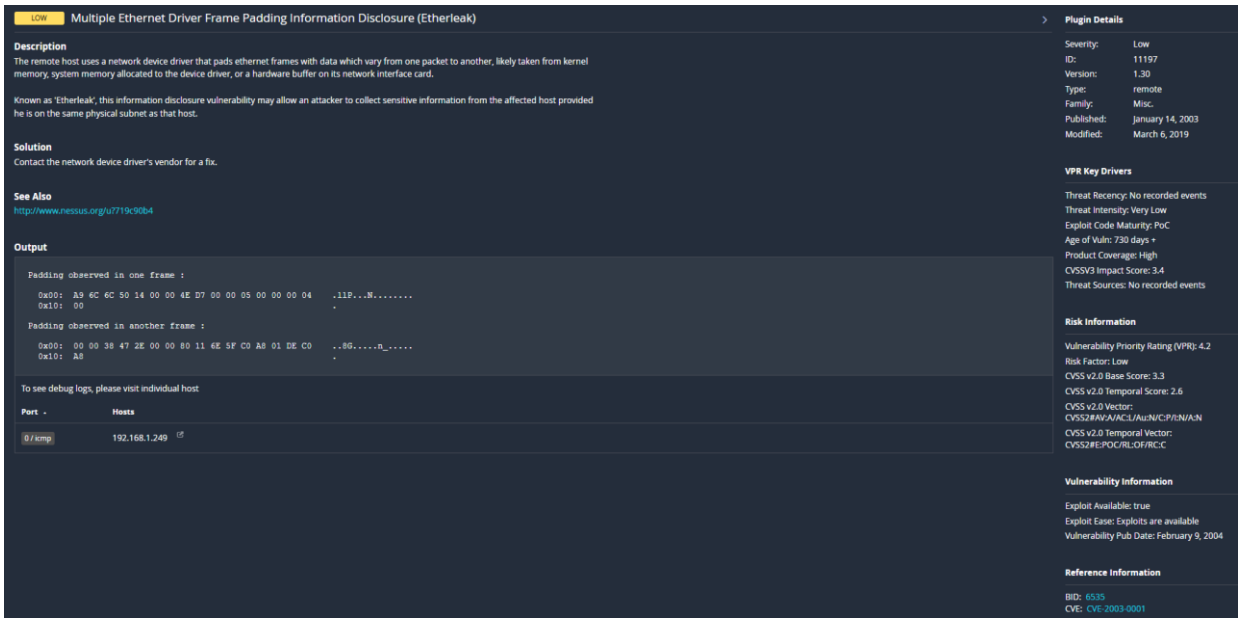
Análisis de vulnerabilidades con la herramienta Nessus – TV LG



En la figura 6, se visualiza que, a más de la descripción de la vulnerabilidad encontrada, se despliega su solución e identifica el puerto en el que se presenta la vulnerabilidad en el dispositivo *TV LG*.

Figura 5.

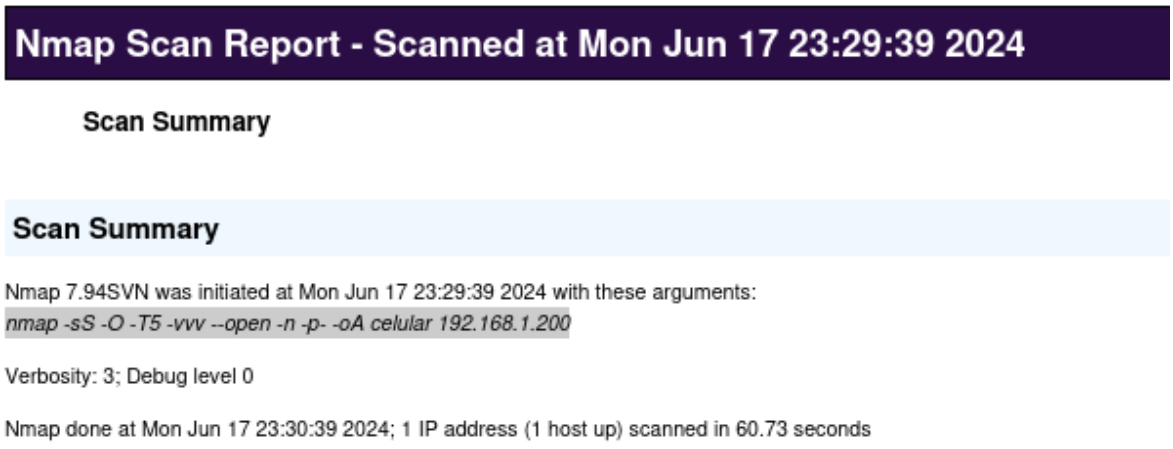
Análisis de vulnerabilidades con la herramienta Nessus – TV LG



En la figura 7, se visualiza que, a más de la descripción de la vulnerabilidad encontrada, se despliega su solución e identifica el puerto en el que se presenta la vulnerabilidad en el dispositivo *TV LG*.

Figura 6.

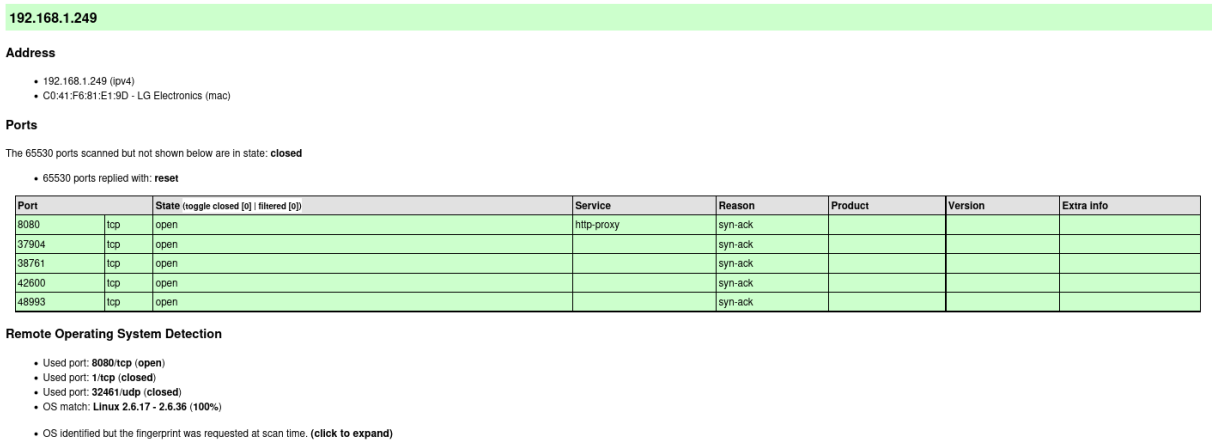
Resultado de reconocimiento de puertos abiertos – Celular



En la figura 8 se visualiza el resultado de reconocimiento de puertos abiertos, no se encuentran puertos abiertos en el dispositivo celular.

Figura 7.

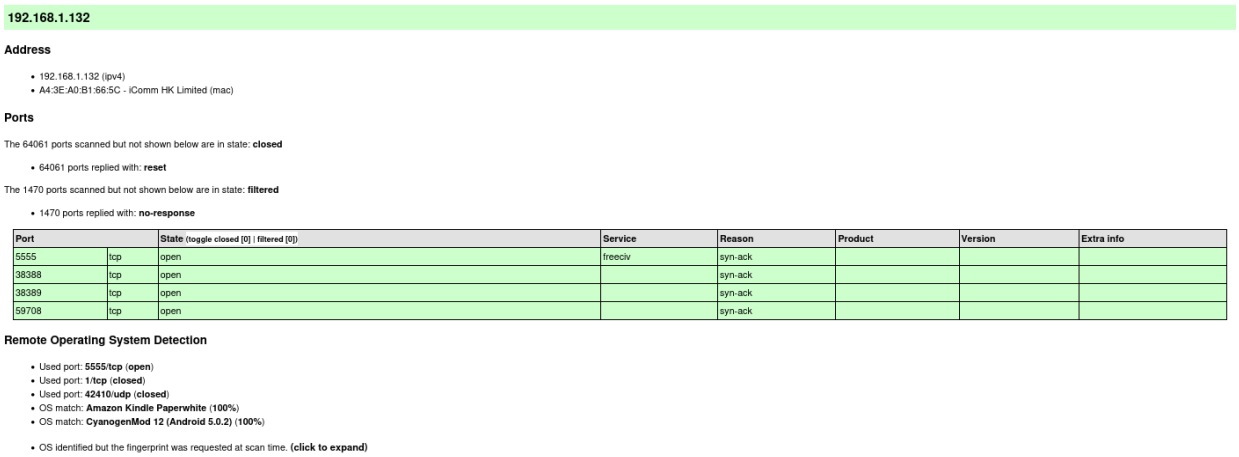
Resultado de reconocimiento de puertos abiertos – TV LG



En la figura 9, se visualiza el resultado de la herramienta Nmap, donde existen puertos abiertos del dispositivo TV LG.

Figura 8.

Resultado de reconocimiento de puertos abiertos– TV BOX



192.168.1.132

Address

- 192.168.1.132 (ipv4)
- A4:3E:A0:B1:66:5C - iComm HK Limited (mac)

Ports

The 64061 ports scanned but not shown below are in state: **closed**

- 64061 ports replied with: **reset**

The 1470 ports scanned but not shown below are in state: **filtered**

- 1470 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
5555	tcp	open	freeciv	syn-ack			
38388	tcp	open		syn-ack			
38389	tcp	open		syn-ack			
59708	tcp	open		syn-ack			

Remote Operating System Detection

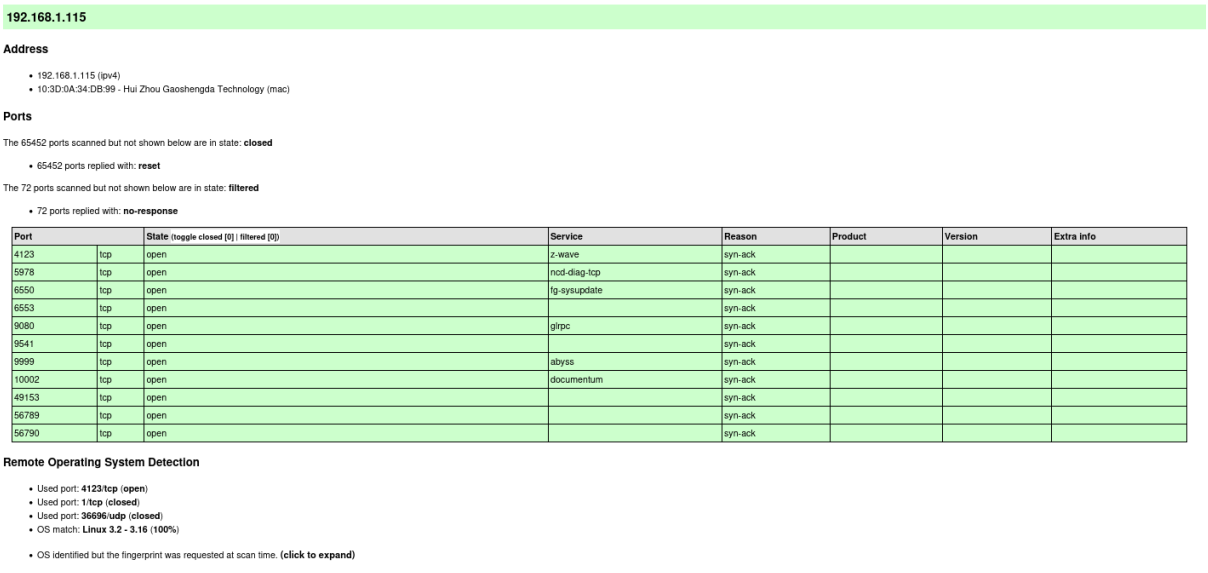
- Used port: **5555/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **42410/udp** (**closed**)
- OS match: **Amazon Kindle Paperwhite** (**100%**)
- OS match: **CyanogenMod 12 (Android 5.0.2)** (**100%**)

- OS identified but the fingerprint was requested at scan time. **(click to expand)**

En la figura 10, se visualiza el resultado de la herramienta Nmap, donde existen puertos abiertos del dispositivo TV BOX.

Figura 9.

Resultado de reconocimiento de puertos abiertos – TV TCL



192.168.1.115

Address

- 192.168.1.115 (ipv4)
- 10:3D:0A:34:DB:99 - Hui Zhou Gaoshengda Technology (mac)

Ports

The 65452 ports scanned but not shown below are in state: **closed**

- 65452 ports replied with: **reset**

The 72 ports scanned but not shown below are in state: **filtered**

- 72 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
4123	tcp	open	z-wave	syn-ack			
5978	tcp	open	ncd-diag-tcp	syn-ack			
6550	tcp	open	fg-sysupdate	syn-ack			
6553	tcp	open		syn-ack			
9080	tcp	open	glrpc	syn-ack			
9541	tcp	open		syn-ack			
9999	tcp	open	abyss	syn-ack			
10002	tcp	open	documentum	syn-ack			
49153	tcp	open		syn-ack			
56789	tcp	open		syn-ack			
56790	tcp	open		syn-ack			

Remote Operating System Detection

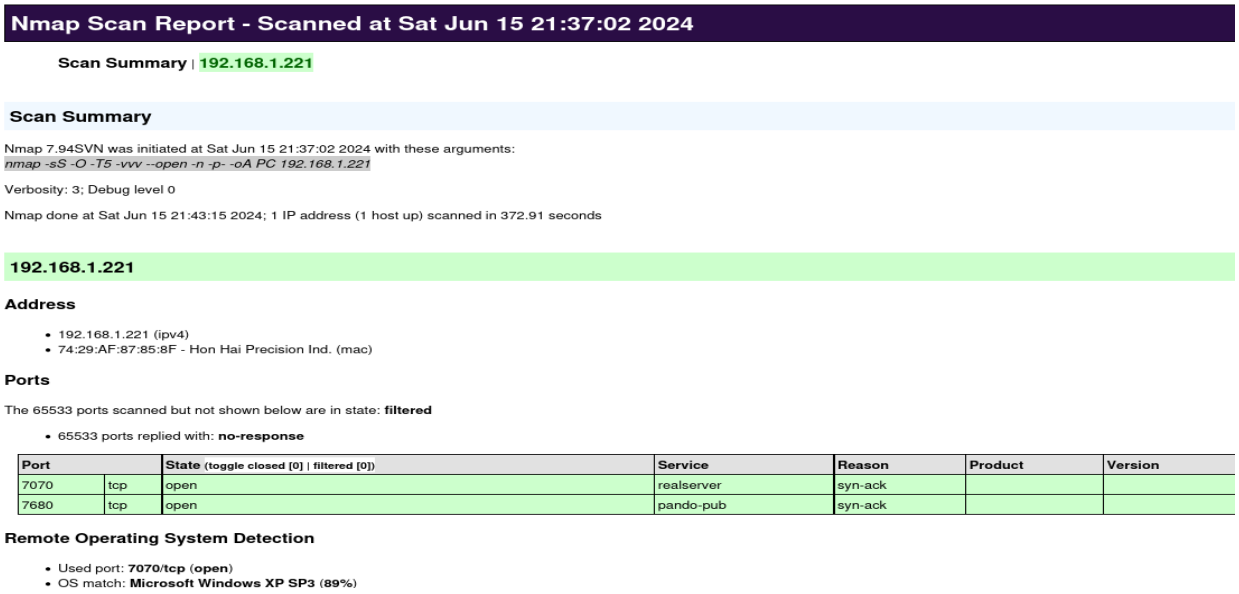
- Used port: **4123/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **36696/udp** (**closed**)
- OS match: **Linux 3.2 - 3.16** (**100%**)

- OS identified but the fingerprint was requested at scan time. **(click to expand)**

En la figura 11, se visualiza el resultado de la herramienta Nmap, donde existen puertos abiertos del dispositivo TV TCL.

Figura 10.

Resultado de reconocimiento de vulnerabilidades – PC HP



Nmap Scan Report - Scanned at Sat Jun 15 21:37:02 2024

Scan Summary | **192.168.1.221**

Scan Summary

Nmap 7.94SVN was initiated at Sat Jun 15 21:37:02 2024 with these arguments:
nmap -sS -O -T5 -vvv --open -n -p- -oA PC 192.168.1.221

Verbosity: 3; Debug level 0

Nmap done at Sat Jun 15 21:43:15 2024; 1 IP address (1 host up) scanned in 372.91 seconds

192.168.1.221

Address

- 192.168.1.221 (ipv4)
- 74:29:AF:87:85:8F - Hon Hai Precision Ind. (mac)

Ports

The 65533 ports scanned but not shown below are in state: **filtered**

- 65533 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version
7070	tcp	open	realserver	syn-ack		
7680	tcp	open	pando-pub	syn-ack		

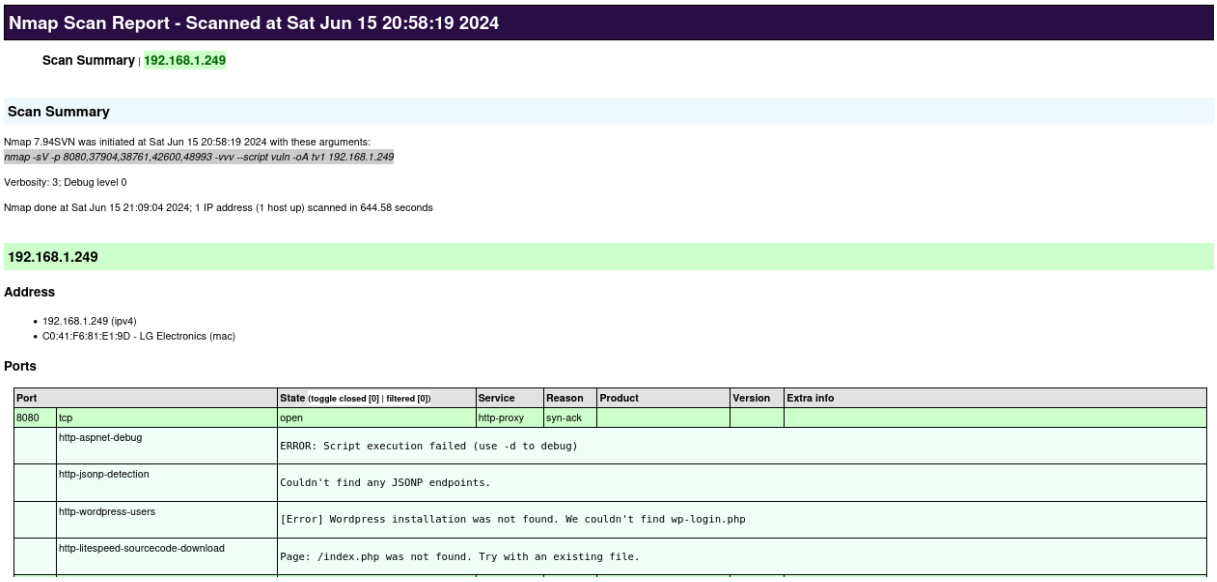
Remote Operating System Detection

- Used port: **7070/tcp** (**open**)
- OS match: **Microsoft Windows XP SP3** (**89%**)

En la figura 12, se visualiza el resultado de la herramienta Nmap, existiendo vulnerabilidades en el dispositivo PC HP.

Figura 11.

Resultado de reconocimiento de vulnerabilidades – TV LG



Nmap Scan Report - Scanned at Sat Jun 15 20:58:19 2024

Scan Summary | 192.168.1.249

Scan Summary

Nmap 7.94SVN was initiated at Sat Jun 15 20:58:19 2024 with these arguments:
nmap -sV -p 8080,37904,38761,42600,48993 -vvv --script vuln -oA tv1 192.168.1.249

Verbosity: 3; Debug level 0

Nmap done at Sat Jun 15 21:09:04 2024; 1 IP address (1 host up) scanned in 644.58 seconds

192.168.1.249

Address

- 192.168.1.249 (ipv4)
- C0:41:F6:81:E1:9D - LG Electronics (mac)

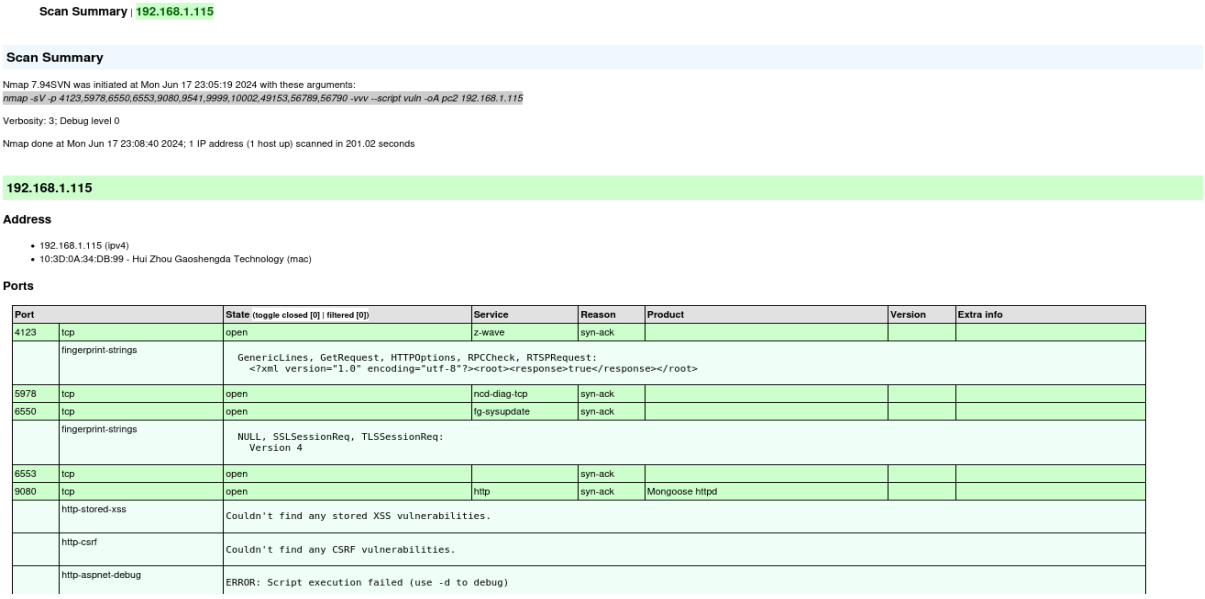
Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
8080	tcp	open	http-proxy	syn-ack			
	http-aspnet-debug	ERROR: Script execution failed (use -d to debug)					
	http-jsonp-detection	Couldn't find any JSONP endpoints.					
	http-wordpress-users	[Error] Wordpress installation was not found. We couldn't find wp-login.php					
	http-litespeed-sourcecode-download	Page: /index.php was not found. Try with an existing file.					

En la figura 13, se visualiza el resultado de la herramienta Nmap, existiendo vulnerabilidades en el dispositivo TV LG.

Figura 12.

Resultado de reconocimiento de vulnerabilidades – TV TCL



Scan Summary | 192.168.1.115

Scan Summary

Nmap 7.94SVN was initiated at Mon Jun 17 23:05:19 2024 with these arguments:
nmap -sV -p 4123,5978,6550,6553,9080,9541,9999,10002,49153,56789,56790 -vvv --script vuln -oA pc2 192.168.1.115

Verbosity: 3; Debug level 0

Nmap done at Mon Jun 17 23:08:40 2024; 1 IP address (1 host up) scanned in 201.02 seconds

192.168.1.115

Address

- 192.168.1.115 (ipv4)
- 10:3D:0A:34:DB:99 - Hui Zhou Gaoshengda Technology (mac)

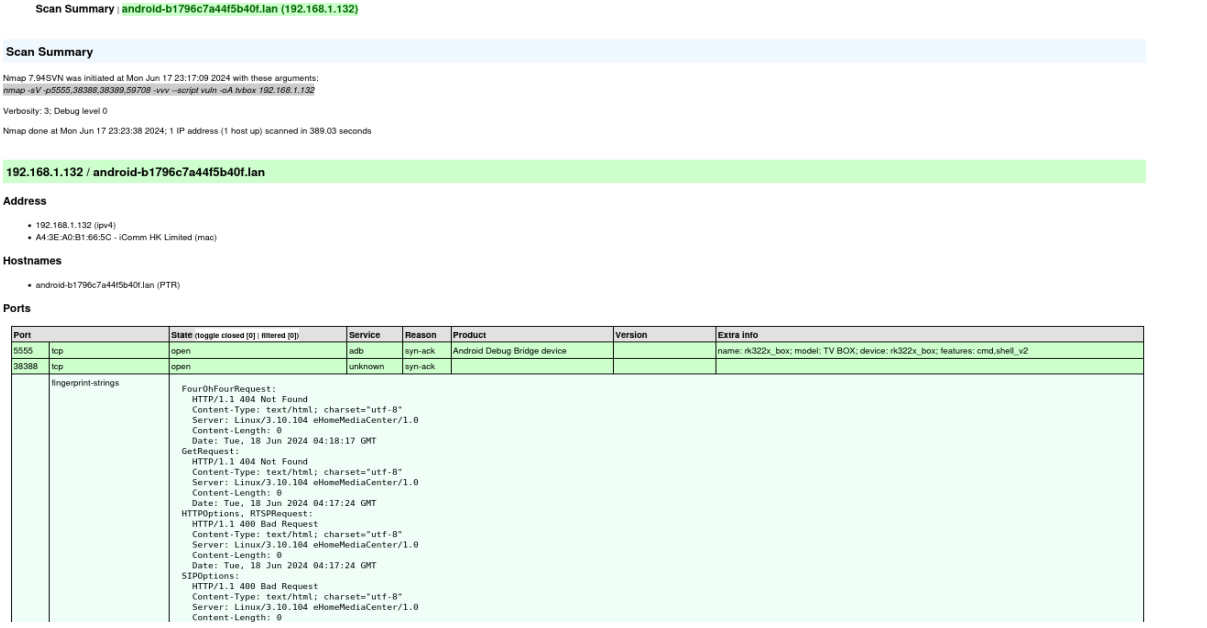
Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
4123	tcp	open	z-wave	syn-ack			
	fingerprint-strings	GenericLines, GetRequest, HTTPOptions, RPCCheck, RTSPRequest: <?xml version="1.0" encoding="utf-8"?><root><response>true</response></root>					
5978	tcp	open	ncd-diag-tcp	syn-ack			
6550	tcp	open	fg-sysupdate	syn-ack			
	fingerprint-strings	NULL, SSLSessionReq, TLSSessionReq: Version 4					
6553	tcp	open		syn-ack			
9080	tcp	open	http	syn-ack	Mongoose httpd		
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.					
	http-csrf	Couldn't find any CSRF vulnerabilities.					
	http-aspnet-debug	ERROR: Script execution failed (use -d to debug)					

En la figura 14, se visualiza el resultado de la herramienta Nmap, existiendo vulnerabilidades en el dispositivo TV TCL.

Figura 13.

Resultado de reconocimiento de vulnerabilidades – TV BOX



Scan Summary | android-b1796c7a44f5b40f.lan (192.168.1.132)

Scan Summary

Nmap 7.94SVN was initiated at Mon Jun 17 23:17:09 2024 with these arguments:
nmap -sV -p5555,38388,38389,59708 -vvv --script vuln -oA tvbox 192.168.1.132

Verbosity: 3; Debug level 0

Nmap done at Mon Jun 17 23:23:38 2024; 1 IP address (1 host up) scanned in 389.03 seconds

192.168.1.132 / android-b1796c7a44f5b40f.lan

Address

- 192.168.1.132 (ipv4)
- A4:3E:A0:B1:66:5C - iComm HK Limited (mac)

Hostnames

- android-b1796c7a44f5b40f.lan (PTR)

Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
5555	tcp	open	adb	syn-ack	Android Debug Bridge device		name: rk322x_box; model: TV BOX; device: rk322x_box; features: cmd,shell_v2
38388	tcp	open	unknown	syn-ack			
	fingerprint-strings	FourOhFourRequest: HTTP/1.1 404 Not Found Content-Type: text/html; charset="utf-8" Server: Linux/3.10.104 eHomeMediaCenter/1.0 Content-Length: 0 Date: Tue, 18 Jun 2024 04:18:17 GMT GetRequest: HTTP/1.1 404 Not Found Content-Type: text/html; charset="utf-8" Server: Linux/3.10.104 eHomeMediaCenter/1.0 Content-Length: 0 Date: Tue, 18 Jun 2024 04:17:24 GMT HTTPOptions, RTSPRequest: HTTP/1.1 400 Bad Request Content-Type: text/html; charset="utf-8" Server: Linux/3.10.104 eHomeMediaCenter/1.0 Content-Length: 0 Date: Tue, 18 Jun 2024 04:17:24 GMT SIPOptions: HTTP/1.1 400 Bad Request Content-Type: text/html; charset="utf-8" Server: Linux/3.10.104 eHomeMediaCenter/1.0 Content-Length: 0					

En la figura 15, se visualiza el resultado de la herramienta Nmap, existiendo vulnerabilidades en el dispositivo TV BOX.

4.3. Descripción de las vulnerabilidades identificadas.

En base a los resultados obtenidos, se creó una tabla que muestra los hallazgos más comunes en los puertos de los dispositivos analizados.

Es importante mencionar que las herramientas utilizadas dieron como resultado vulnerabilidades distintas entre ellas. Además, se evaluó la gravedad de estas vulnerabilidades en cada dispositivo y se identificaron los afectados.

Tabla 2.
Vulnerabilidades encontradas en los dispositivos IoT del negocio caso de estudio

Nombre de la vulnerabilidad	Descripción	Ip	Dispositivo	Puertos
Desbordamientos de búfer basados en pila múltiple rce	**Cve-2012-5958:** existe un desbordamiento de búfer basado en pila en la función unique_service_name() del archivo ssdp/ssdp_server.c al manejar solicitudes del protocolo simple de descubrimiento de servicios (ssdp), activado al copiar el urn devicetype. Un atacante remoto no autenticado puede explotar esto mediante una solicitud ssdp especialmente diseñada para ejecutar código arbitrario. **Cve-2012-5959:** hay un desbordamiento de búfer basado en pila en la función unique_service_name() del archivo ssdp/ssdp_server.c al manejar solicitudes ssdp, activado al copiar el udn antes de dos puntos. Un atacante remoto no autenticado puede explotar esto mediante una solicitud ssdp especialmente diseñada para ejecutar código arbitrario.	192.168.1.115	S5400a	1900 / udp / ssdp

	Cve-2012-5960: se presenta un desbordamiento de búfer basado en pila en la función unique_service_name() del archivo ssdp/ssdp_server.c al manejar solicitudes ssdp, activado al copiar el udn antes de la cadena '::upnp'. Un atacante remoto no autenticado puede explotar esto mediante una solicitud ssdp especialmente diseñada para ejecutar código arbitrario.			
	Cve-2012-5961, cve-2012-5962, cve-2012-5963, cve-2012-5964, cve-2012-5965: existen varias condiciones de desbordamiento de búfer basadas en pila en la función unique_service_name() del archivo ssdp/ssdp_server.c debido a una validación incorrecta de los campos udn, devicetype y servicetype al analizar solicitudes ssdp. Un atacante remoto no autenticado puede explotar estos problemas mediante solicitudes ssdp especialmente diseñadas para ejecutar código arbitrario.			
Divulgación remota de fecha de solicitud de marca de tiempo icmp	El host remoto responde a una solicitud de marca de tiempo icmp. Esto permite a un atacante conocer la fecha que se establece en la máquina de destino, lo que puede ayudar a un atacante remoto no autenticado a vencer los protocolos de autenticación basados en el tiempo. las marcas de tiempo devueltas por equipos que ejecutan windows vista / 7 / 2008 / 2008 r2 son deliberadamente incorrectas, pero generalmente dentro de los 1000 segundos de la hora real del sistema.	192.168.1.115 192.168.1.132 192.168.1.249 192.168.1.200	S5400a Tv box 4k mxq pro Webos 2.0 pro-smart tv Poco x5 5g	0 / icmp

Divulgación de información sobre relleno de tramas de controladores ethernet múltiples (etherleak)	El host remoto utiliza un controlador de dispositivo de red que rellena las tramas ethernet con datos que varían de un paquete a otro, probablemente tomados de la memoria del núcleo, de la memoria del sistema asignada al controlador del dispositivo o de un búfer de hardware en su tarjeta de interfaz de red. conocido como 'etherleak', esta vulnerabilidad de divulgación de información puede permitir a un atacante recopilar información confidencial del host afectado siempre que esté en la misma subred física que ese host.	192.168.1.249	Webos 2.0 pro-smart tv	0 / icmp
Ataque dos de slowloris	Slowloris intenta mantener muchas conexiones abiertas al servidor objetivo el mayor tiempo posible mediante el envío de solicitudes parciales, agotando los recursos del servidor y causando denegación de servicio (dos).	192.168.1.132	Tv box 4k mxq pro	5555 / tcp, 38388 / tcp, 38389 / tcp, 59708 / tcp
Android debug bridge device	Adb (android debug bridge) es una herramienta que permite la comunicación entre un dispositivo android y una computadora para realizar diversas operaciones como depuración, instalación de aplicaciones, y otros comandos del sistema.	192.168.1.132	Tv box 4k mxq pro	5555/tcp
Unknown service on port 38388, port 38389	Servicio desconocido que responde con el servidor ehomemediacenter en linux.	192.168.1.132	Tv box 4k mxq pro	38388/tcp 38389/tcp
Jetty http server	Servidor http jetty que responde en el puerto 59708, identificado como potencialmente vulnerable al ataque slowloris dos.	192.168.1.132	Tv box 4k mxq pro	59708/tcp
Z-wave controller	Controlador z-wave que responde en el puerto 4123.	192.168.1.115	S5400a	4123/tcp
Ncd diagnostic tcp service	Servicio de diagnóstico tcp de ncd en el puerto 5978.			5978/tcp
Fortiguard system update	Servicio de actualización del sistema fortiguard en el puerto 6550.			6550/tcp

Http server (mongoose httpd)	Servidor http mongoose en el puerto 9080, con múltiples verificaciones de vulnerabilidades incluyendo csrf, xss, y otros.			9080/tcp
Websocket++ server	Servidor websocket++ en el puerto 9541, versión 0.7.0.			9541/tcp
Abyss web server	Servidor web abyss en el puerto 9999.			9999/tcp
Documentum content server	Servidor de contenido documentum en el puerto 10002.			10002/tcp
Portable sdk for upnp devices	Upnp sdk en el puerto 49153, versión 1.6.22, ejecutándose en linux 3.10.40.			49153/tcp
Lg lw5700 tv upnp	Servicio upnp del televisor lg lw5700 en el puerto 37904 y 48993.	192.168.1.249	Webos 2.0 pro-smart tv	37904/tcp 48993/tcp
Http server (mongoose httpd)	Servidor http mongoose en el puerto 38761, con múltiples verificaciones de vulnerabilidades incluyendo csrf, xss, y otros.			38761/tcp 42600/tcp

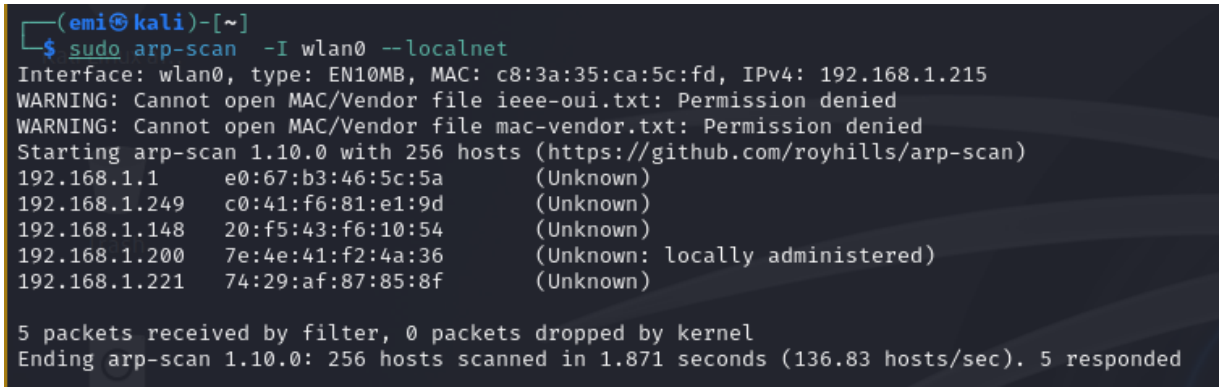
En la tabla 2 se describen las vulnerabilidades encontradas al ejecutar las herramientas nmap y nessus. En la tabla se presenta el nombre de la vulnerabilidad, una explicación detallada, la IP, el tipo de dispositivo y los puertos.

4.4. Ataque simulado

4.4.1. Etapa de escaneo y enumeración

En la figura 16 se ejecuta la herramienta arp-scan la cual escanea la red local para obtener la lista de los dispositivos conectados. Esta herramienta realiza un envío de paquetes ARP el cual permite mapear las direcciones MAC e IP dentro de una red local

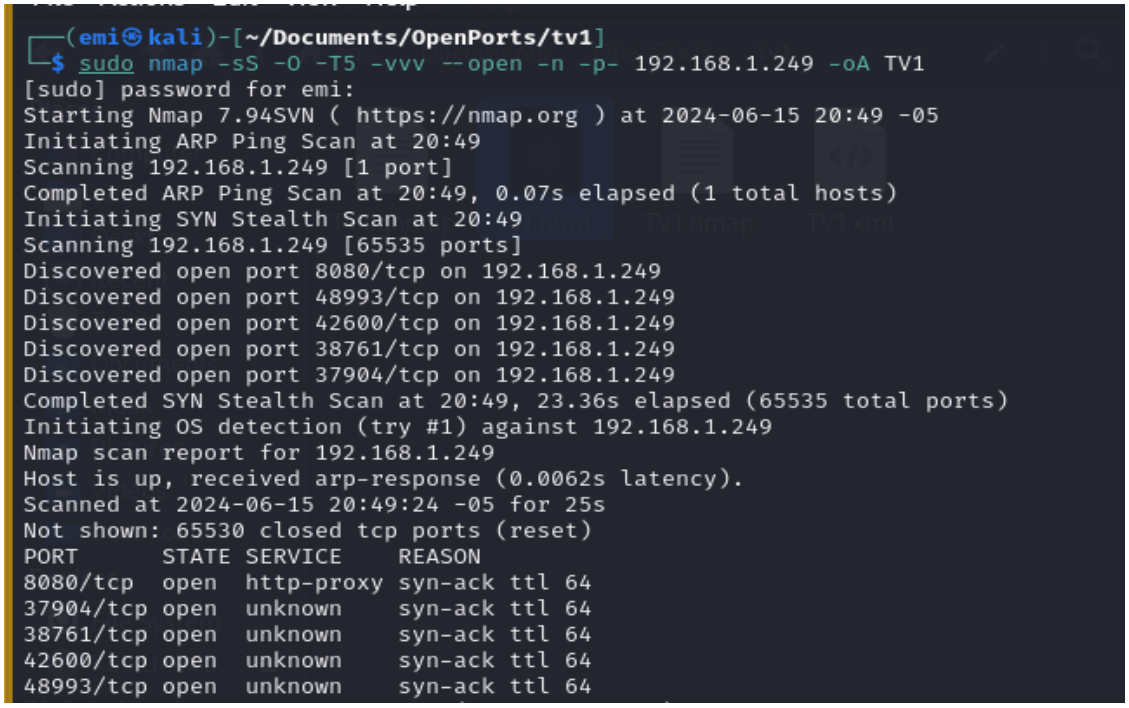
Figura 14.
Identificación de dispositivos conectados a la red con la herramienta arp-sacn



En la figura 16 se visualizan los dispositivos que se encuentran conectados a la red inalámbrica con su dirección IP y la MAC Adress.

En la figura 17, se realiza el escaneo intensivo de la uno de los televisores de la red mediante el uso de la herramienta Nmap. El comando que se visualiza realiza el reconocimiento de puertos y su estado, al igual que identifica que tipo de sistema operativo tiene el dispositivo escaneado.

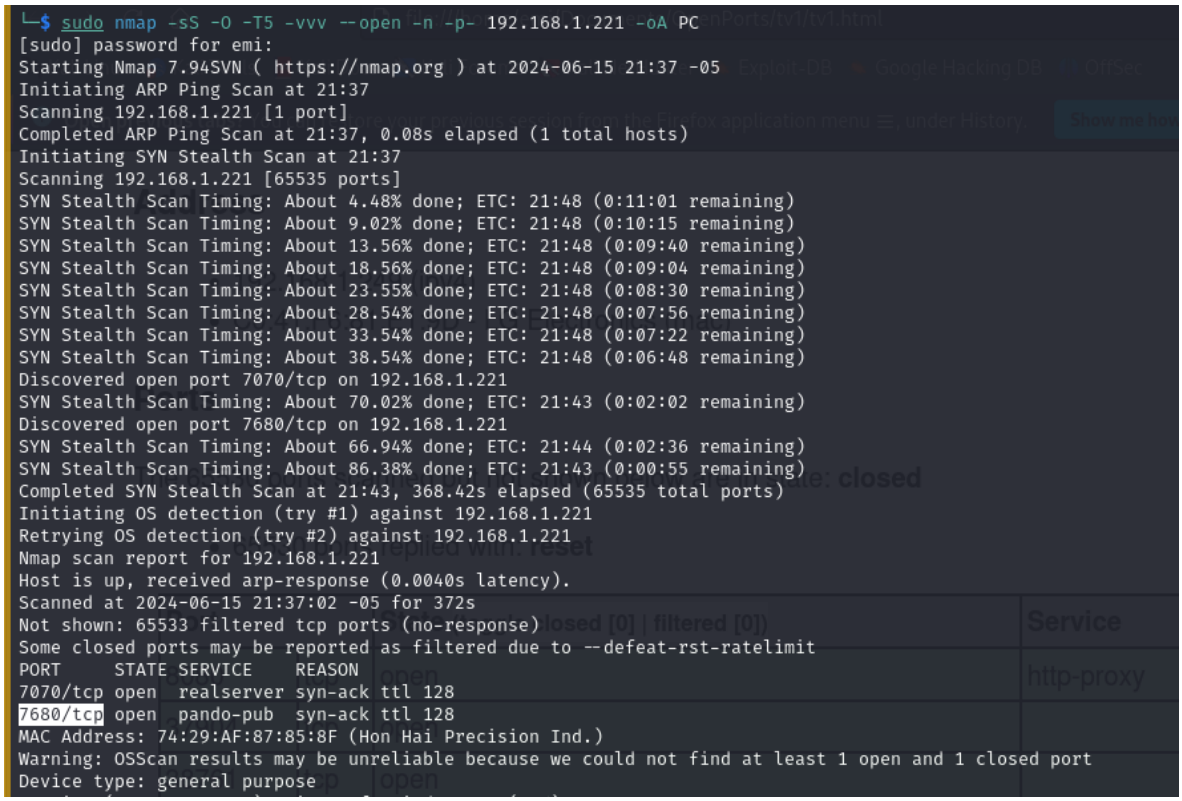
Figura 15.
Escaneo de puertos abiertos - dispositivo TV1



Se realiza el escaneo de los puertos abiertos junto a sus versiones para conocer las posibles vulnerabilidades que tienen cada uno de ellos junto al tipo de protocolo: TCP o UDP.

En la figura 18, se realiza un escaneo intensivo de una de las computadoras que se encuentran en la red mediante el uso del comando mostrado en la imagen anterior.

Figura 16.
Escaneo de puertos abiertos – dispositivo computador portátil



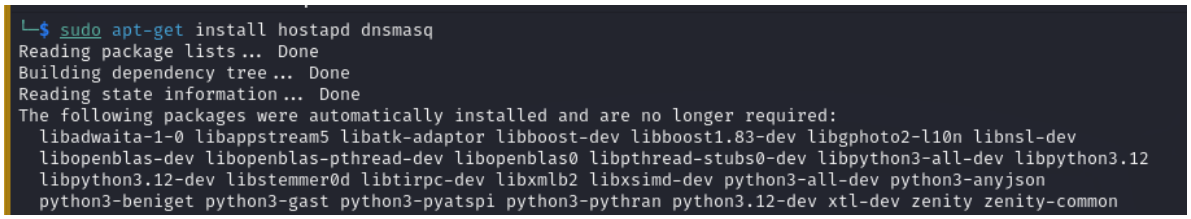
Se escanean los 65,535 puertos que utiliza un dispositivo en una red. Los puertos abiertos cumplen con la función de brindar un servicio de conexión, por lo que pueden ser vulnerables en caso de no encontrarse con sus versiones más actuales.

4.4.2. Etapa de explotación

En la figura 19, se realiza la instalación del paquete hostapd dnsmasq. El paquete hostapd permiten realizar el cambio de modo de la antena Wi-Fi para convertirla en un punto de acceso

inalámbrico, mientras que el paquete dnsmasq proporciona servicios como DNS, DHCP, entre otros; los cuales permiten asignar direcciones IPs y la conectividad hacia el equipo del atacante

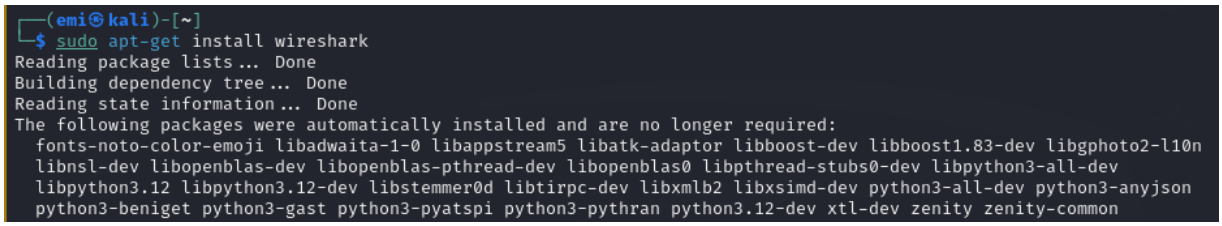
Figura 17.
Instalación de paquetes hostapd dnsmasq para ataques



Nota. Se utilizan los paquetes para crear una red inalámbrica

En la figura 20, se realiza la instalación de la herramienta Wireshark, esta permite visualizar protocolos, puertos, direcciones IP y datos entre información que contienen los paquetes en una transmisión de datos.

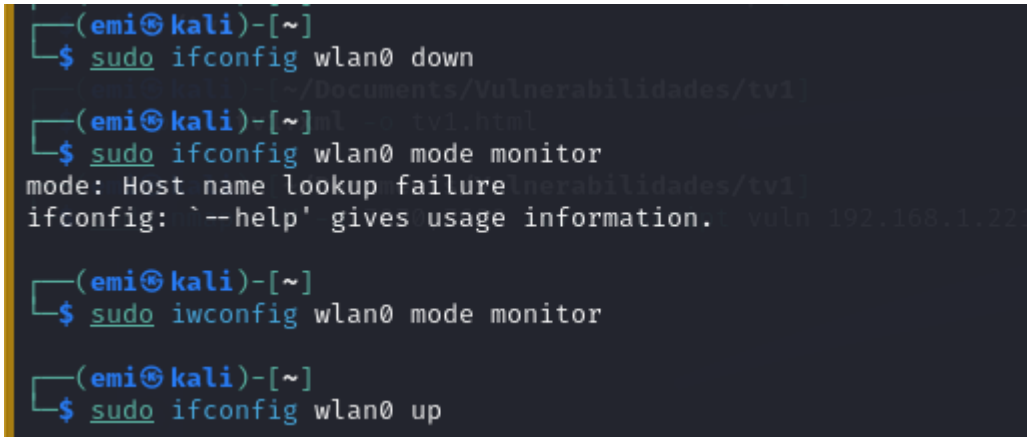
Figura 18.
Instalación de paquete para la captura de paquetes (sniffer)



Nota. Wireshark es un sniffer que permite capturar los paquetes que pasan por una interfaz de red.

Con el uso de los comandos de la figura 21, se establece a la tarjeta Wi-Fi a modo monitor, esto permite capturar todo el trafico de red que pasa a su alrededor, independientemente si estos son enviados o no a la computadora en la que esta instalada.

Figura 19.
Establecer tarjeta wi-fi modo monitor



Nota. Se establece la tarjeta inalámbrica en modo monitor para el escaneo de redes inalámbricas.

En la figura 22 se ejecuta el comando sudo airodump-ng wlan0 para realizar la captura de los paquetes de datos, esto permite identificar si la red victima se encuentra disponible en el perímetro, así como se muestra en la figura 23.

Figura 20.
Comando para el escaneo de redes wi-fi disponibles según el alcance

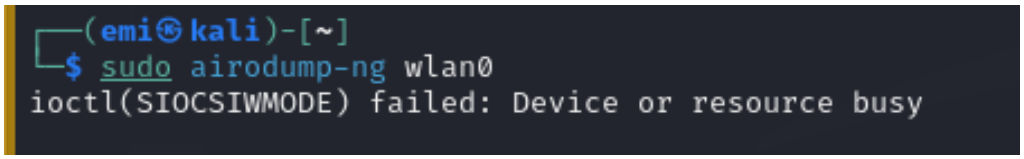
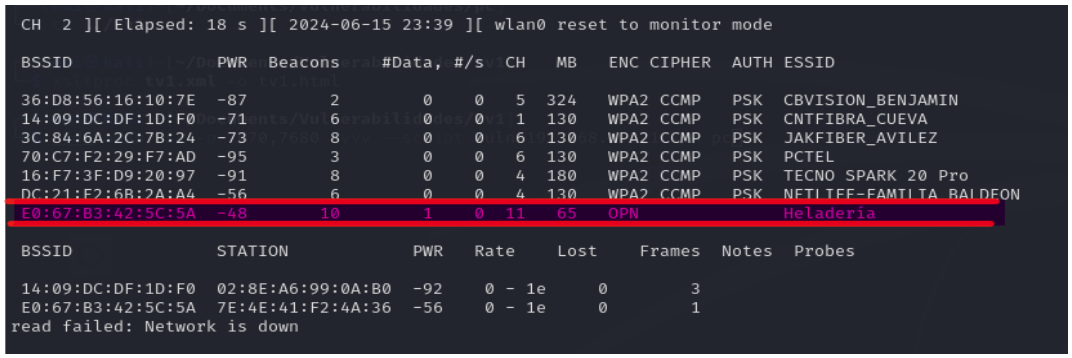


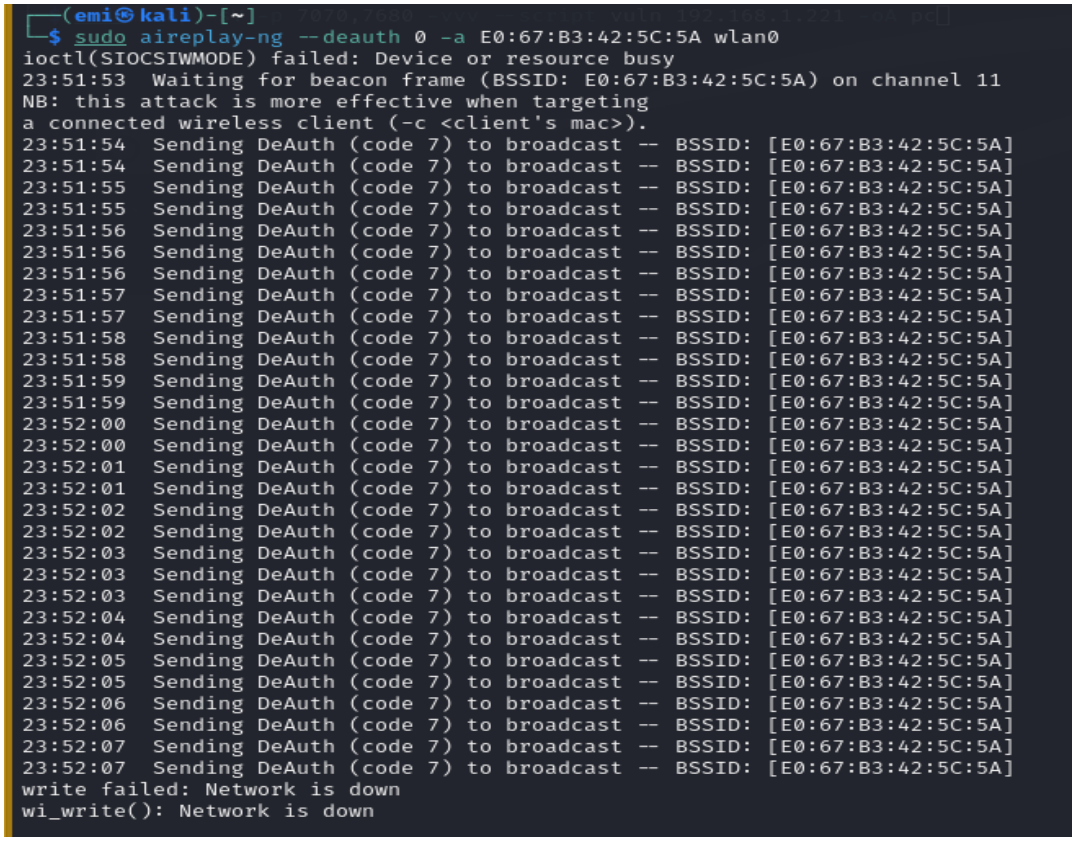
Figura 21.
Identificación de la red wi-fi a ser atacada



Nota. Mediante el comando se puede observar las redes inalámbricas que se encuentran disponibles junto al canal de tx, tipo de seguridad, tipo de autenticación, dirección mac y ssid.

La figura 24 utiliza una de las herramientas que ofrece aircrack-ng. Este comando tiene el fin de lograr realizar una desautenticación de los dispositivos de la red, mediante el envío de paquetes Wi-Fi.

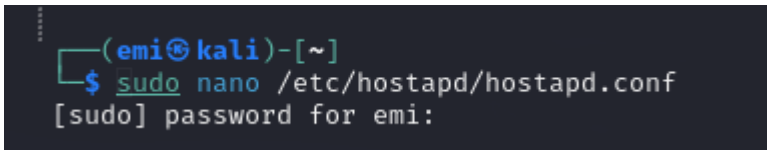
Figura 22.
Inicio de ataque de desauntenticación



Nota. Se envía un ataque que expulsar a cada uno de los dispositivos que se encuentran conectados en ese instante de manera forzada.

La figura 25 muestra como se realiza la modificación del archivo de configuración. El comando permite establecer los parámetros que tendrá la red inalámbrica del access point falso, canal de transmisión, tipo de tecnología 802.11, entre otros.

Figura 23.
Creación de archivo de configuración hostapd



La figura 26, contiene todos los parámetros configurados dentro del archivo de configuración modificado en la figura 25.

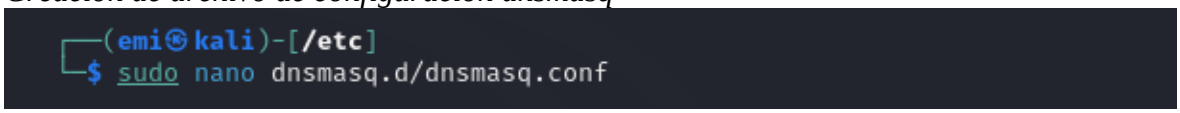
figura 26.

Parámetros de configuración archivo hostapd

```
interface=wlan0
driver=nl80211
ssid=Nombre_del_AP_Falso
hw_mode=g
channel=6
macaddr_acl=0
ignore_broadcast_ssid=0
auth_algs=1
```

En la figura 27 ejecuta el comando nano seguido de la ruta del archivo dnsmasq el que permite realizar su edición.

figura 24.
Creación de archivo de configuración dnsmasq



En la figura 28, establece los parámetros a configurar en el archivo dnsmasq, en este se configura el pool de direcciones que asignará el punto de acceso falso, el DNS que resolverá nombres de dominio, entre otros.

Figura 28.
parámetros de configuración archivo dnsmasq

```
interface=wlan0
dhcp-range=192.168.1.10,192.168.1.100,12h
dhcp-option=3,192.168.1.1
dhcp-option=6,192.168.1.1
server=8.8.8.8
log-queries
log-dhcp
```

La figura 29 muestra como establecer una ruta estática a la interfaz inalámbrica, el cual será el Access point falso.

Figura 25.
Asignación de una dirección ip estática a la interfaz inalámbrica

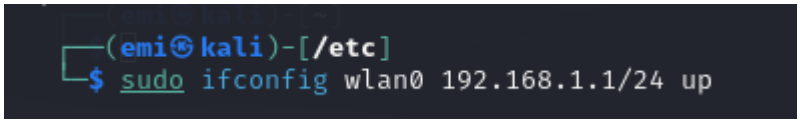
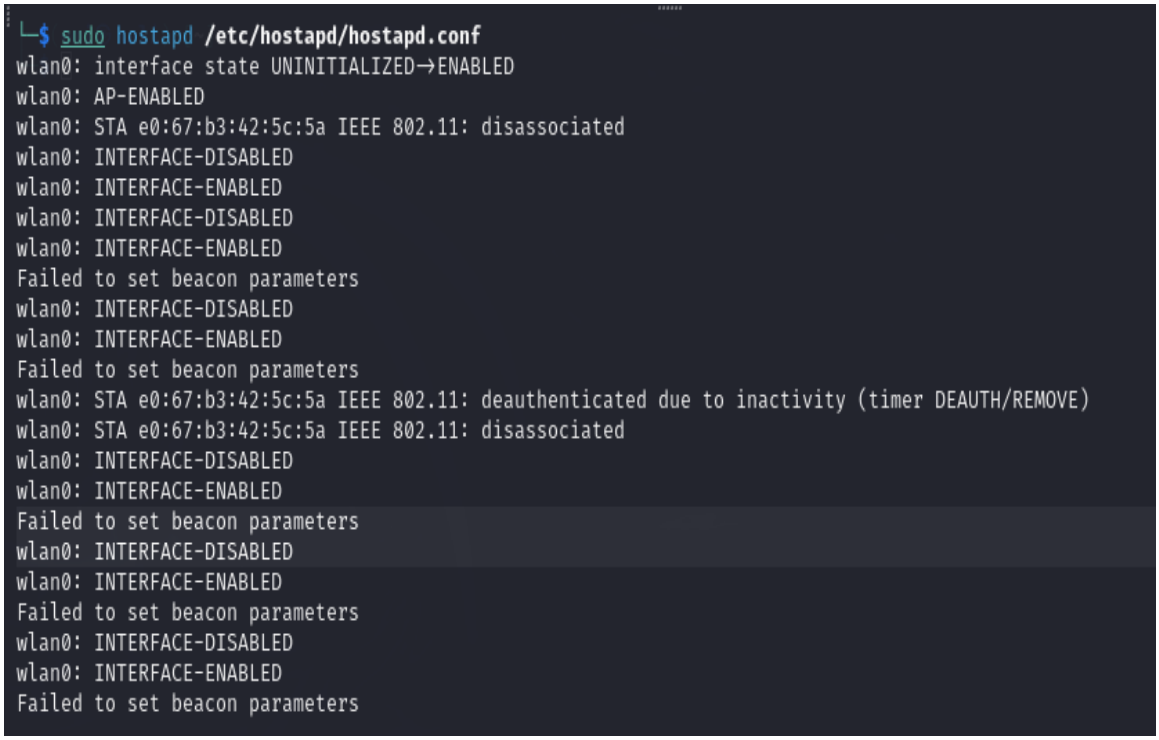
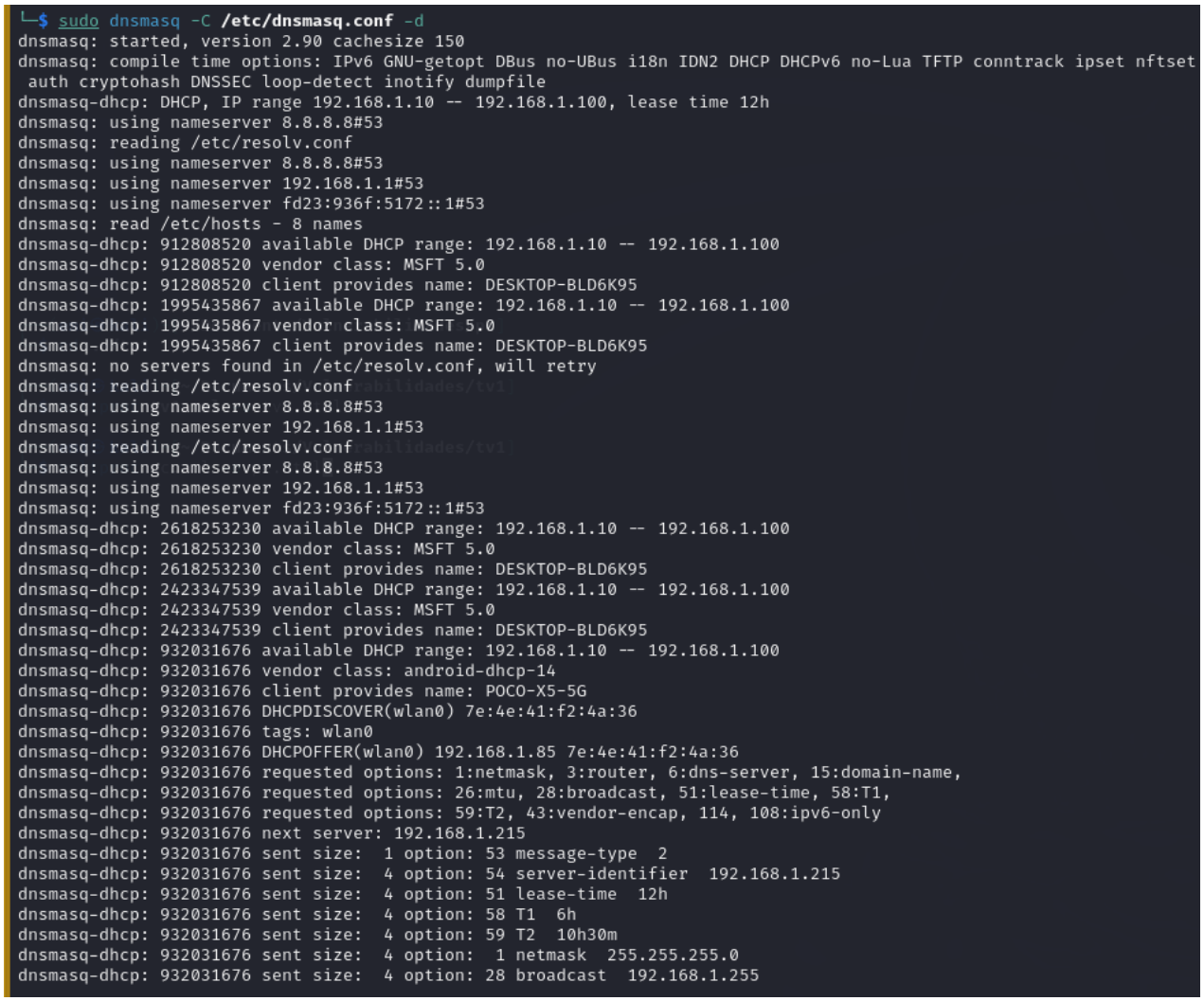


Figura 26.
Inicio de servicio hostapd para inicio de ataque man-in-the-middle



Nota. Se corre el servicio haciendo que se active la tarjeta de red inalámbrica como punto de acceso para que los equipos se conecten a través de estos dispositivos, los cuales desean propiamente conectarse, generando un ataque de hombre en el medio o man in the middle entre el dispositivo y el access point legitimo.

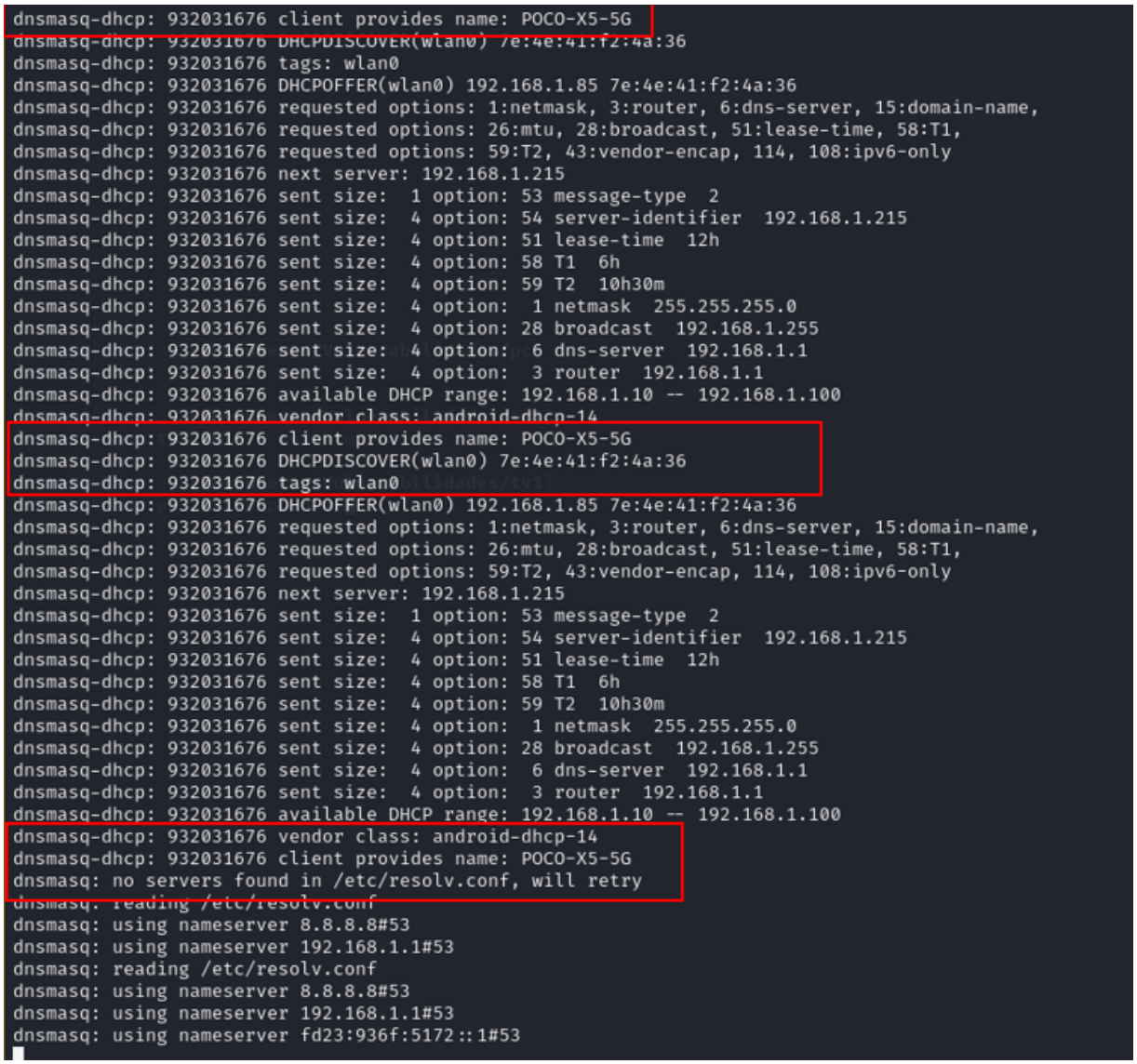
Figura 27.
Ejecución del ataque man-in-the-middle



Nota. Al ejecutar el servicio se configura un servidor de direcciones ip, dns en el cual, al mantener un dns caché, lo que facilita es responder de manera más ágil las consultas que realicen los clientes y, a su vez, registrar mediante logs cada una de las consultas y asignaciones que ha realizado el servidor.

Al realizar todos los pasos anterior mente vistas, se creará el Access point falso. En la figura 32 se muestra los datos de todos los dispositivos que se conectan a la red que se configuró previamente, también se puede realizar la capturar paquetes, es importante conocer que puede existir tráfico que al no estar cifrados pueden ser descifrable.

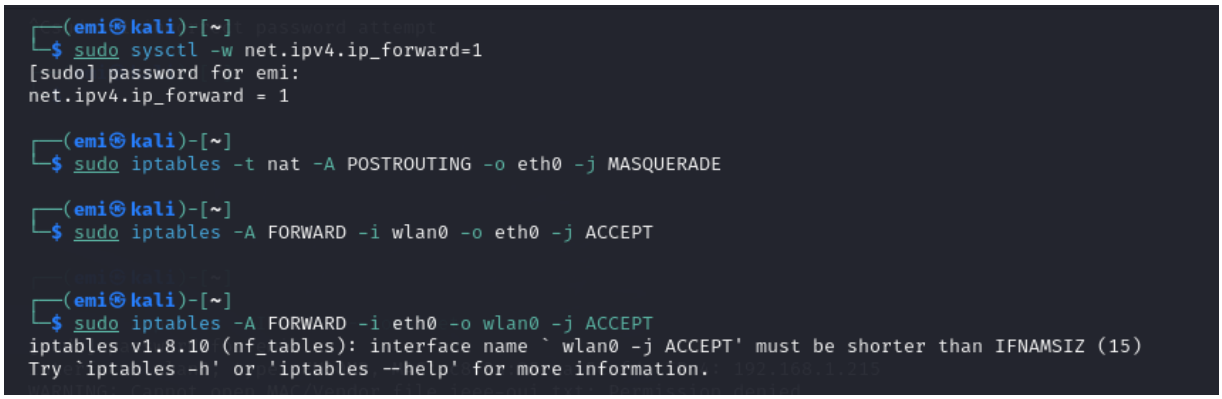
Figura 28.
Ejecución del ataque man-in-the-middle – parte 2



Nota Se detalla el modelo de los dispositivos conectados a la red.

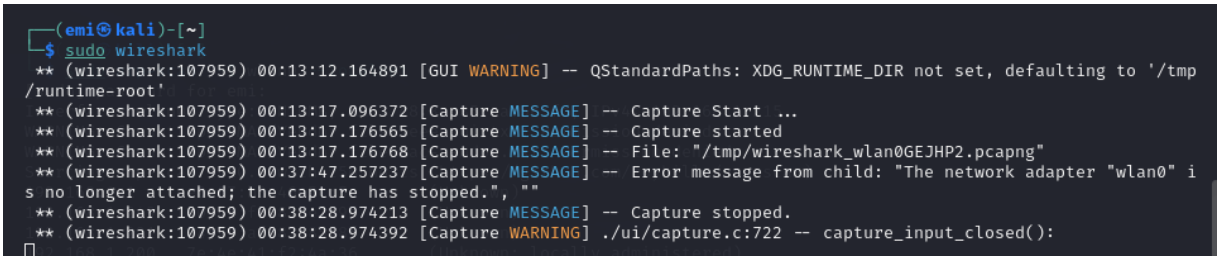
En la figura 23 se realiza el redireccionamiento del tráfico IP, este permite conmutar entre las interfaces de red del computador del atacante para manejar cada una de las peticiones dirigidas a Internet. Como objetivo, todo el tráfico generado por la PC del atacante, actua como un puente de conexión entre el dispositivo objetivo y el Internet.

Figura 29.
Redireccionamiento del tráfico IP por la computadora del atacante



Se ejecuta Wireshark para filtrar y capturar cada paquete que está pasando por el computador del atacante, se observa el flujo del tráfico, los datos de los paquetes y, en caso de no estar cifrados, pueden ser utilizados para actividades no éticas con dichos datos. Así como se muestra en la figura 34.

Figura 30.
Inicio de servicio Wireshark



Nota. Se visualiza el trafico que se encuentra generado en la red falsa

4.5. Análisis de resultados

Para el presente trabajo de titulación, se siguió un proceso de identificación de vulnerabilidades basado en el marco conceptual y teórico previamente establecido. Se llevó a cabo un proceso de hacking ético para explotar las vulnerabilidades encontradas en los dispositivos IoT dentro de la red en estudio. Se realizó la identificación de las vulnerabilidades más críticas detectadas por las herramientas Nmap y Nessus, las cuales proporcionaron información detallada sobre los puertos abiertos en cada dispositivo y los riesgos asociados. Se evaluó el nivel de criticidad de estas vulnerabilidades, tomando en cuenta el sistema CVE, el cual estandariza la identificación y categorización de vulnerabilidades en software y hardware para mejorar la interoperabilidad entre herramientas y servicios destinados a detectar, mitigar y prevenir vulnerabilidades.

Basado en los resultados obtenidos, se creó una tabla de vulnerabilidades que refleja el impacto potencial de cada una, destacando su integración en diferentes puertos y dispositivos. Se emplearon herramientas prácticas para comprender los riesgos potenciales explotables y se identificaron posibles soluciones para mitigar estos riesgos específicos. Se observaron diferencias en los resultados entre las herramientas Nmap y Nessus, lo cual contribuyó a identificar las vulnerabilidades más críticas y relevantes para cada dispositivo analizado.

Adicionalmente, se llevó a cabo un taller de concientización con los propietarios mediante un ataque simulado controlado. Este ejercicio permitió ilustrar cómo un ciberatacante podría comprometer la seguridad y robar información, simulando una red falsa dentro del entorno del lugar de estudio. Es fundamental que los propietarios y la comunidad en general comprendan los riesgos potenciales asociados no solo a sus negocios, sino también a la seguridad de sus datos en redes abiertas o compartidas. Esto subraya la importancia de mantener herramientas actualizadas, configuraciones de seguridad adecuadas y una formación continua sobre las prácticas de seguridad y las regulaciones legales relacionadas con la protección de datos.

Como se discutió en capítulos anteriores, es crucial mantener un consentimiento informado con los propietarios y el personal del lugar de estudio, asegurándose de que comprendan los objetivos del proyecto, los posibles riesgos y las medidas preventivas propuestas. La capacitación continua es fundamental para mantenerse actualizado sobre las mejores prácticas de seguridad y cumplir con las normativas legales que protegen la privacidad y la integridad de los datos en entornos comerciales.

Como resultados de la ejecución de las herramientas de ciberseguridad, se identificaron las vulnerabilidades de los dispositivos IoT conectados a la red local, centrándose exclusivamente en los dispositivos propios del entorno local, que se encuentran en una situación de riesgo en un nivel mediano, al compartir una red comunitaria con los clientes del lugar. Por consiguiente, se buscó concienciar a los propietarios sobre los riesgos y la posible pérdida de datos que podrían experimentar si no se toman medidas preventivas. Se propuso la separación y creación de una red exclusiva para los dispositivos IoT propios del lugar, con el fin de evitar la pérdida de datos y reducir el riesgo de ser víctimas de ciberdelincuencia.

4.6. Propuesta de buenas practicas

Se proponen soluciones para la prevención de riesgos ante ataques cibernéticos en los dispositivos IoT dentro de esta red, así como la creación de una red pública para brindar un servicio óptimo a los clientes del lugar. Entre las posibles configuraciones y soluciones se encuentran:

- Realizar una actualización constante en el firmware y software de todos los dispositivos para mantenerlos actualizados y así mantener los parches de seguridad creados por los fabricantes para evitar riesgos dentro de los dispositivos.
- Cambiar las credenciales predeterminadas dentro de cada dispositivo y crear contraseñas más seguras y robustas para evitar el acceso no autorizado.
- Deshabilitar servicios y puertos innecesarios, considerando el funcionamiento deseado del dispositivo dentro de la red.
- Configurar firewalls para mantener una red más segura.

- Instalar y configurar sistemas de detección y prevención de intrusiones para monitorear y bloquear actividades sospechosas dentro de la red y en los dispositivos.
- Deshabilitar el acceso remoto si no es estrictamente necesario.
- Implementar la autenticación de doble factor en los sistemas compatibles para aumentar la seguridad.
- Segmentar la red para aislar los dispositivos propios del lugar y reducir la superficie de ataque.

Es fundamental proporcionar capacitación continua a los usuarios de los dispositivos IoT mencionados en este documento para mantenerlos informados sobre los posibles riesgos y las medidas preventivas a implementar.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

1. La seguridad de una red IoT es crucial tanto para la empresa como para los usuarios y clientes. Al estar expuestos al público en general, estos dispositivos son susceptibles a diferentes tipos de ataques, tanto a nivel de red como físicos. La implementación de medidas de seguridad adecuadas es esencial para proteger la integridad y la privacidad de todos los involucrados.

2. En cumplimiento de las etapas de un pentesting, se realizó el reconocimiento de los dispositivos IoT mediante una matriz de observación detallada. Esta matriz incluye direcciones IP, sistemas operativos, puertos de comunicación y otras especificaciones de los equipos IoT, proporcionando una base sólida para la evaluación de seguridad.

3. Las herramientas de pentesting, como Nmap y Nessus, proporcionaron información crítica sobre las vulnerabilidades en los puertos y los CVE asociados. Esta información es esencial para identificar las debilidades de seguridad en los dispositivos IoT y facilitar la implementación de actualizaciones que protejan tanto los dispositivos como la red en su conjunto.

4. A partir de las vulnerabilidades identificadas, se estableció un comparativo para demostrar cómo la seguridad de la red y de los dispositivos IoT mejora mediante la adopción de buenas prácticas. La implementación de estas prácticas es fundamental para establecer estándares de seguridad en redes IoT, aplicables en contextos como SmartCities y SmartHomes.

5. El ataque controlado se llevó a cabo con las debidas autorizaciones del encargado del local, en cumplimiento con las leyes de protección de datos. Este ataque, realizado a nivel de capa 1 (Física) y capa 3 (Red), desautenticó a los usuarios y

luego intervino en la comunicación entre el endpoint y el Access Point. La exposición a protocolos no seguros podría resultar en la interceptación de datos por parte del atacante.

6. Durante la ejecución de los ataques, se documentaron detalladamente todas las vulnerabilidades junto con recomendaciones para mitigarlas. Estas recomendaciones son esenciales para reducir los riesgos dentro de la red y proteger la información de los usuarios. Este estudio subraya la importancia de concientizar sobre el uso seguro de dispositivos IoT y la implementación de medidas de seguridad adecuadas.

5.2. Recomendaciones

1) Es recomendable mantener los dispositivos IoT actualizados, ya que los fabricantes trabajan para mitigar posibles vulnerabilidades identificadas en las pruebas, proporcionando actualizaciones de parches de seguridad.

2) A medida que un local comercial crece, es importante identificar su expansión tecnológica para poder realizar las configuraciones de red adecuadas. Es fundamental ser conscientes de la necesidad de una inversión tecnológica que permita implementar las configuraciones necesarias, de esta manera se evitaría la filtración de datos y se puede proteger de manera adecuada los dispositivos contra diversos riesgos.

3) Se recomienda instalar antivirus tanto en la red como en los dispositivos IoT conectados a la misma, para prevenir posibles riesgos y mantener la integridad de los equipos.

4) Es importante conocer todas las herramientas proporcionadas por el fabricante de cada dispositivo, para así poder controlar su comportamiento en la red y configurarlo según las funciones específicas que se desea que cumpla.

5) Se recomienda realizar capacitaciones constantes a los propietarios y trabajadores del lugar para poder disminuir la probabilidad de ser víctimas de los ciberdelincuentes.

Anexos

Tabla 3.
Matriz de observación

Fabricante	Modelo	Tipo	Dirección ip

Tabla 4.
Tabla de identificación de vulnerabilidades

Nombre	Descripción	Solución	Criticidad	Ip	Puertos

Tabla 5.

Siglas con sus significados

Sigla	Descripción
RCE	Remote Code Execution (Ejecución Remota de Código)
ICMP	Internet Control Message Protocol
CSRF	Cross-Site Request Forgery (Falsificación de Petición en Sitio Cruzado)
XSS	Cross-Site Scripting (Scripting entre Sitios)
DNS	Domain Name System (Sistema de Nombres de Dominio)
DHCP	Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Hosts)
MAC	Media Access Control (Control de Acceso a Medios)

IP	Internet Protocol (Protocolo de Internet)
DOS	Denial of Service (Denegación de Servicio)
ADB	Android Debug Bridge
HTTP	Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto)
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión)
UDP	User Datagram Protocol (Protocolo de Datagrama de Usuario)
SSL/TLS	Secure Sockets Layer/Transport Layer Security
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
WPA2	Wi-Fi Protected Access 2
IoT	Internet of Things (Internet de las Cosas)
SSID	Service Set Identifier (Identificador de Conjunto de Servicios)
API	Application Programming Interface (Interfaz de Programación de Aplicaciones)
WLAN	Wireless Local Area Network (Red de Área Local Inalámbrica)
SNMP	Simple Network Management Protocol (Protocolo Simple de Gestión de Red)
LAN	Local Area Network (Red de Área Local)
NAT	Network Address Translation (Traducción de Direcciones de Red)
FTP	File Transfer Protocol (Protocolo de Transferencia de Archivos)
SSH	Secure Shell (Cáscara Segura)
VPN	Virtual Private Network (Red Privada Virtual)
UPnP	Universal Plug and Play
AP	Access Point (Punto de Acceso)
DNSMASQ	DNS Forwarder and DHCP Server
GUI	Graphical User Interface (Interfaz Gráfica de Usuario)
CLI	Command-Line Interface (Interfaz de Línea de Comandos)
MAC Address	Media Access Control Address (Dirección de Control de Acceso a Medios)
MITM	Man-in-the-Middle (Hombre en el Medio)
VLAN	Virtual Local Area Network (Red de Área Local Virtual)
Nmap	Network Mapper (Mapeador de Red)

Nessus	Vulnerability Scanner (Escáner de Vulnerabilidades)
Wireshark	Network Protocol Analyzer (Analizador de Protocolos de Red)
ARP	Address Resolution Protocol (Protocolo de Resolución de Direcciones)
HTTPD	Hypertext Transfer Protocol Daemon (Demonio de Protocolo de Transferencia de Hipertexto)

Tabla 6.

Diccionario de términos

Término	Descripción
Remote Code Execution	Vulnerabilidad que permite ejecutar código de manera remota en un sistema
ICMP	Protocolo de Control de Mensajes de Internet, utilizado para diagnósticos de red
CSRF	Ataque que engaña al usuario para que realice acciones no deseadas en una aplicación web
XSS	Vulnerabilidad que permite a un atacante insertar código malicioso en páginas web
DNS	Sistema que traduce nombres de dominio a direcciones IP
DHCP	Protocolo que asigna direcciones IP automáticamente a dispositivos en una red
MAC Address	Dirección única asignada a cada dispositivo de red
IP	Protocolo que facilita la comunicación entre dispositivos en una red
DOS	Ataque que intenta agotar recursos de un sistema para denegar el servicio
ADB	Puente de depuración de Android que permite la comunicación con dispositivos Android
HTTP	Protocolo para transferir información en la World Wide Web
TCP	Protocolo de comunicación que garantiza la entrega de datos sin errores
UDP	Protocolo de comunicación que envía datos sin establecer una conexión previa

SSL/TLS	Protocolos de cifrado para conexiones seguras en Internet
IDS/IPS	Sistemas que detectan y previenen intrusiones en redes
WPA2	Protocolo de seguridad para redes Wi-Fi
IoT	Red de dispositivos conectados a Internet que intercambian datos
SSID	Identificador único asignado a una red Wi-Fi
API	Interfaz que permite la comunicación entre diferentes aplicaciones de software
WLAN	Red inalámbrica de área local
SNMP	Protocolo para administrar dispositivos de red
LAN	Red de área local
NAT	Técnica que permite a múltiples dispositivos compartir una única dirección IP pública
FTP	Protocolo para la transferencia de archivos
SSH	Protocolo seguro para acceder a sistemas remotos
VPN	Red privada virtual que extiende una red privada a través de una red pública
UPnP	Protocolo que permite a dispositivos conectarse automáticamente a una red
AP	Dispositivo que permite a dispositivos inalámbricos conectarse a una red Wi-Fi
DNSMASQ	Servicio de DNS y DHCP que simplifica la configuración de redes
GUI	Interfaz gráfica de usuario
CLI	Interfaz de línea de comandos
MITM	Ataque en el que un atacante intercepta y modifica la comunicación entre dos partes
VLAN	Red de área local virtual que agrupa dispositivos en diferentes redes lógicas

Nmap	Herramienta de escaneo de red
Nessus	Escáner de vulnerabilidades
Wireshark	Analizador de protocolos de red
ARP	Protocolo para asociar direcciones IP con direcciones físicas (MAC)
HTTPD	Servidor HTTP Daemon

Bibliografía

Medina rojas, e. F. (2015). *Hacking ético: una herramienta para la seguridad informática* (bachelor's thesis, universidad piloto de colombia).

Voutssas, juan (2010), "preservación documental digital y seguridad informática", *investigación biblIoTecológica*, 24-50, pp. 127-155, doi: http://dx.doi.org/10.22201/iibi.0187358xp.2010.50.21416.

Cruz, j. (2021). Análisis de vulnerabilidades ¿qué es y para qué le sirve a las empresas? Easysec. Https://blog.easysec.com.mx/2021/09/que-es-un-analisis-de-vulnerabilidades.html#:~:text=el%20an%c3%a1lisis%20de%20vulnerabilidades%20se%20encarga%20de%20detectar%2c,si%20un%20ciberdelincuente%20llegara%20a%20realizar%20un%20ataque.

Elastic. (s.f.). ¿qué es ciberseguridad? Elastic. Https://www.elastic.co/es/what-is/cybersecurity

red hat. (2022). Seguridad para los dispositivos del IoT. Red hat. Https://www.redhat.com/es/topics/security/security-for-IoT-devices

herrero, m. (2023). Educación y conciencia en seguridad cibernética. Escueladeinternet. Https://www.escueladeinternet.com/educacion-y-conciencia-en-seguridad-cibernetica/#:~:text=en%20resumen%2c%20la%20educaci%c3%b3n%20y%20la%20concienciaci%c3%b3n%20en,l%c3%adnea%20son%20aspectos%20clave%20de%20la%20seguridad%20cibern%c3%a9tica.

Ecured (s.f).ataque informático. Recuperado de: https://www.ecured.cu/ataque_inform%c3%a1tico

martínez, e. (2018). Las diferentes amenazas de seguridad informática. Recuperado de: Https://sites.google.com/site/lasamenazaslainformatica/

malwarebytes (2019). Ransomware. Recuperado de: https://es.malwarebytes.com/ransomware/

olaya, a. (2021). "ataques cibernéticos" ("cyber attacks"). Universidad militar nueva granada. Https://repository.unimilitar.edu.co/bitstream/handle/10654/39021/olayaoliverosalexander2021.pdf?sequence=1&isallowed=y

parra tapia, e. A. (2020). Identificación y análisis de vulnerabilidades en los portales web de la universidad politécnica salesiana a través de técnicas de pentesting (bachelor's thesis).

Gutiérrez, f. (2014). Laboratorio virtualizado de seguridad informática con kali linux.

Universidad de valladolid. Escuela universitaria de informática. Http://uvadoc.uva.es/handle/10324/5792

abba, m. (2023). Qué es wireshark, para qué sirve y casos de uso. Innovacióndigital360. Https://www.innovaciondigital360.com/IoT/que-es-wireshark-y-casos-de-uso/

Red hat. (2023). ¿qué es el internet de las cosas (IoT)? Red hat. Https://www.redhat.com/es/topics/internet-of-things/what-is-IoT

ibm. (s.f.). ¿qué es la seguridad de datos? Ibm. Https://www.ibm.com/es-es/topics/data-security

trevino, a., cutler, a. & darren, g. (2023). ¿qué es una política de privacidad?. Keeper. Https://www.keepersecurity.com/blog/es/2023/03/28/what-is-a-privacy-policy/

microsoft. (s.f). ¿qué es el control de acceso?. Microsoft. Https://www.microsoft.com/es-es/security/business/security-101/what-is-access-control

Microsoft. (s.f.). ¿qué es la protección de datos?. Microsoft. Https://www.microsoft.com/es-mx/security/business/security-101/what-is-data-protection

Ibm. (s.f.). ¿qué es la seguridad de red?. Ibm. Https://www.ibm.com/es-es/topics/network-security

ibm. (s.f.). ¿qué es un ciberataque?. Ibm. Https://www.ibm.com/es-es/topics/cyber-attack

Canle, e. (2022). El internet de las cosas: su evolución en los últimos años. Tokio school. Https://www.tokioschool.com/noticias/internet-de-las-cosas-evolucion/

Patiño, d. & sánchez, e. (2021). Las amenazas de seguridad a las que se enfrenta IoT y las soluciones en desarrollo. Universidad distrital francisco josé de caldas. Http://hdl.handle.net/11349/29310

Engebrestson, p. (2011). The basics of hacking and penetration testing

Enríquez, l. (2017). Paradigmas de la protección de datos personales en ecuador. Análisis del proyecto de ley orgánica de protección a los derechos a la intimidad y privacidad sobre los datos personales. Scielo. Http://scielo.senescyt.gob.ec/scielo.php?pid=s2631-24842017000100043&script=sci_arttext

Gómez, j. (2023). ¿cómo garantizar la confidencialidad de la información en tu empresa?. Apolo. Https://www.deltaprotect.com/blog/confidencialidad-de-la-informacion

National cybersecurity aliance, (2022). ¿qué es la protección de datos?. Https://staysafeonline.org/es/online-safety-privacy-basics/what-is-data-privacy/

Cuevas, e. (2018). La transparencia en el nuevo reglamento general de protección de datos. Académica correspondiente de la sección de derecho de la real academia de doctores de españa. Https://www.rade.es/doc/2v3n1%20-garciacuevas%20-%20protecci%c3%b3n%20de%20datos.pdf

Nmap.org. (s.f.). Guía de referencia de nmap (página de manual). Https://nmap.org/man/es/index.html

Elaborado por:	Revisado por:	Revisado y visto bueno por:
Emuly rea	Beatriz campos	
Emily rea	Ing. Beatriz campos	Ing. Oswaldo espinosa
Fecha: 25 junio 2024	Fecha: 28 junio 2024	Fecha: xxxxxx