Fortalecimiento de la Cultura de Seguridad en el Hogar: Promoviendo Prácticas Seguras en el Uso de Dispositivos IoT

Adriana Forero Polanco, Yohana Marcela Castro

Especialización en Seguridad informática, Fundación Universitaria Compensar

Proyecto fin de grado Proyecto fin de grado Seguridad en el hogar en relación con el uso de dispositivos IoT (Internet de las Cosas).

M.Sc., Jaime Andrés Chaparro Sanchez

31 de mayo de 2024

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Fortalecimiento de la Cultura de Seguridad en el Hogar: Promoviendo Prácticas Seguras en el Uso de Dispositivos IoT

Adriana Forero Polanco, Yohana Marcela Castro

Trabajo de grado presentado como requisito parcial para optar al título de:

Especialista en Seguridad Informática

Director (a):

M.Sc., Jaime Andrés Chaparro Sanchez

Línea de Investigación:

Seguridad en el hogar en relación con el uso de dispositivos IoT (Internet de las Cosas).

Fundación Universitaria Compensar

Facultad de Ingeniería, Especialización en Seguridad Informática

Bogotá, Colombia

2024

Resumen

El presente proyecto tiene como propósito investigar y promover la cultura de seguridad en el hogar en relación con el uso de dispositivos IoT (Internet de las Cosas). Con el creciente número de dispositivos conectados en los hogares, es crucial comprender las percepciones, conocimientos y prácticas de seguridad de los propietarios de hogares, así como desarrollar estrategias efectivas para promover prácticas de seguridad más sólidas y conscientes en el entorno doméstico.

Para lograr este objetivo, se llevará a cabo una investigación a través de ejecución de pruebas que permitan demostrar algunas vulnerabilidades a las que están expuestas los dispositivos IoT en el hogar.

El proyecto busca contribuir a mejorar la seguridad y privacidad de los hogares al aumentar la conciencia sobre las mejores prácticas de seguridad en el uso de dispositivos IoT y fomentar cambios positivos en la cultura de seguridad doméstica. Además, proporcionará información valiosa para diseñadores de políticas, fabricantes de dispositivos y proveedores de servicios para desarrollar productos y servicios más seguros y centrados en el usuario.

Palabras clave: (IoT, seguridad, hogar, dispositivos, riesgo, data).

Abstract

The present project aims to investigate and promote home security culture regarding the use of IoT (Internet of Things) devices. With the increasing number of connected devices in homes, it is crucial to understand homeowners' perceptions, knowledge, and security practices, as well as to develop effective strategies to promote stronger and more mindful security practices in the domestic environment.

To achieve this goal, research will be conducted through the execution of tests to demonstrate some vulnerabilities to which IoT devices in the home are exposed.

The project seeks to contribute to improving the security and privacy of homes by raising awareness about best security practices in the use of IoT devices and fostering positive changes in home security culture. Additionally, it will provide valuable information for policymakers, device manufacturers, and service providers to develop safer and user-centric products and services.

Keywords: (IoT, security, home, devices, risk, data).

Contenido

PÁG.

RESUMEN ..... **V**

INTRODUCCIÓN **1**

ANTECEDENTES Y JUSTIFICACIÓN 2
FORMULACIÓN DEL PROBLEMA 3
OBJETIVO GENERAL 4
Objetivos Específicos *4*
ALCANCES 5

1. MARCO TEÓRICO **7**

1.1 SEGURIDAD EN EL HOGAR 7
1.2 INTERNET DE LAS COSAS (IOT) 7
1.3 PERCEPCIÓN DEL RIESGO 7
1.4 AFECTACIÓN AL USUARIO 8

2. DISEÑO METODOLÓGICO **9**

2.1 FASE 1 (IDENTIFICACIÓN DE EQUIPOS CONECTADOS A LA RED WIFI HOGAR) 9
2.2 FASE 2 (ESCANEO DE PUERTOS ABIERTOS, NMAP-KALI LINUX OPEN SOURCE) 10
2.3 FASE 3 (ESCANEO DE VULNERABILIDADES) 11
2.4 FASE 4 (ANÁLISIS ESCANEO) 11
2.5 FASE 5 (ESCANEO AIRCRACK-MG SOBRE RED WIFI DOMESTICA) 14
2.6 FASE 6 (INTEGRACIÓN DE *AIRCRACK* CON *JOHN THE RIPPER*) 15

3. RESULTADOS **17**

4. CONCLUSIONES Y RECOMENDACIONES **18**

4.1 CONCLUSIONES 18
4.2 RECOMENDACIONES 19

BIBLIOGRAFÍA **21**

Introducción

Con el creciente número de dispositivos conectados en los hogares, es crucial comprender las prácticas de seguridad de los propietarios de hogares, así como desarrollar estrategias efectivas para promover prácticas de seguridad más sólidas y conscientes en el entorno doméstico.

Para alcanzar este objetivo, realizaremos pruebas en un dispositivo doméstico utilizando aplicaciones de ciberseguridad. Esto nos ayudará a identificar sus vulnerabilidades y mostrar el riesgo de seguridad al que están expuestas las personas.

El proyecto busca contribuir a mejorar la seguridad y privacidad de los hogares al aumentar la conciencia sobre las mejores prácticas de seguridad en el uso de dispositivos IoT y fomentar cambios positivos en la cultura de seguridad doméstica. Además, proporcionará información valiosa para diseñadores de políticas, fabricantes de dispositivos y proveedores de servicios para desarrollar productos y servicios más seguros y centrados en el usuario.

Antecedentes y Justificación

Se estima que para el 2020 existen más de 21 billones de dispositivos IoT y que este número se duplique para 2025. Empresas como Intel y Cisco están empezando a ofrecer portafolios de servicios que incluyen múltiples dispositivos IoT y algunos operadores de telecomunicaciones como Telenor30 han empezado a desarrollar redes dedicadas exclusivamente al uso en masa de estos dispositivos31. Se estima que el mercado global de IoT en 2019 alcanzó una valoración de 1.7 trillones de dólares, con potencial de llegar a alcanzar una valoración entre 4 y 11 trillones de dólares para el 2025.

El crecimiento de los dispositivos IoT también ha aumentado el riesgo de ataques y fraudes cibernéticos. El ataque a estos dispositivos se incrementó más de un 300% en la primera mitad del 2019 y estos dispositivos han sido utilizados para interrumpir el servicio de páginas como Wikipedia (CRCOM, 2020).

La importancia de este proyecto radica en su capacidad para abordar una brecha crítica en la investigación y la práctica relacionada con la seguridad en el hogar en la era de la IoT. Aunque se han realizado esfuerzos significativos para mejorar la seguridad de los dispositivos IoT a nivel técnico, hay una falta de comprensión sobre cómo los usuarios finales perciben y gestionan estos riesgos en el entorno doméstico. Al investigar las prácticas de seguridad de los propietarios de viviendas en relación con los dispositivos IoT, este proyecto proporcionará información valiosa que puede utilizarse para informar políticas, diseñar productos más seguros y desarrollar programas de concientización para promover una cultura de seguridad más sólida en los hogares. En última instancia, se espera que los hallazgos de este proyecto contribuyan a mejorar la seguridad y privacidad de los hogares en la era digital.

Formulación del Problema

El creciente número de dispositivos IoT en los hogares plantea nuevos desafíos en términos de seguridad y privacidad. A pesar de los beneficios que ofrecen estos dispositivos en términos de comodidad y eficiencia, también representan puntos de acceso potenciales para amenazas de seguridad cibernética. La falta de comprensión sobre cómo los propietarios de viviendas perciben y gestionan estos riesgos en el entorno doméstico es una barrera significativa para abordar eficazmente los desafíos de seguridad en la era de la IoT.

Por lo tanto, el problema central que este proyecto busca abordar es:

¿Cómo proteger la seguridad en el hogar para dispositivos IoT considerando las prácticas de seguridad de las personas en sus viviendas?

Objetivo General

Evaluar las vulnerabilidades de seguridad en un dispositivo IoT doméstico, con el propósito de identificar riesgos potenciales que generen recomendaciones específicas para mejorar la seguridad, protegiendo así a los usuarios finales.

Objetivos Específicos

1. Identificar las vulnerabilidades presentes en un dispositivo IoT de hogar realizando pruebas con aplicaciones de ciberseguridad.

2. Demostrar el impacto potencial de las vulnerabilidades detectadas a través de simulaciones utilizadas comúnmente por los atacantes.

3. Proponer recomendaciones y buenas prácticas de seguridad que puedan ser aplicadas e implementadas por los usuarios para mitigar los riesgos.

Alcances

- Comprensión del nivel de conocimiento y conciencia sobre seguridad en el uso de dispositivos IoT en los hogares.
- Identificación de prácticas de seguridad actuales y áreas de mejora en el entorno doméstico relacionadas con dispositivos IoT.
- Evaluación de la promoción de estándares de seguridad por parte de fabricantes y entidades de seguridad cibernética.
- Facilitar la divulgación de información sobre mejores prácticas de seguridad a los usuarios finales.
- Cooperación con entidades gubernamentales de seguridad cibernética para mejorar la seguridad en el uso de dispositivos IoT en el hogar.
- Evaluación de un dispositivo IoT (Televisor Samsung).

Limitaciones:

- Restricciones de tiempo y recursos para llevar a cabo observaciones exhaustivas de prácticas de seguridad en los hogares.
- Dependencia de la información proporcionada por fabricantes y entidades de seguridad cibernética, que puede no ser completa o actualizada.
- Posibles barreras en la colaboración con entidades gubernamentales debido a políticas o agendas institucionales. Cambios rápidos en la tecnología IoT y en las amenazas de seguridad, lo que puede hacer que algunas conclusiones o recomendaciones sean obsoletas rápidamente.
- Al realizar análisis únicamente de un dispositivo se sugiere realizar en la modalidad de pregrado ampliar el tema, abarcando diferentes dispositivos.

1. Marco teórico

1.1 Seguridad en el hogar

La seguridad en el hogar es un aspecto fundamental para el bienestar de las personas y la protección de sus bienes. Los estudios previos han identificado factores como la ubicación geográfica, el nivel socioeconómico y la experiencia previa con dispositivos de domótica, variables que influyen en las medidas de seguridad adoptadas por los residentes. La tendencia de crecimiento de los dispositivos IoT es exponencial y se estima que en 2025 estos sean más de 21.000 millones, en comparación con los dispositivos non-IoT los cuales presentan un crecimiento lineal. (INCIBE, 2019).

1.2 Internet de las cosas (IoT)

Internet de las Cosas (IoT) ha revolucionado la forma en que interactuamos con el mundo digital y físico, permitiendo la interconexión de dispositivos cotidianos. Sin embargo, el crecimiento exponencial de dispositivos IoT también ha planteado preocupaciones significativas en términos de seguridad y privacidad. Se puede acceder desde cualquier dispositivo en cualquier momento, siempre y cuando se disponga de acceso a Internet. Lo anterior, combinado con la autonomía que por naturaleza presentan los sistemas IoT, su sensibilidad a los cambios en su entorno gracias a los sensores, su asequibilidad y su escalabilidad, hacen de las tecnologías IoT una solución rentable y cómoda en escenarios que requieran de un monitoreo constante. (Fernandez, 2022).

1.3 Percepción del riesgo

La manera en que las personas perciben y evalúan los riesgos asociados con el uso de dispositivos IoT en el hogar es un factor crucial que influye en sus comportamientos de seguridad. Los estudios han demostrado que la percepción del riesgo puede variar

significativamente entre los individuos y puede estar influenciada por factores como la familiaridad con la tecnología, la confianza en las medidas de seguridad y la exposición a incidentes de seguridad previos.

La relevancia de las tecnologías IoT, así como las ventajas que ofrecen en nuestro día a día, es una realidad. Sin embargo, también presentan varios inconvenientes para tener en cuenta. La información que manejan estos dispositivos es cada vez más sensible o relevante, por lo que mantenerlos seguros resulta de vital importancia. (INCIBE, 2019).

1.4 Afectación al usuario

Entre los errores más comunes que comprometen la seguridad de los dispositivos IoT se encuentran la falta de credenciales robustas y la configuración inadecuada o inexistente de medidas de seguridad. Estos errores crean oportunidades que los ciberdelincuentes aprovechan para ejecutar diversas formas de ataques. Al no implementar contraseñas fuertes y únicas, los usuarios dejan sus dispositivos expuestos a accesos no autorizados. Además, una configuración de seguridad deficiente permite a los atacantes explotar vulnerabilidades conocidas para infiltrarse en los dispositivos.

Una vez que los ciberdelincuentes logran penetrar estos dispositivos, pueden acceder a datos sensibles, como información personal y financiera, que puede ser utilizada para diversos fines maliciosos, incluidos el robo de identidad y fraude. Más allá de la extracción de datos, los atacantes pueden tomar el control de los dispositivos IoT para realizar prácticas de amenazas, estafa o extorsión.

El desconocimiento y la falta de medidas preventivas adecuadas por parte de los usuarios son factores que incrementan la vulnerabilidad de los sistemas IoT. Es fundamental que los usuarios sean conscientes de la importancia de configurar adecuadamente sus dispositivos, utilizar contraseñas complejas, y mantener sus sistemas actualizados con los últimos parches de seguridad. La educación en ciberseguridad y la adopción de buenas prácticas son cruciales para mitigar los riesgos asociados con la creciente digitalización y el uso de tecnologías IoT. (Sicajá, L. F., Morales, V. A., Velásquez, J. G., León, M., & Velásquez).

2.Diseño Metodológico

En este proyecto se utilizó el diseño metodológico de modelo cascada como metodología para el desarrollo del proyecto. Consiste en la secuencia de las fases ejecutadas en cada una de las actividades para llegar al resultado.

Análisis: planificación, análisis y especificación de los requisitos.

Diseño: diseño y especificación del sistema.

Implementación: configuración y uso de aplicaciones.

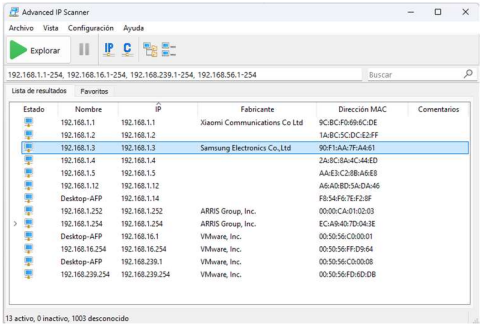
Verificación: pruebas y análisis del resultado

Mantenimiento: recomendaciones y mejora.

3.Desarrollo

3.1 Fase 1 (Identificación de equipos conectados a la red wifi hogar)

Se realiza escaneo a través del aplicativo gratuito *Advanced IP Scanner*, mostrando los siguientes dispositivos conectados a la *red* ***Wifi Tigo-A78F***, que corresponde al hogar de la Ing. Adriana Forero.

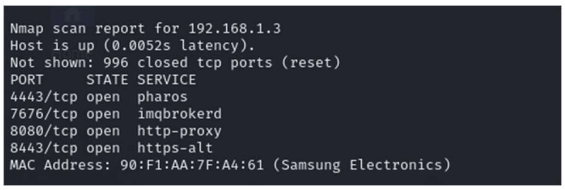


Se observa a través del aplicativo, direccionamiento IP, Fabricante y MAC Address, identificando la dirección IP 192.168.1.3 que corresponde al televisor Smart TV Samsung. Se valida la información del dispositivo mediante el Aplicativo *MacVendor:* ***Samsung 40"Full HD T5290.***



3.2 Fase 2 (Escaneo de puertos abiertos, Nmap-Kali Linux Open Source)

Posterior al haber instalado las librerías en Kali Linux de Nmap se configura un escaneo, a fin de identificar los puertos abiertos del Televisor Samsumg. IP 192.168.1.3.



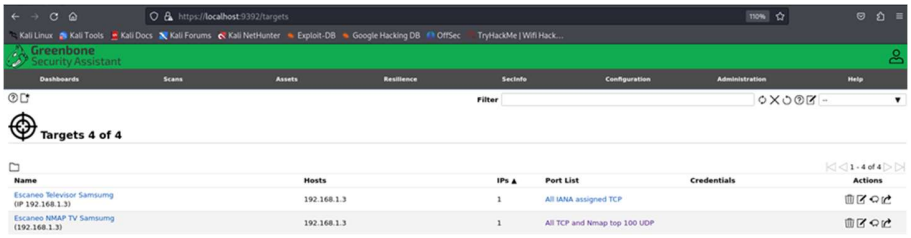
Informe de Escaneo Nmap para 192.168.1.3:

Estado del Host: Activo
Latencia: 0.0052 segundos
Puertos Abiertos:
4443/tcp: Pharos (Protocolo no especificado)
7676/tcp: imqbrokerd (Protocolo no especificado)
8080/tcp: HTTP Proxy
8443/tcp: HTTPS Alternate

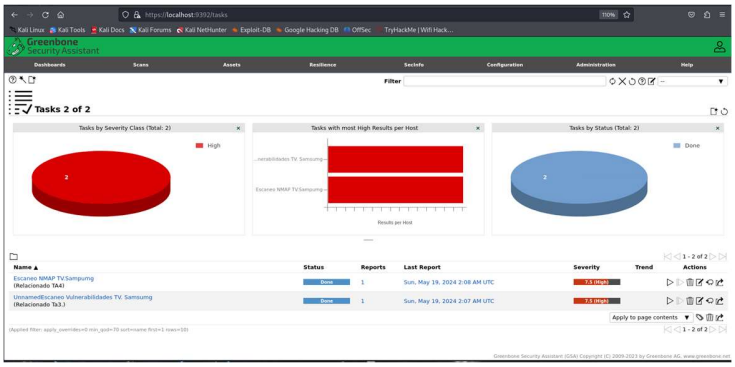
Información Adicional:
Dirección MAC: 90:F1:AA:7F:A4:61 (Samsung Electronics).

3.3 Fase 3 (Escaneo de vulnerabilidades)

A través de la herramienta Openvas, se crean dos tareas para análisis de vulnerabilidades una para el protocolo TCP y el otro para análisis de puertos Nmap.

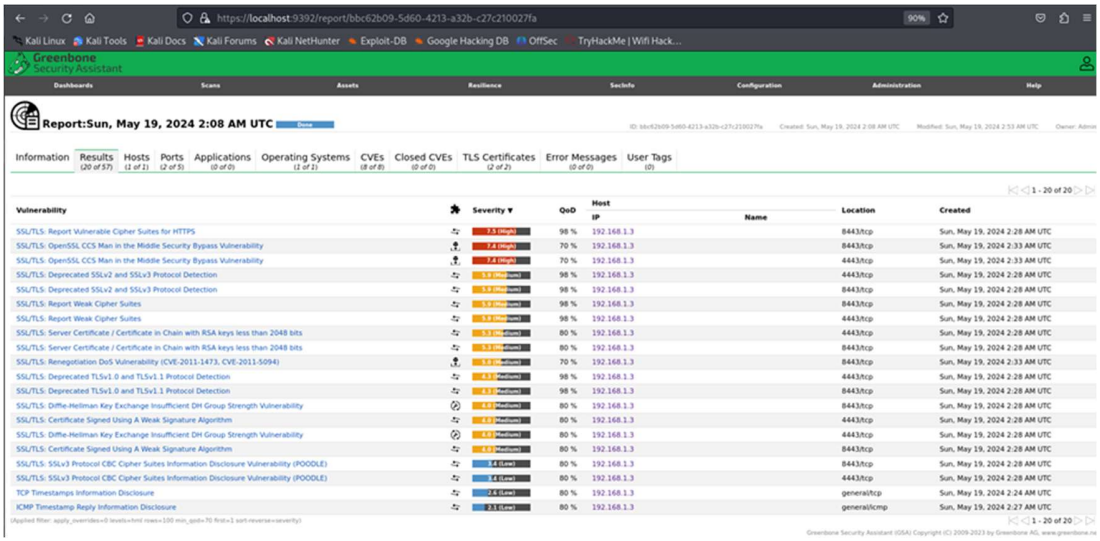


Se ejecuta esta tarea sobre Openvas para detectar las vulnerabilidades presentadas, de las cuales se encuentran severidades críticas.

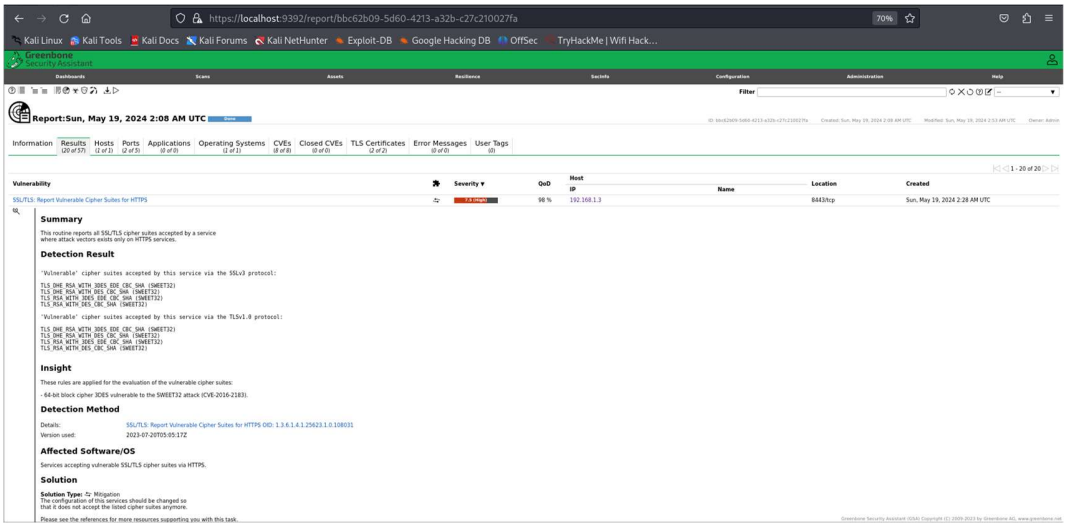


3.4 Fase 4 (Análisis escaneo)

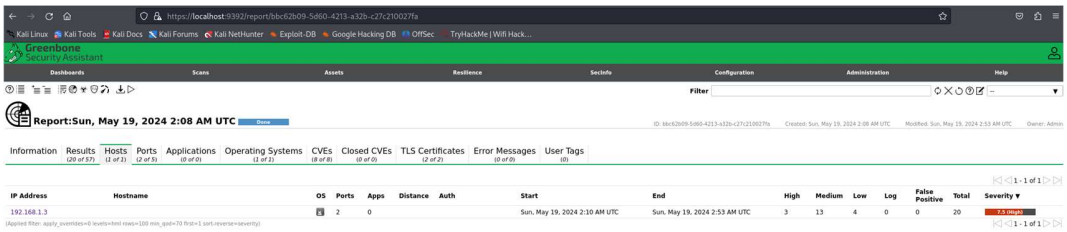
Dentro de los resultados para estas vulnerabilidades se encontraron categorizados los grados de severidad en cuanto a detección de Vulnerabilidades.



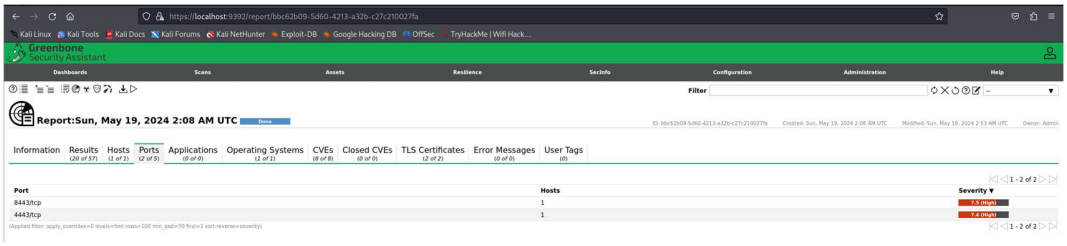
Para el desarrollo del presente trabajo se evaluó la criticidad más alta de las vulnerabilidades encontradas.



Informe de Host: Se genera informe del Host IP 192.168.1.3, encontrando que tiene un sistema operativo basado en Linux, tiene 2 puertos habilitados y 17 vulnerabilidades entre criticidades medias y bajas. Tres (3) vulnerabilidades con una criticidad Alta de 7.5/10.

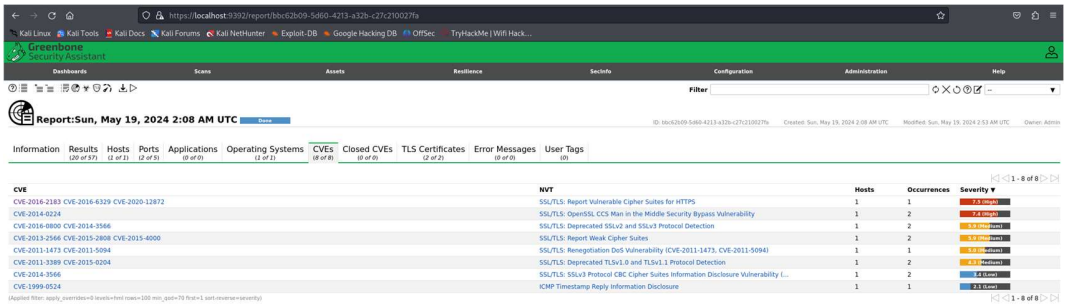


Estado de los puertos: Se encuentran abiertos los puertos 8443,4443 con severidad críticos que permiten el acceso remoto.

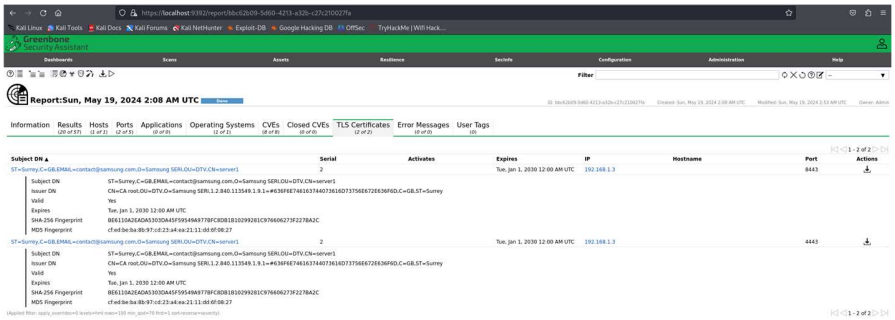


Este informe destaca la presencia de suites de cifrado consideradas vulnerables en un servicio HTTPS y proporciona orientación sobre cómo abordar esta vulnerabilidad mediante la modificación de la configuración del servicio.

Los CVE relacionados para este informe son los siguientes:



Informe de Certificados TLS: Los certificados TLS son esenciales para establecer conexiones seguras a través de Internet, y proporcionan autenticación y cifrado para proteger la privacidad y la integridad de los datos transmitidos entre un cliente y un servidor.

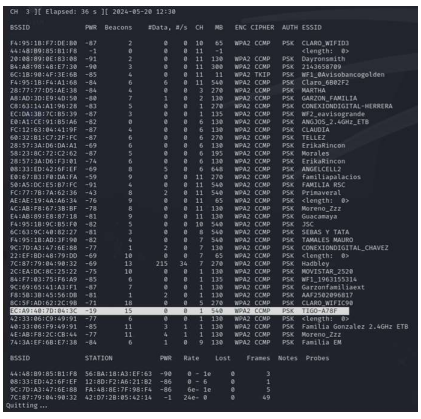


3.5 Fase 5 (Escaneo Aircrack-MG sobre red WIFI Domestica)

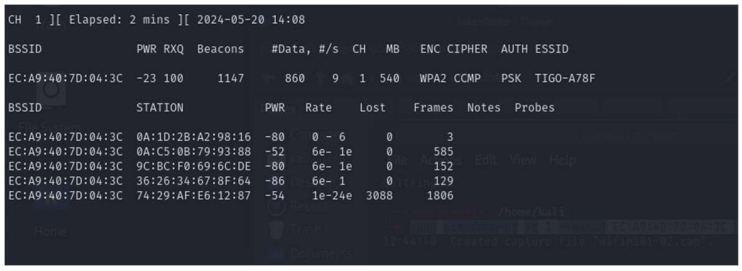
A través de una *Antena USB TP_LINK REF TL-WN7200N/150MB/*, se realiza la configuración de red en Kali Linux e instalación de librerías *aircrack-mg*. Se ajusta la red de la mv Kali-Linux en modo puente, para establecer la conexión entre la maquina física y la virtual. La tarjeta de red de la antena se configura en modo monitor (wlan0mon) para ver los dispositivos cercanos, se configura por DHCP con los DNS de Google.



Se inicia el escaneo y se observa la lista de redes que la antena logra captar:



Con Aircrack se ejecuta un escaneo selectivo de la red TIGO-A78F de propiedad de la Ing. Adriana Forero, identificando los siguientes dispositivos conectados a la red:

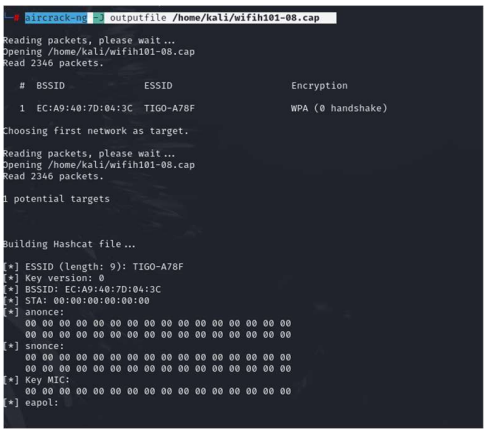


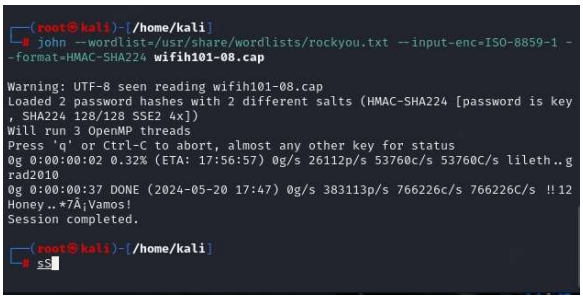
Al completar el escaneo de la red, Aircrack genera información del escaneo y la almacena en el archivo wifih101-08.cap.



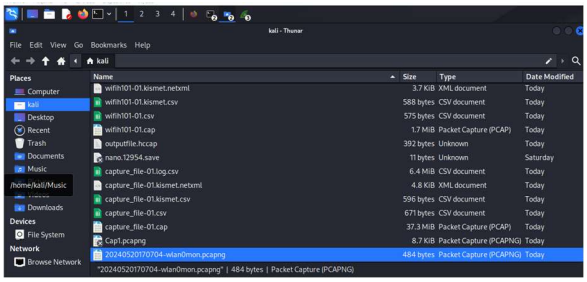
3.6 Fase 6 (Integración de *Aircrack* con *John The Ripper*)

Se carga el archivo *wifih101-08.cap* y se ejecuta un escaneo a través de la librería *John the Ripper* a fin de capturar el tráfico. Se integran las dos herramientas a través de la interfaz Wlan0mon, a continuación, se detalla la integración exitosa:

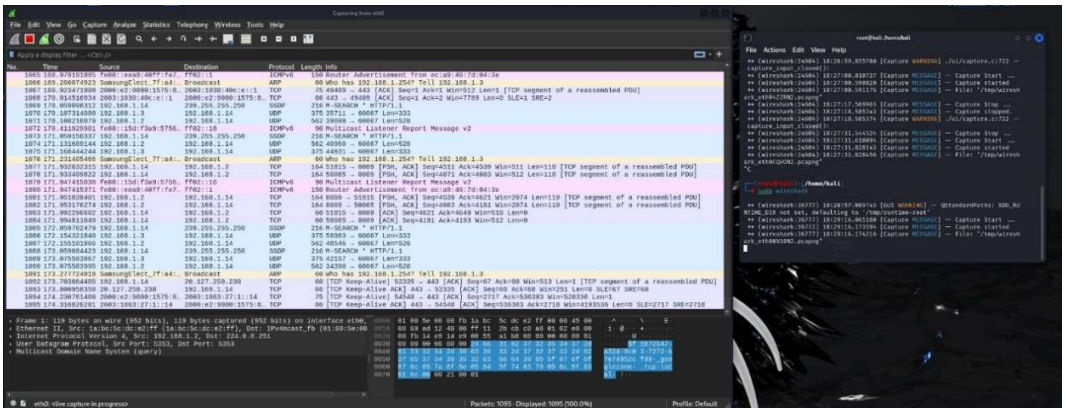




Finalizada la tarea se genera el archivo 20240520170704-wlan0mon.pcapng, que contiene el detalle de la captura del tráfico.



A través de whireshark se carga el archivo 20240520170704-wlan0mon.pcapng, se ejecuta el análisis de trafico de la red del televisor SAMSUMG IP 192.168.1.3.



Muestra de la información de conexiones:

Protocolo Ethernet II:

Dirección MAC de origen: 90:f1:aa:7f:a4:61 (SamsungElect_7f:a4:61)
Dirección MAC de destino: 01:00:5e:7f:ff:f6 (IPv4mcast_7f:ff:f6)

Protocolo IPV4:

Dirección IP de origen: 192.168.1.3
Dirección IP de destino: 239.255.255.246
Protocolo: IGMP (2)
Longitud total: 32 bytes
DSCP: CS6 (Clase de Servicio Diferenciado)

IGMP (Protocolo de Administración de Grupos de Internet):

Versión IGMP: 2
Tipo: Informe de membresía (0x16)
Tiempo máximo de respuesta: 0.0 seg
Dirección Multicast: 239.255.255.246

UDP:

Puerto de origen: 34313
Puerto de destino: 64968
Longitud: 341 bytes

4. Resultados

Vulnerabilidades con criticidad alta identificadas en el dispositivo:

CVE-2009-1925: describe una vulnerabilidad en ciertos televisores Samsung que podría permitir a un atacante ejecutar código arbitrario a través de un archivo de subtítulos especialmente diseñado. Es crítica porque podría permitir a un atacante tomar el control del televisor afectado al reproducir un archivo de subtítulos malicioso, comprometiendo así la seguridad del dispositivo.

Recomendación: Dado que se trata de una vulnerabilidad crítica y que puede ser explotada de forma remota, se recomienda la aplicación de parches de seguridad proporcionados, la implementación de filtros de firewall para bloquear tráfico malicioso y la actualización de políticas de seguridad para minimizar la exposición a amenazas externas.

CVE-2009-1918: La vulnerabilidad permite a atacantes remotos ejecutar código arbitrario mediante la manipulación de operaciones de tablas en un documento HTML. Esto se logra al agregar elementos malformados a un elemento DIV vacío, lo que provoca una corrupción de memoria. Esta vulnerabilidad se conoce como "HTML Objects Memory Corruption Vulnerability".

Recomendación: tomar medidas inmediatas para mitigar el riesgo. Esto puede incluir la aplicación de parches de seguridad proporcionados por fabricante, la actualización a una versión más reciente del navegador.

CVE-2014-2323: es una vulnerabilidad que afecta a ciertos modelos de televisores Samsung. Este problema de seguridad implica múltiples fallos en la validación adecuada de las entradas, lo que podría permitir a un atacante ejecutar código arbitrario en el dispositivo afectado. Esta vulnerabilidad impacta específicamente a los televisores inteligentes de Samsung, representando un riesgo significativo ya que podría ser explotada para la ejecución remota de código.

5. Conclusiones y recomendaciones

5.1 Conclusiones

Se identificaron vulnerabilidades en el televisor Samsung, dentro de ellas, puertos abiertos críticos y suites de cifrado SSL/TLS vulnerables, lo que podría exponer el dispositivo a diversos ataques cibernéticos.

En el reporte de la plataforma de OpenVas se detectaron 20 vulnerabilidades en total y 3 de ellas con una criticidad de 7.5/10, lo que indica un alto riesgo para la seguridad del dispositivo y la red doméstica.

Se destaca la importancia de actualizar el firmware del televisor para mitigar vulnerabilidades conocidas y mejorar la seguridad del dispositivo. Dos de las

vulnerabilidades reportadas en el cve hacen referencia a la actualización del firmware como mitigación. La falta de actualizaciones regulares podría dejar el televisor vulnerable a ataques cibernéticos.

Riesgos Asociados al Protocolo IGMP debido a que se detecto un riesgo potencial asociado al protocolo IGMP que podría detonar en posibles ataques de denegación de servicio (DoS) e interceptación de tráfico multicast en dispositivos IoT, como los televisores Smart.

Es importante utilizar cifrado SSL/TLS al conectar dispositivos IoT a servicios en línea para proteger la privacidad y la integridad de los datos transmitidos, ya que garantiza un protocolo seguro en la transmisión.

5.2 Recomendaciones

Cuando se trata de la seguridad en el hogar en relación con el uso de dispositivos IoT, como televisores inteligentes u otro dispositivo, es importante tener en cuenta las siguientes recomendaciones específicas:

1. Actualización regular del firmware: se debe asegurar que los dispositivos se utilicen con la última versión del firmware proporcionada por el fabricante. Las actualizaciones de firmware suelen incluir correcciones de seguridad que pueden abordar vulnerabilidades conocidas, incluidas aquellas relacionadas con los puertos SSL/TLS. En Smart TV se recomienda habilitar las opciones: Ajustes/ Actualización de Firmware o Actualización de Software/Busquemos la opción de habilitar actualizaciones automáticas para que se descarguen periódicamente.

2. Configuración segura del router: se sugiere solicitar al proveedor de servicio limitar el acceso a los puertos SSL/TLS y adicional utilizar contraseñas seguras para proteger la red Wi-Fi y cambiarlas periódicamente.

3. Habilitar el cifrado SSL/TLS: Asegurar que el dispositivo se encuentre configurado para utilizar cifrado SSL/TLS al conectarse a servicios en línea. Esto ayudará a proteger la privacidad y la integridad de los datos transmitidos entre otros dispositivos. Al aplicar la configuración seleccionar una versión SSL/TLS 1.2 o superior.

4. Desactivar servicios no utilizados: Si el equipo incluye servicios que no se usan, como aplicaciones de transmisión o funciones de red social, se recomienda desactivarlos para reducir la superficie de ataque y mejorar la seguridad general del dispositivo.

5. Utilizar una red de invitados: Si el router permite, se debe considerar configurar una red de invitados separada para dispositivos IoT. Esto ayudará a aislar los dispositivos IoT del resto de la red doméstica y reducirá el riesgo de compromiso de seguridad.

6. Configuración de firewall: configurar un equipo de borde en la red doméstica para monitorear y controlar el tráfico entrante y saliente hacia los dispositivos inteligentes. Esto puede ayudar a bloquear actividades maliciosas y proteger los datos personales, en el mercado existen soluciones gratuitas en el campo de cortafuegos, recomendamos las siguientes marcas pfSence, OPNsense, IPFire, FireHOL, entre otros

7. Conciencia de la seguridad: Educar a todos los miembros del hogar sobre las mejores prácticas de seguridad en línea y la importancia de proteger los dispositivos IoT, como los televisores inteligentes, contra posibles amenazas cibernética

Bibliografía

Comisión de regulación de telecomunicaciones CRCOM (2020). Monitoreo de tendencias tecnológicas y de consumidores. 7

Instituto Nacional de Ciberseguridad. (04 de 2019). *Normas APA*. Obtenido de *https://www.incibe.es/incibe-cert/blog/importancia-seguridad-iot-principales-amenazas*

Fúnez-Fernandez, E. (2022). *Diseño de un sistema de seguridad en el hogar basado en IoT y creación de prototipo.* 6

Sicajá, L. F., Morales, V. A., Velásquez, J. G., León, M., & Velásquez, N. O. El Impacto de las redes domésticas en la seguridad IoT.

Aplicación de metodología de seguridad en un entorno IoT doméstico. (12 de 2021). *Normas APA*. Obtenido de *https://openaccess.uoc.edu/handle/10609/138633*

García, A. A. (2019). Ciberseguridad:¿ Por qué es importante para todos?. 1-20

John the Ripper password cracker. *Normas APA*. Obtenido *https://www.openwall.com/john/*

Find my MAC Address. *Normas APA*. Obtenido https://macvendors.com/