Ciencia Latina Revista Científica Multidisciplinar
Marzo-Abril, 2023, Volumen 7, Número 2.
https://doi.org/10.37811/cl_rcm.v7i2.5763

Un breve Análisis de Vulnerabilidades en dispositivos IOT en Ecuador

Edison Jumbo[1]
edison.jumbo@epn.edu.ec
https://orcid.org/0009-0001-3245-8329
Escuela de Formación de Tecnólogos, Escuela Politécnica Nacional
Quito – Ecuador

Jefferson Llumiquinga
jefferson.llumiquinga@epn.edu.ec
https://orcid.org/0009-0007-9858-3046
Escuela de Formación de Tecnólogos, Escuela Politécnica Nacional
Quito – Ecuador

Fernando Uyaguari
fernando.uyaguari@wissen.edu.ec
https://orcid.org/0000-0001-7060-1002
Instituto Superior Tecnológico Wissen
Cuenca – Ecuador

Andrés Tenezaca
andres.tenezaca@wissen.edu.ec
https://orcid.org/0009-0006-9222-7094
Instituto Superior Tecnológico Wissen
Cuenca – Ecuador

Leandro Pazmiño
leandro.pazmiño@epn.edu.ec
https://orcid.org/0000-0002-9241-8409
Escuela de Formación de Tecnólogos, Escuela Politécnica Nacional
Quito – Ecuador

Richard Rivera
richard.rivera@wissen.edu.ec
https://orcid.org/0000-0002-5702-4965
Instituto Superior Tecnológico Wissen
Cuenca – Ecuador

RESUMEN

Este trabajo presenta un breve análisis de vulnerabilidades en dispositivos del Internet de las cosas (IoT) en Ecuador, mediante el desarrollo de una herramienta de software que busca direcciones IPv4 que están dentro del rango del territorio ecuatoriano y analiza los puertos de comunicación comunes de estas direcciones observando si dichos puertos están activos o abiertos exponiendo información sensible. Los resultados obtenidos durante el proceso de búsqueda de direcciones IPv4 han sido satisfactorios, encontrando información como: cámaras web, servidores Apache, páginas web e incluso petición de credenciales para acceder a la configuración de un router, con estos resultados se refleja que el nivel de seguridad informática en el Ecuador se encuentra en un nivel bajo. Considerando que Pichincha y Guayas, son las dos provincias más grandes del Ecuador, tienen la mayor cantidad de direcciones IPv4 con puertos activos y la mayor cantidad de exposición de información sensible sin medidas de seguridad.

Palabras clave: *IoT; IoT Ecuador; vulnerabilidades; IoT seguridad.*

[1] Autor Principal

A brief analysis of vulnerabilities in IoT devices in Ecuador

ABSTRACT

This paper presents a brief analysis of vulnerabilities in Internet of Things (IoT) devices in Ecuador, through the development of a software tool that searches for IPv4 addresses that are within the range of the Ecuadorian territory and analyzes their common communication ports, observing if those ports are active or open exposing sensitive information. The results obtained during the IPv4 address search process have been satisfactory, finding information from different devices such as: web cameras, Apache servers, web pages and even requests for credentials to access the router configuration, with these results it is reflected that the Information security level in Ecuador is at a low level. Considering that Pichincha and Guayas, are the two largest provinces in Ecuador, they have the largest number of IPv4 addresses with active ports and the largest amount of exposure of sensitive information without securities measures.

Keywords: *IoT; IoT Ecuador; vulnerabilities; IoT security*

Artículo recibido 20 marzo 2023

Aceptado para publicación: 05 abril 2023

1. INTRODUCCIÓN

El internet de las cosas (Internet of Things, en adelante IoT) hace referencia a dispositivos u objetos comunes que tienen la capacidad de conectarse a internet (Wignore, 2017). Durante los últimos años, se ha establecido la tendencia de tener cada vez más dispositivos interconectados a través de internet, con el objetivo de poder realizar de forma remota y/o automática acciones que permitan controlar tareas que se llevan a cabo de forma manual como el acceso a domicilios, control de luces, entre otros (INCIBE, 2019). Esto ha provocado una gran demanda de fabricación de dispositivos inteligentes con acceso a Internet, más conocidos como "dispositivos IoT". Un estudio realizado por IoT Analytics (Lueth, 2018) indica que en el 2018 existían alrededor de 7 mil millones de dispositivos IoT conectados en el mundo, y se espera que para el 2025 la cantidad de dispositivos IoT conectados aumente a 22 mil millones.

Actualmente, las funciones principales de los dispositivos IoT son captar, controlar, procesar y almacenar los datos, los dispositivos IoT suelen ser cada vez más pequeños (Chamorro & Rivera, 2019) (Pazmiño, et al., 2019), por lo que dependen de las puertas de enlace para poder comunicarse y ejecutar sus funciones (Cruz, 2016). Sin embargo, los dispositivos inteligentes desde un inicio no fueron diseñados para conectarse a Internet y esto provoca que sean más propicios a ciberataques; un ejemplo son los sistemas de control industrial (SCADA), que fueron diseñados para situarse en redes aisladas y actualmente se conectan a Internet (Corrales, 2017). Los mismos fabricantes de hardware se encargan del mantenimiento del software de los dispositivos IoT y gran parte de los fabricantes no disponen de la experiencia o recursos para poder responder ante posibles brechas de seguridad (Guevara R. R., 2014) o en algunos casos la seguridad no es una prioridad para ellos (Csirt-cv, 2014), (Rivera, Pazmiño, Becerra, & Barriga, 2021).

Por otro lado, los usuarios son conscientes de los problemas de seguridad que afectan a los dispositivos IoT, y así lo demuestra una encuesta realizada por Enjoy Safer Technology (ESET), donde el 70% de los participantes considera que este tipo de dispositivos no son seguros, fundamentalmente en términos de privacidad, que es donde radica la principal preocupación. Sin embargo, el 62% considera que no dejara de comprar este tipo de tecnología (Albors, 2018).

En Ecuador los dispositivos IoT todavía no se han posicionado masivamente como en otros países de

Europa (Jiménez & Rivera, 2021), Asia o América del Norte. Algunas operadoras móviles y empresas privadas ya están empezando a ofrecer algunos servicios que involucran a dispositivos IoT (Pazmiño, et al., 2019), sin tomar en cuenta, aspectos de seguridad (Guevara R. R., 2018) y privacidad con respecto a los servicios que ofrecen y la información que procesan. En la ciudad de Quito con el inicio de operaciones del Metro se espera que la cantidad de dispositivos IoT se incremente en gran medida (Pazmiño, et al., 2019), lo cual puede conllevar a un incremento de riesgos de la seguridad de la información, si estos dispositivos no consideran la seguridad como un aspecto fundamental de su despliegue.

Este proyecto tiene como objetivo desarrollar una herramienta que permita realizar un análisis de seguridad a dispositivos IoT conectados a Internet en el Ecuador, con la finalidad de obtener información sobre las vulnerabilidades más comunes y problemas de seguridad a los que se enfrenta el despliegue de dispositivos IoT en Ecuador. En este sentido, este objetivo pretende responder la siguiente pregunta de investigación. ¿Cuál es el nivel de seguridad de los dispositivos IoT desplegados en el Ecuador?

El presente artículo está estructurado de la siguiente forma. Luego de esta Introducción en la Sección 2, se presenta la Metodología que describe las fases de esta investigación. En la sección 3, se presentan los resultados y una discusión sobre estos. Finalmente, la Sección 4 presentar las conclusiones de este trabajo.

2. METODOLOGÍA

Esta investigación aplica un enfoque cuantitativo de tipo exploratorio, para alcanzar el objetivo planteado y conocer el nivel de seguridad de los dispositivos IoT desplegados en Ecuador. Para el desarrollo de esta investigación se realizaron dos fases que comprenden el desarrollo de una herramienta de software para recolección de datos expuestos a Internet en direcciones IP geolocalizadas en Ecuador. Segundo, la recolección y análisis de los datos recolectados.

Fase 1 - Desarrollo de la Herramienta de análisis.

Para el desarrollo de esta herramienta de software denominada “IoT-Ecuador”, se utiliza el método de investigación de caso de estudio mediante la utilización de la metodología de desarrollo de software ágil Scrum. Las metodologías ágiles son indispensables dentro del desarrollo de software (Pareja Quinaluisa,

2012) ya que aportan eficiencia, calidad, flexibilidad y una pronta y efectiva respuesta con los involucrados en el proyecto.

Scrum es una metodología de desarrollo ágil y flexible la cual permite abordar proyectos complejos desarrollados dentro de un entorno dinámico y cambiante, este tipo de metodología permite que los equipos de trabajo se organicen en base a las experiencias, todo esto se da bajo una serie de herramientas y recursos que ayudan al equipo para poder organizarse y se desempeñen con mayor agilidad (Galiana, 2021).

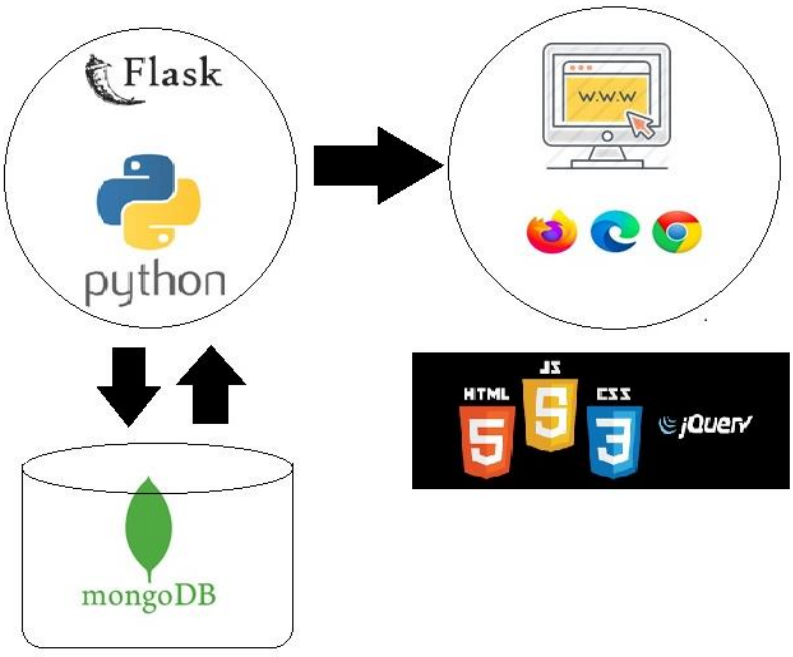
La herramienta IoT-Ecuador se desarrolla mediante la metodología *Scrum* la cual parte con un levantamiento de requerimientos plasmados en 15 Historias de Usuario (HU), estas son descripciones cortas y simples que describen una tarea concisa, mediante la cual se recoge información sobre la funcionalidad con la que contara el software, esto se da desde la perspectiva del usuario final o cliente (Rehkopf, 2021). La generación de las Historias de usuario es una de las tareas más importante porque permite determinar las necesidades de la herramienta, estas historias se organizan en el *Product Backlog* para determinar su importancia y asignarlas a cada una de las iteraciones del desarrollo las cuales se conocen como *Sprints*. En la **Tabla 1** se presenta el *Product Backlog*, donde se muestra para cada Historia de Usuario su identificador, el *Sprint* al que fue asignado considerando el flujo del desarrollo de los componentes del sistema y su prioridad.

Tabla 1. Product Backlog

ID-HU	HISTORIA DE USUARIO	Sprint	Prioridad
HU001	Inicio de Sesión del usuario	4	Baja
HU002	Búsqueda de direcciones IPv4	1	Alta
HU003	Recolección de direcciones IPv4	2	Media
HU004	Actualización de direcciones IPv4	1	Alta
HU005	Capturas de pantalla de puertos abiertos	1	Alta
HU006	Visualizar página informativa en el Sistema Web	4	Media
HU007	Registro de usuarios	4	Baja
HU008	Editar Cuenta	4	Baja
HU009	Iniciar y cerrar sesión de Administrador	3	Media
HU010	Activación de cuenta	3	Media
HU011	Visualizar direcciones IPv4 encontradas	4	Alta
HU012	Visualizar los detalles de cada dirección IPv4	4	Alta
HU013	Búsqueda y filtrado de direcciones IPv4	4	Alta
HU014	Visualizar los resultados de la búsqueda	4	Alta
HU015	Análisis de puertos por ciudad	4	Alta

La herramienta de software desarrollada comprende dos componentes diferenciados. El primero, es un Script de búsqueda de direcciones IPv4; el segundo, es el Sistema Web para visualizar y analizar los resultados de la ejecución de la herramienta. El Script de búsqueda es desarrollado en su totalidad en Python, un lenguaje de programación multiplataforma de código limpio y versátil. Por otra parte, el desarrollo del Sistema Web que permite visualizar, buscar y detallar las direcciones IPv4 ha sido desarrollado mediante Flask, este es un *Microframework* para Python que permite trabajar con el patrón de diseño arquitectónico Modelo-Vista-Controlador (MVC). Esta arquitectura del software permite separa los datos de una aplicación, la interfaz de usuario y la lógica en 3 componentes distintos (Universidad de Alicante, s.f.). En la **Figura 1** se muestra el patrón de arquitectura que se implementa para el desarrollo de la herramienta y el sistema web esto en función a las herramientas utilizadas.

Figura 1. *Patrón Arquitectónico del Sistema Web.*



Para el desarrollo de los dos componentes se utilizaron varias librerías que nos permitieron interactuar con las herramientas del patrón arquitectónico MVC cumpliendo las Historias de usuario de una manera más rápida, aplicando el principio de la ingeniería de software de la reutilización, estas incluyen PyMongo, Ice-cream, Loggins, Sockets, DNS, Selenium, PygeoIP, IPWhois.

Fase 2 – Recolección y análisis de los datos.

Una vez que se ha completado el desarrollo de los dos componentes de la herramienta de software, para recolectar los datos se procede a su ejecución de acuerdo con el flujo que se describe a continuación.

El usuario administrador puede directamente ejecutar el Script para empezar la búsqueda de direcciones IPv4, estas son filtradas de acuerdo con su geolocalización en territorio ecuatoriano. Esto permite popular la base de datos no relacional MongoDB para que posteriormente puedan ser visualizados los datos en el Sistema Web. En la Figura 2 se muestra el inicio de ejecución del Script.

Figura 2. *Inicio de la ejecución de la Herramienta IoT Ecuador.*

El sistema permite hacer una búsqueda de direcciones de forma aleatoria o analizar los puertos abiertos de una dirección específica proporcionada por el administrador desde la interacción del Script o desde el sistema web por un usuario final. Si una dirección IPv4 que se quiere analizar previamente ya ha sido analizada hace menos de 30 días solo se entrega la información desde la base de datos, si el análisis es más antiguo, se realiza un nuevo análisis de los puertos. El usuario administrador determina que se van a realizar capturas de pantalla en todos los puertos abiertos que lleguen a tener cada dirección IPv4, esta función se la realiza mediante Selenium para poder obtener dichas capturas de los puertos. En la Figura 3, se muestra el análisis 568 realizado a una dirección IP de Ecuador donde se encuentra tres puertos abiertos y se procede a obtener las capturas de pantalla de la información recolectada en esos puertos.

Figura 3. *Ejecución de la herramienta.*

Por otra parte, el sistema web permite el registro e ingreso de usuarios. Dada la confidencialidad de la información que se recolecta y como el sistema es desarrollado con fines académicos para poder acceder al sistema cada cuenta de usuario debe ser aprobada por el administrador, de esta forma un usuario puede acceder al Sistema Web mediante correo y contraseña para tener el permiso de uso en el filtrado y búsqueda de direcciones IPv4. El usuario final puede observar las direcciones IPv4, los puertos recolectados por el Script y realizar una búsqueda filtrada por medio de los siguientes parámetros: dirección, puerto, geolocalización; un ejemplo de esto se muestra en la Figura 4, donde se realiza una búsqueda por el parámetro ciudad desde el Sistema Web, en esta se puede apreciar que para cada dirección IP analizada, se presenta la ciudad en la que esta ubicada, las fechas de los análisis y los puertos abiertos que se encontraron.

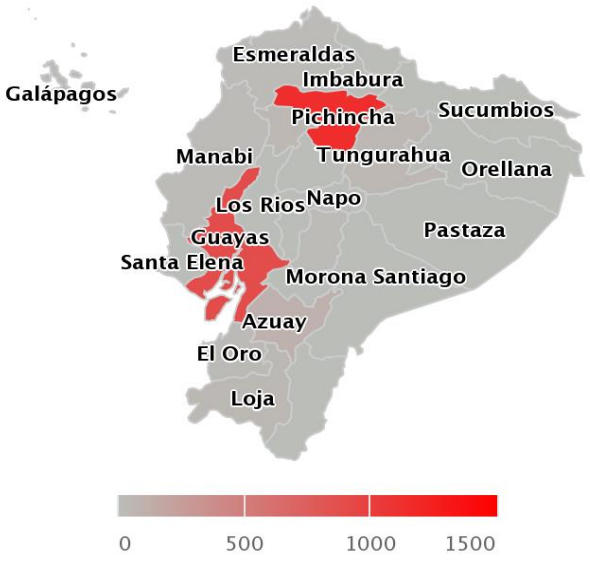
Figura 4. *Búsqueda por el parámetro ciudad "Quito".*

3. RESULTADOS Y DISCUSIÓN

Luego de obtener los datos recolectados durante la segunda fase de la metodología descrita en la sección anterior, en esta sección se describen algunos de los resultados principales y se da respuesta a la pregunta de investigación.

De acuerdo con IP2Location, Ecuador tiene 2 801 920 direcciones IP asignadas (IP2Location.com, 2022). Para obtener una muestra significativa de direcciones IP del Ecuador, se utiliza el sistema para recolectar información de 100 000 direcciones aleatorias, verificando que se encuentren dentro del territorio del país. En la Figura 5, se muestra un mapa de las direcciones IP con puertos activos por provincias del Ecuador, notando que como se esperaba la gran mayoría de estas se encuentran en las dos provincias principales del país como son Pichincha y Guayas con 1 137 y 879 direcciones respectivamente. Hay varias provincias que no presentan puertos activos como es el caso de todas las provincias del Oriente ecuatoriano que incluyen a Sucumbíos, Orellana, Pastaza, Morona Santiago y Zamora Chinchipe, en la Sierra Cotopaxi, Bolívar y Cañar y en la Costa solo la provincia de Los Ríos no presenta puertos activos es sus direcciones IP analizadas. Por otra parte, la provincia del Azuay alcanza un valor de 99 puertos activos y las demás provincias presentan esta situación en un rango que va de 1 a 40 direcciones IP con puertos activos.

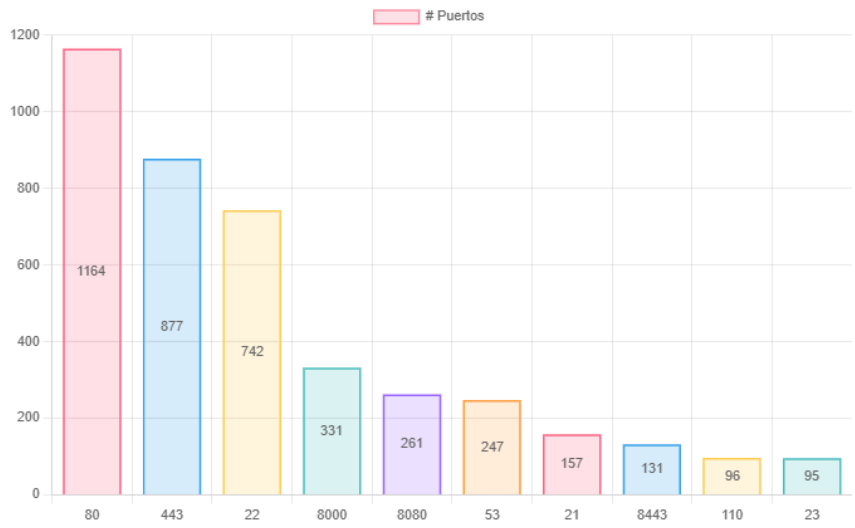
Figura 5. *Mapa de direcciones IPv4 con puertos activos.*



Para entender mejor la problemática cuando se realiza la búsqueda en el Sitio Web desarrollado, se presenta un gráfico de barras que se muestra en la Figura 6, donde también como era de esperarse los

puertos activos más comunes son el puerto 80 y el 443 con 1164 y 877 respuestas activas, estos puertos de comunicación son los que por defecto se utiliza para sitios web respondiendo a los protocolos de comunicación HTTP y HTTPS respectivamente. Si bien esto es algo común, que un servicio web este expuesto a Internet, el que no se utilice comunicaciones seguras en todos los casos, presenta una brecha de seguridad pues dichas comunicaciones son susceptibles de ataques de seguridad como un ataque de hombre en el medio. Otros puertos que también se encuentran activos, pero en menor medida son el puerto 22, utilizado comúnmente para conexiones remotas mediante el protocolo SSH; los puertos 8000, 8080 y 8443, típicamente utilizados por servidores web en lugar de utilizar los puerto por defecto de los protocolos HTTP y HTTPS; el puerto 53, utilizado por el servicio de DNS, el puerto 21, utilizado por el protocolo de transferencia de archivos FTP; el puerto 110, que suele ser utilizado para el protocolo de correo electrónico POP; y el puerto 23 utilizado por el protocolo de comunicación Telnet.

Figura 6. *Cantidad de puertos abiertos por puertos comunes.*

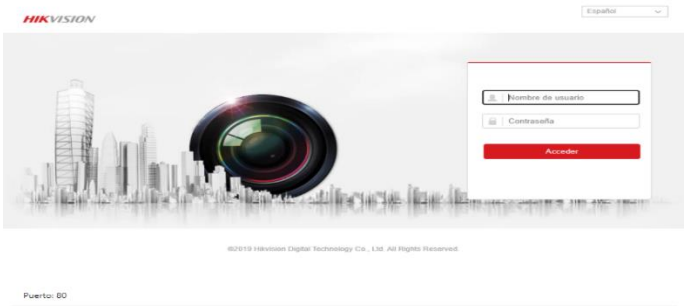


Como se menciona anteriormente, que los puertos utilizados por servidores web estén expuestos de forma pública en Internet no es como tal un problema de seguridad, el problema se presenta por la información que están exponiendo, en nuestro análisis la herramienta al recolectar las capturas de pantalla de lo que exponen estos servicios en los puertos activos nos encontramos con diversos sistemas que incluyen servidores web inicializados, sin ningún sitio Web activo, es decir que la captura detecta la pantalla por defecto que se obtiene cuando se levanta un servidor web de Apache o Internet

Information Services. Esto podría presentar una brecha de seguridad para las organizaciones dueñas de estas direcciones IP porque el tener un servidor web activo manteniendo las configuraciones por defecto, permitiría que un atacante aproveche esta vulnerabilidad.

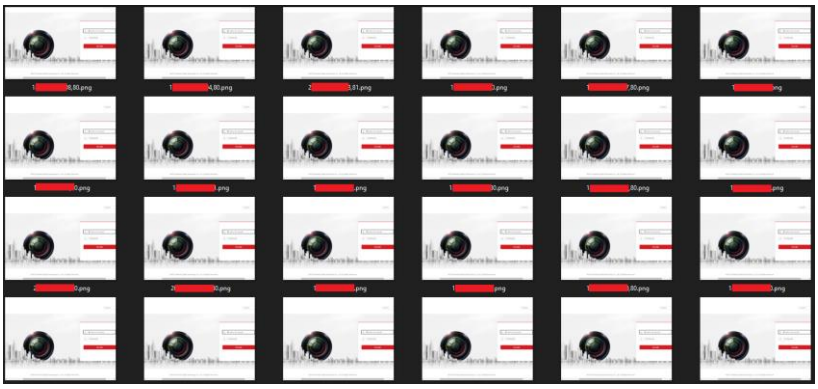
Otro tipo de sistema que encontramos son los sistemas de acceso a cámaras IP, lo cual en principio es el propósito de estos dispositivos que el usuario pueda acceder a estas desde cualquier lugar, en estos casos la vulnerabilidad que se puede presentar es que los usuarios estén usando las credenciales de acceso por defecto, lo que permitiría que un atacante pueda acceder directamente al sistema. En la Figura 7, se muestra la captura de pantalla de la imagen de una dirección con un puerto activo donde podemos ver el acceso a una cámara IP de la marca HIKVISION, esta es una situación bastante común, en los datos analizados, ya que encontramos 63 direcciones IP distintas que exponen públicamente el sitio de inicio de sesión de estas cámaras, un detalle de esto se muestra en la Figura 8, donde se presenta un captura de pantalla del directorio donde la herramienta de software almacena las capturas de pantalla que realiza durante los escaneos.

Figura 7. *Captura de pantalla de una cámara web expuesta a Internet.*



Un sistema encontrado que es aún más preocupante son los sistemas de acceso web a routers, en los cuales potencialmente podría presentarse el mismo problema anterior de las credenciales por defecto, pero en este caso no solo se podría acceder a un dispositivo, si no se podría acceder potencialmente a todos los dispositivos dentro de una red. Sobre este mismo contexto, lo más extremo fue encontrar accesos a 5 routers que por defecto no tenían configurado el acceso mediante credenciales, es decir que se tiene acceso directo al sistema RouterOS a través del puerto 80, permitiendo que cualquier persona en Internet pueda administrar este dispositivo.

Figura 8. *Dispositivo más común encontrado en más de 63 direcciones IP.*



Estos hallazgos que se presentan en este análisis indican que de las 100 000 direcciones IPv4 analizadas, 2 560 direcciones presentan puertos de comunicación abiertos, esto representa el 2,56% de direcciones que potencialmente podría presentar una vulnerabilidad. Como se menciono antes, no es un problema que se encuentre un servidor web, el acceso a una cámara IP, acceso a servicios de Webmail, acceso a dispositivos de red como routers, pues en muchos casos ese es el propósito de un servicio web. El problema se presenta al utilizar protocolos inseguros, inadecuadas configuraciones de sus servicios, configuraciones por defecto de los dispositivos. Este porcentaje que se indica aún cuando es muy bajo consideramos que actualmente debería ser mucho menor.

Considerando aspectos legales y éticos de la seguridad de la información, nuestro sistema únicamente toma una captura de pantalla de los servicios web que están expuestos a Internet, cuando no hay una respuesta de un servidor web, pero el puerto esta activo, nuestra herramienta de software también captura la información del banner, para obtener más información sobre los servicios que se ejecutan en estos puertos abiertos. Hasta ese punto llega nuestro sistema, ya que un atacante podría continuar probando algunos de los problemas de seguridad que hemos mencionado a lo largo de este estudio, o incluso ataques más sofisticados.

4. CONCLUSIONES

En este trabajo se presenta un breve análisis de la seguridad de los dispositivos IoT en el Ecuador, centrando el estudio en los puertos de comunicación abiertos y expuestos al público que mantienen en estos dispositivos. Para esto se desarrolla una herramienta de software aplicando la metodología de desarrollo de software ágil SCRUM, con esta herramienta se recolecta información sobre los puertos

abiertos de 100 000 direcciones IP, donde se encuentra 2560 direcciones con puertos abiertos de forma pública, en su mayoría estos representan dispositivos de cámaras de seguridad, servidores web, accesos a routers, entre otros; donde varios dispositivos se encuentran sin implementar ningún mecanismo de seguridad. Si bien el porcentaje de direcciones IP analizadas representa solo el 3% del total de direcciones IPv4 que se estima que existen en el Ecuador, este estudio indica que de la muestra analizada el 2.56% de direcciones IP presentan un bajo nivel de seguridad.

Los datos obtenidos durante este análisis pueden generar mucha más información que motiva a continuar con esta investigación en trabajos futuros. En estos se podría analizar las fechas estimadas del firmware de algunos dispositivos expuestos a Internet, dado que comúnmente esta información aparece en el Copyright de las capturas de pantalla, donde nuestro análisis indica que hay algunos dispositivos que mantienen un software de antes de 2010. Por otra parte, al profundizar en la información recolectada, se podría extender el estudio no solo para un conjunto de direcciones aleatorias, si no para todas las direcciones IP del Ecuador e incluso otros países de Latinoamérica, adicional se podría analizar en detalle la respuesta de la recolección de banners que realiza la herramienta cuando un servicio que se ejecuta en un puerto activo responde. Estos futuros trabajos se plantean siempre manteniendo los aspectos éticos y legales de un estudio académico relacionado con la seguridad de la información.

5. BIBLIOGRAFÍA

Albors, J. (25 de 07 de 2018). *ESET*. Recuperado el 22 de 10 de 2019, de https://www.welivesecurity.com/la-es/2018/07/25/seguridad-iot-a-tiempo-ganar-batalla

Calles, A. (8 de Diciembre de 2016). *FluProject*. Obtenido de https://www.flu-project.com/2016/12/construyendo-nuestro-propio-escaner-de.html

Chamorro, V., & Rivera, R. (2019). Twitter mining for multiclass classification events of traffic and pollution. *International Conference on Human Systems Engineering and Design: Future Trends and Applications.* Munich.

Corrales, L. P. (05 de 10 de 2017). *BIBDIGITAL-EPN*. Recuperado el 20 de 11 de 2019, de https://bibdigital.epn.edu.ec/handle/15000/10020

Cruz, E. V. (13 de 05 de 2016). Recuperado el 12 de 11 de 2019, de https://www.edgarvasquez.com/Vulnerabilidad-internet-de-las-cosas

Csirt-cv. (23 de 12 de 2014). Recuperado el 01 de 11 de 2019, de http://www.csirtcv.gva.es/es/noticias/csirt-cv-publica-el-informe-%E2%80%9Cseguridad-en-internet-de-las-cosas%E2%80%9D.html

De la Vega, R. (26 de Enero de 2021). *Pharos*. Obtenido de https://pharos.sh/integrar-mongodb-con-python-usando-pymongo/

Dnspython. (05 de Julio de 2020). *Dnspython*. Obtenido de https://www.dnspython.org/about/

Espinosa, O. (9 de Diciembre de 2019). *RedesZone*. Obtenido de https://www.redeszone.net/tutoriales/internet/que-es-whois/

Fernandez, R. (17 de Abril de 2020). *Unipython*. Obtenido de https://unipython.com/programacion-de-redes-en-python-sockets/

Galiana, P. (20 de 04 de 2021). *IEBS*. Obtenido de https://www.iebschool.com/blog/metodologia-scrum-agile-scrum/

Guevara, R. R. (2014). *ANÁLISIS DE CARACTERÍSTICAS ESTÁTICAS DE FICHEROS EJECUTABLES PARA LA CLASIFICACIÓN DE MALWARE*. UNIVERSIDAD POLITÉCNICA DE MADRID.

Guevara, R. R. (2018). *Tools for the detection and analysis of potentially unwanted programs.* España: (Doctoral dissertation, Tesis doct. Nov. de 2018. doi: 10.20868/UPM. thesis.53395). doi:10.20868/UPM.thesis.53395

INCIBE. (25 de 04 de 2019). *incibe-cert*. Recuperado el 06 de 11 de 2019, de https://www.incibe-cert.es/blog/importancia-seguridad-iot-principales-amenazas

Ionos, D. G. (07 de Julio de 2021). *Digital Guide Ionos*. Obtenido de https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/logging-de-python/

Jiménez, C., & Rivera, R. (2021). Ciberseguridad del IoT: Un Análisis en Países de la Unión Europea. (A. I. Informacao, Ed.) *Revista Ibérica de Sistemas e Tecnologias de Informação*(E39), 461-476.

Lueth, K. L. (08 de 08 de 2018). *IOT ANALYTICS*. Recuperado el 30 de 10 de 2019, de https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b

Mohammad, W. (11 de Mayo de 2021). *Browserstack*. Obtenido de https://www.browserstack.com/guide/take-screenshot-with-selenium-python

Pareja Quinaluisa, J. F. (08 de 02 de 2012). *Evaluación de procesos de software utilizando EvalProSoft Aplicado a un caso de estudio*. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/4491

Pazmiño, L., Flores, F., Ponce, L., Zaldumbide, J., Parraga, V., Loarte, B., . . . Rivera, R. (2019). Challenges and Opportunities of IoT Deployment in Ecuador. *2019 International Conference on Information Systems and Software Technologies (ICI2ST)* (pp. 108-115). Quito: IEEE.

Rehkopf, M. (2021). *Atlassian*. Obtenido de https://www.atlassian.com/es/agile/project-management/user-stories

Rivera, R., Pazmiño, L., Becerra, F., & Barriga, J. (2021). An Analysis of Cyber Espionage Process. *Developments and Advances in Defense and Security. Proceedings of MICRADS 2021*. Cartagena.

Tran, K. (13 de Enero de 2021). *Towards Data Science*. Obtenido de https://towardsdatascience.com/stop-using-print-to-debug-in-python-use-icecream-instead-79e17b963fcc

Universidad de Alicante. (s.f.). Recuperado el 10 de 07 de 2021, de https://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html

Wignore, I. (02 de 09 de 2017). *techtarget*. Recuperado el 19 de 11 de 2019, de https://searchdatacenter.techtarget.com/es/definicion/Internet-de-las-cosas-IoT