UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del artículo
COMPARATIVA DE LAS PRINCIPALES VULNERABILIDADES DE DOMINIOS DE ISP EXTRAÍDOS MEDIANTE API'S PÚBLICAS
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación
Autora:
Trujillo Morales Andrea Paulina
Tutor:
MSc. Recalde Varela Pablo Marcel

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Marcel Recalde Varela con C.I: 171168505-5 en mi calidad de Tutor del proyecto de investigación titulado: Comparativa de las principales vulnerabilidades de dominios de ISP extraídos mediante API's públicas.

Elaborado por: Trujillo Morales Andrea Paulina, de C.I: 1721648606, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2022

_____

Firma

ORCID: 0000-0003-4710-1178

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Trujillo Morales Andrea Paulina con C.I: 1721648606, autora del proyecto de titulación denominado: Comparativa de las principales vulnerabilidades de dominios de ISP extraídos mediante API's públicas. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2022

Firma

ORCID: 0000-0003-4710-1178

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Actualmente la tecnología ha evolucionado a gran escala, siendo así que casi todos los usuarios de una empresa, una familia, etc, tienen acceso a la misma mediante teléfonos móviles, laptops, tablets, básicamente cualquier equipo que disponga de Internet (Vulnerabilidades de sitios web gubernamentales en Ecuador, 2019) y así mismo las empresas públicas y privadas han creado sitios web para mejorar los servicios que brindan a los usuarios, pero dichos sitios no siempre son implementados por personal especializado, hosting confiables y que se tome en cuenta las medidas de seguridad para que no sean vulnerados, para esto sería de gran utilidad tener el conocimiento de las vulnerabilidades a las que están expuestos los sitios web (García, 2019).

Existen varias herramientas públicas de pruebas de penetración (pentesting) que sirve para analizar sitios web expuestos al mundo pero no se consolidan en dashboards (Pallarés, 2021), esto ocasiona que los usuarios no puedan visualizar la comparación de las vulnerabilidades encontradas por las diferentes herramientas.

En el año 2020 con la declaración de la pandemia de SARS-COV-2 casi todas las empresas entre públicas y privadas incrementaron sus servicios web por el hecho que no se podía salir a realizar ningún trámite o compra, así como aumentaron los servicios web aumentaron los ciberataques siendo Ecuador uno de los países que ha tenido varios ataques cibernéticos a entidades financieras, gubernamentales, ISP (Internet Service Providers), ocasionando pérdida o robo de información, suspensión parcial o total de los servicios, incomodidad hacia el usuario y pérdida de confiabilidad (Vulnerabilidades de sitios web gubernamentales en Ecuador, 2019).

Una de las herramientas que se pueden utilizar para el análisis de sitios web en Internet es Shodan, fácil de usar, accesible con una cuenta gratuita y la información que se obtiene por la búsqueda se puede acceder mediante API (Application Programming Interface) (Palencia, 2021), con este buscador especializado se puede visualizar las vulnerabilidades que puede tener determinado sitio web (Fernández y Hernáiz, 2018).

Problema de investigación

Todas las empresas que brindan algún servicio a la comunidad en algún momento registran los datos de sus clientes, mismos que son utilizados para entregas a domicilio y ventas en línea, cuando los clientes ingresan por la Uniform Resource Locator (URL) de la página web están confiando en que los datos que han ingresado están siendo resguardados por el proveedor del servicio, lo que lleva a cuestionar a los usuarios.

¿Cómo influyen las vulnerabilidades asociadas a los nombres de los sitios web que gestionan los ISP, en el control de la seguridad de los clientes?

Objetivo general

Comparar las vulnerabilidades asociadas a los nombres de los sitios web que gestionan los ISP, en el control de la seguridad de los clientes

Objetivos específicos

Identificar las vulnerabilidades más comunes que tienen los nombres de los sitios web de los ISP que son visualizadas por el mundo mediante la utilización de API públicas.

Evaluar los puertos que son expuestos en los nombres de los sitios web de los ISP.

Definir qué información de los clientes puede ser sustraída por las diferentes vulnerabilidades encontradas en los nombres de los sitios web de los ISP.

Vinculación con la sociedad y beneficiarios directos:

El presente trabajo tiene como objetivo vincular a la sociedad con la tecnología en temas de seguridad. En la actualidad con la aparición de la pandemia del SARS-COV-2 se ha podido evidenciar que era necesario evolucionar en la tecnología de forma acelerada, muchos negocios tuvieron que implementar páginas web para seguir a flote y continuar brindando servicios a sus clientes, pero esta evolución en la mayoría de los casos fueron implementados por personas con poco conocimiento de seguridad o sin las debidas seguridades, lo que ocasiona que los negocios sean suplantados por los delincuentes informáticos haciendo que afecte a las empresas y colateralmente a los clientes.

El proyecto de investigación plantea mostrar las vulnerabilidades obtenidas de diferentes API públicas de los nombres de sitios web, con el fin de que los usuarios que los administran puedan analizar las medidas a tomar y comparar las vulnerabilidades que se pueden observar mediante Internet y que pueden ser explotadas por cualquier delincuente informático. Esto no sustituye a los antivirus, firewalls, desarrollo seguro, etc, pero permitirá tener información de primera mano de lo que se puede observar y que pueden mitigar sea corrigiendo internamente en la empresa o contratando servicios de seguridad.

CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

1.1. Contextualización general del estado del arte

Con el paso de los años se ha evidenciado que la tecnología se va haciendo parte de nuestra vida diaria así como en el trabajo, hogar, educación, salud, etc y por tanto toda la información se ha convertido en un bien muy preciado que genera gran interés para los delincuentes que también han evolucionado ya que no se encuentran solo en las calles, al momento son delincuentes informáticos que se encuentran a la espera de un descuido en los usuarios de la tecnología, puertos expuestos al Internet que no son necesarios, claves débiles o claves por defecto, falta de software o hardware de seguridad (Zelada, 2022).

Los delincuentes informáticos generalmente antes de atacar realizan ingeniería social para poder identificar a su víctima, análisis de puertos y redes por donde podrán acceder y tomar control de la información, de los dispositivos y afectar los servicios que se brinden a los usuarios, por tal motivo también han evolucionado muchas aplicaciones y buscadores para el análisis de vulnerabilidades mismas que pueden ser físicas, sitios web, lógicas, etc, el propósito de estas aplicaciones o buscadores es ayudar a los usuarios de la tecnología a cuidar la información personal como empresarial (Avances de la Ciberseguridad y el Cibercrimen desde la realidad de Ecuador [Parte 2/4], 2021).

Dependiendo el análisis de vulnerabilidades que se requiera realizar existen las aplicaciones o buscadores especializados, en esta investigación se centrará en tres buscadores públicos especializados que pueden ser usadas por cualquier usuario con el fin de verificar las vulnerabilidades o puertos que se encuentran expuestos al Internet con respecto a los sitios web de ISP.

En el año 2020 todo el mundo fue impactado por el virus mortal del SARS-COV-2, ocasionando que las personas no puedan salir a realizar compras, pagos de servicios, realicen teletrabajo o teleducación y esto ocasionó que la evolución de la tecnología avance a pasos gigantescos, este impacto se evidenció en que las empresas para poder subsistir durante la pandemia implementarán sitios web para que los usuarios puedan realizar las compras o pagos online, pero la mayoría de los sitios web por la premura de su implementación no se encuentran implementadas con las debidas seguridades o se encuentran publicados en servidores que tiene muchos puertos abiertos que no son necesarios y publicados hacia el Internet, con esta información cualquier atacante puede utilizarla para obtener información, suplantar identidad, interferir con los servicios que brinde la empresa (Zelada, 2022). Las empresas pueden realizar análisis interno de los nombres de sus sitios web mediante la utilización de motores de búsqueda especializados en

vulnerabilidades y que son de uso público como Shodan, Censys y VirusTotal, para poder determinar las acciones que se debe seguir.

Shodan, Censys y VirusTotal son motores de búsqueda especializada en equipos conectados o expuestos al Internet, la ventaja que tienen estos motores es que se puede obtener información por la API que disponen, solo con el registro en la plataforma, esta data se encuentra almacenada en la base de datos de los motores de búsquedas y facilitan la extracción para el usuarios que se encargará del análisis.

En los motores de búsqueda de Shodan y Censys se puede analizar nombres de sitios web e identificar los puertos expuestos y vulnerabilidades, la ventaja que se extraer la data mediante el API que ambos motores disponen, la desventaja de Shodan es que el API tiene un límite para los usuarios gratuitos pero es suficiente como para un primer análisis (Drago, 2016).

VirusTotal es un buscador especializado y también una herramienta ya que dentro de sus características tiene antivirus y motores de detección (Fernández, 2018), también dispone de una API que permitirá extraer la data y compararla con la información obtenida de las otras API

En la actualidad se ha podido observar que las aplicaciones se comunican mediante API con otras aplicaciones sin necesidad que los desarrolladores tengan que volver a crear aplicaciones para validar pagos, publicar mensajes en redes sociales u obtener datos que luego serán utilizados para presentar análisis, etc, la comunicación entre las API se da mediante el protocolo http (*What Is an API?*, 2022).

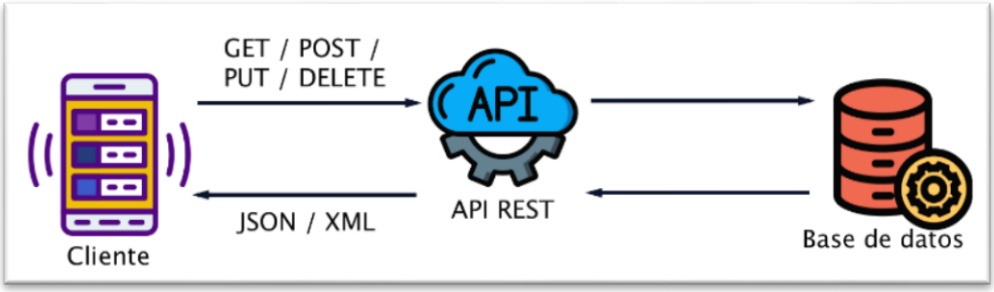
Las API permiten la comunicación fluida entre aplicaciones aunque pueden tener sus restricciones mismas que son configuradas por los desarrolladores propietarios del API, estas restricciones en ocasiones es para limitar el número de usuarios que pueden utilizarla o cantidad de datos a consultar (Fernández, 2019), esto generalmente sucede cuando se vuelven populares en su uso y también para implementar nuevos servicios.

Las API pueden ser privadas, entre socios de negocios y públicas, generalmente las privadas se utilizan dentro del mismo entorno empresarial permitiendo que todas las aplicaciones de la empresa utilicen la misma información como sea necesaria, mientras que las API entre socios se puede utilizar conforme el giro del negocio lo necesite como por ejemplo el API de Paypal y las públicas son utilizadas por cualquier usuario que tenga acceso al Internet e incluso puede mejorar el API cuando permiten el desarrollo colaborativo (*What Is an API?*, 2022).

Al momento se utilizan las API REST ya que cumple con un estilo arquitectónico y la respuesta de los mensajes generalmente son en formato JavaScript Object Notation (JSON) que ayudan al desarrollador a entender la información que está obteniendo para luego extraerla con el lenguaje de programación que el desarrollador lo requiera (*What Is an API?*, 2022) como se muestra en la Figura 1.

Figura 1

Funcionamiento del API REST



Nota: Adaptado de *Funcionamiento del API REST***,** por ¿Qué es una api rest? ¿Cómo funciona? ¿En que tipo de web utilizarlas? (2021, diciembre 21). *Dos Setenta: Agencia de Marketing Online y Desarrollo Web y Consultoría Digital*. https://dossetenta.com/que-es-una-api-rest/

Los motores de búsqueda especializados cómo Shodan, Censys y VirusTotal permiten utilizar API REST para poder obtener los datos que se requiera y poder analizar los puertos que se tienen expuestos o las vulnerabilidades de los servidores que son encontrados en los motores de búsqueda.

1.1.1. Motor de búsqueda Shodan

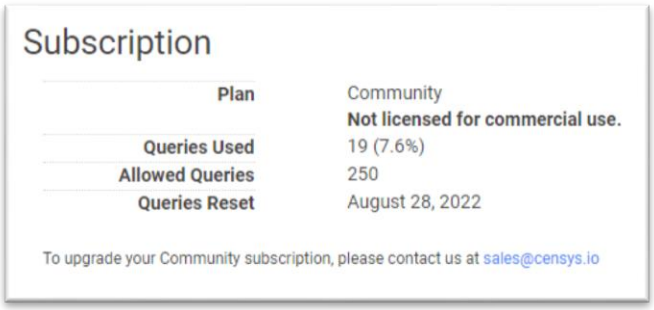
En el caso de Shodan con una cuenta sin costo solo con registro se puede observar información entre los top 5, es decir solo los datos más relevantes, en el caso que se realice una búsqueda con muchos filtros o preguntas (query) solicita actualizar la cuenta a una de pago, pero si se puede realizar búsquedas individuales siempre y cuando los resultados no sean muy extensos.

1.1.2. Motor de búsqueda Censys

El motor de búsqueda Censys permite registrarse y generar un key sin costo que permite realizar varias consultas mediante el API hasta un límite que es reseteado cada mes, como se indica en la figura 2.

Figura 2

Subscripción plan comunitario



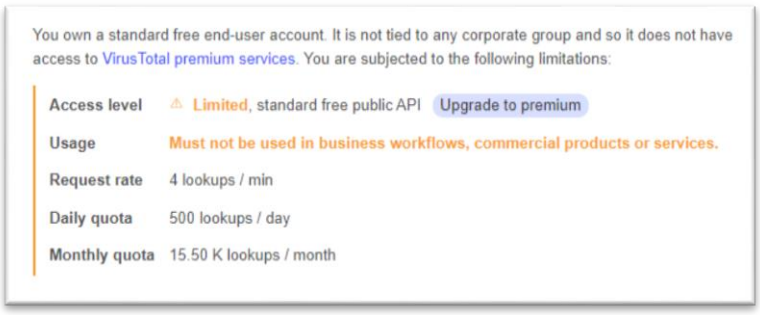
Nota: Autoría propia

1.1.3. Motor de búsqueda VirusTotal

El motor de búsqueda Virustotal, al igual que los otros motores antes mencionados genera un key sin costo con solo registrarse que permite realizar algunas búsquedas con restricciones por día y por mes como se indica en la figura 3.

Figura 3

API con límite Standard



Nota: Autoría propia

1.2. Proceso investigativo metodológico

El proceso de investigación que se utilizará para el problema planteado se basa en los siguientes puntos:

Diseño no experimental - transversal se utilizará para los nombres de los sitios web de los ISP ya se encuentran en funcionamiento y las vulnerabilidades y puertos serán mostrados en el instante de tiempo que se realice la consulta al API de los motores de búsqueda avanzada para poder determinar las diferentes soluciones que los usuarios deben realizar o solicitar asesoría según sea el caso.

Muestreo: se plantea sea Intencional ya que se va a aplicar para los nombres de los sitios web de los ISP más conocidos en el país como netlife.ec, puntonet.ec, cnt.com.ec, telconet.net con el fin escanear las vulnerabilidades y los puertos que tengan expuestos al Internet y que los puedan visualizar en dashboards.

Comparativo: se mostrará en los paneles de la aplicación Grafana ya que los datos obtenidos por las API se almacenarán en una base de datos misma que luego se leerá y mostrará por el Grafana para que el usuario pueda interpretar la cantidad de puertos y vulnerabilidades con respecto a los nombres de sitios web y realice las mitigaciones correspondientes de acuerdo a los datos obtenidos.

La técnica que se plantea es la encuesta con cuestionarios estructurados para verificar si los ISP tienen conocimiento de lo que deberían tener expuesto al mundo sus nombres de sitios web, si conocen o no las vulnerabilidades de los mismos y si creen que es de utilidad la presentación consolidada y comparada en dashboards.

Con el resultado se espera tener un consolidado de las vulnerabilidades o puertos en dashboards, se plantea que el enfoque de la investigación sea cuantitativo con alcance descriptivo ya que se va a obtener las vulnerabilidades mediante las API de los motores de búsqueda avanzada como Shodan, Censys y VirusTotal, posteriormente se mostrarán los resultados obtenidos para que se puedan analizar de mejor forma la solución que se debe realizar.

1.3. Análisis de resultados

La pandemia de SARS-COV-2 ha obligado al mundo a avanzar en tecnología para el comercio creando sitios web para ofrecer diferentes tipos de servicios, el servicio de Internet ha sido implementado en casi todos los lugares del planeta (Zelada, 2022), en muchas ocasiones los nombres de los sitios web no son tan seguros, para esta investigación se ha tomado como muestra los nombres de los sitios web de los ISP más conocidos en el Ecuador como son los siguientes: netlife.ec, puntonet.ec, cnt.com.ec, telconet.net para ser escaneados por las API de los motores de búsqueda avanzada como son: Shodan, Censys y VirusTotal, se presentará la comparación de las vulnerabilidades y puertos obtenidos de las API.

1.3.1. Situación actual de los ISP

Se ha realizado una encuesta a personal de uno de los ISP antes mencionados para analizar qué tanto conocen sobre las herramientas como los motores de búsqueda avanzada de vulnerabilidades y puertos del nombre de su sitio web, si conoce que se puede escanear utilizando el API de los motores de búsqueda y si le sería de utilidad poder

visualizar los datos obtenidos por el API en dashboards, también es necesario conocer si realizan algún escaneo para lo cual se ha obtenido las siguientes estadísticas.

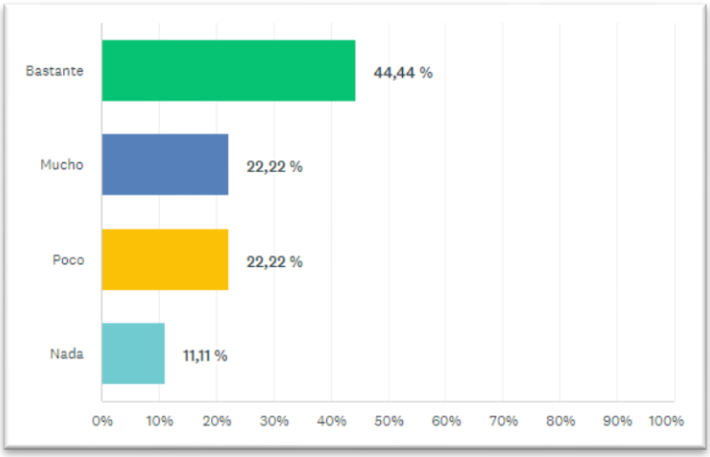
Como se puede observar en la Tabla 1 y Figura 4 para la pregunta ¿Qué tanto conoce sobre las vulnerabilidades del nombre de su sitio web?, para el número de personas que han respondido la encuesta existe un gran porcentaje que conocen bastante las vulnerabilidades del nombre del sitio web obteniendo el 44.44%, pero también existen personas que no conocen de estas vulnerabilidades.

Tabla 1
Conocimiento de las vulnerabilidades

Conocimiento de Vulnerabilidades	Porcentaje	No. Personas
Bastante	44,44%	4
Mucho	22,22%	2
Poco	22,22%	2
Nada	11,11%	1
TOTAL	**100,00%**	**9**

Nota. Autoría propia

Figura 4
Porcentaje de conocimiento de Vulnerabilidades



Nota. Autoría propia

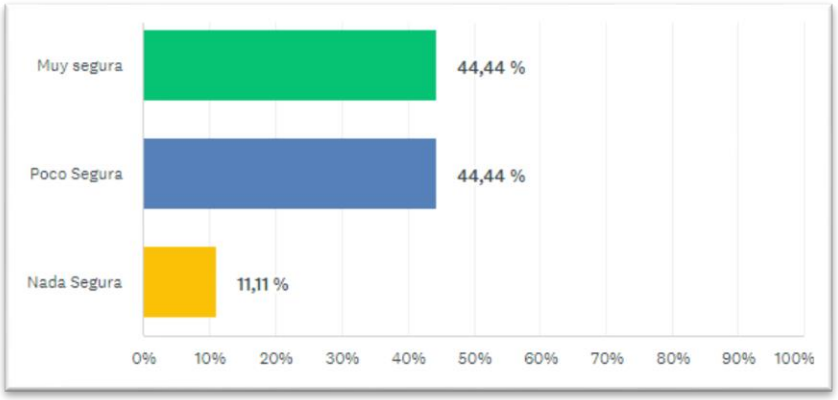
Para la segunda pregunta ¿Qué tan segura cree que se encuentra la información entregada por parte de sus clientes hacia usted como proveedor del servicio de Internet? Se puede observar en la Tabla 2 y Figura 5 que el ISP cree que está muy segura y al mismo porcentaje poco segura, esto podría indicar que el ISP se encuentra consciente de que las vulnerabilidades no desaparecen por completo ya que si las mitigan al día siguiente pueden aparecer nuevas.

Tabla 2
Seguridad de la Información de clientes

Seguridad de la Información de clientes	Porcentaje	No. Personas
Muy segura	44,44%	4
Poco Segura	44,44%	4
Nada Segura	11,11%	1
TOTAL	**100,00%**	**9**

Nota. Autoría propia

Figura 5
Porcentaje de seguridad de la información de clientes



Nota. Autoría propia

En la tercera pregunta: Como proveedor del servicio de Internet indique los motores de búsqueda avanzados que conoce para el análisis de vulnerabilidades del nombre de su sitio web, se observa en la Tabla 3 y Figura 6 que la mayoría de usuarios conocen por lo menos un de los motores de búsqueda y que la más utilizada es Shodan que se destaca con 54.55%

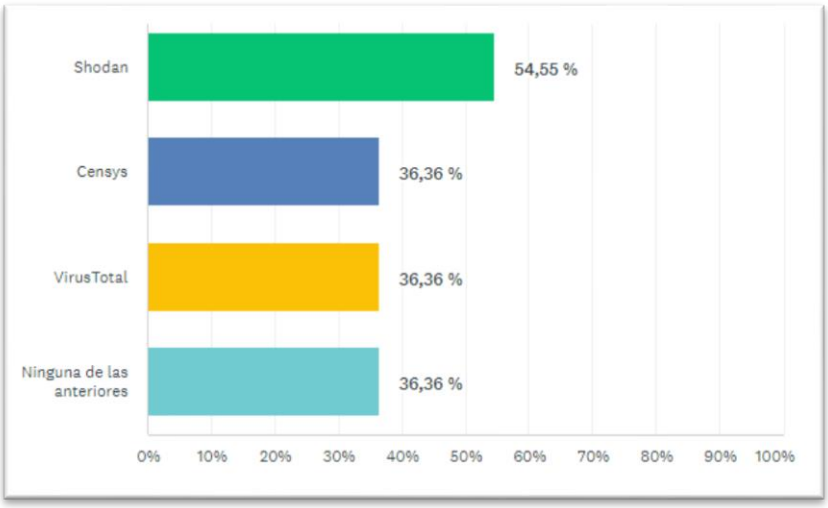
Tabla 3
Motores de búsqueda avanzada de vulnerabilidades

Motores de búsqueda avanzada de vulnerabilidades	Porcentaje	No. Personas
Shodan	54,55%	6
Censys	36,36%	4
VirusTotal	36,36%	4
Ninguna de las anteriores	36,36%	4
TOTAL	**100,00%**	**18**

Nota. Autoría propia

Figura 6

Porcentaje de conocimiento de motores de búsqueda avanzada



Nota. Autoría propia

En la cuarta pregunta ¿Ha realizado en algún momento un escaneo de vulnerabilidades y puertos del nombre de su sitio web que se encuentran expuestos en el Internet?, se puede observar en la Tabla 4 y Figura 7 que los ISP si realizan escaneo de vulnerabilidades y puertos expuestos al Internet de su respectivo nombre del sitio web con un 81.82%.

Tabla 4

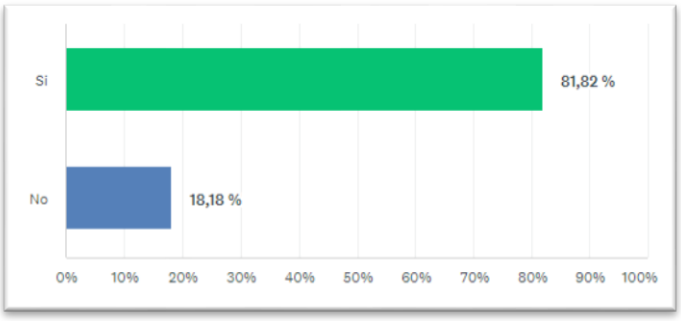
Porcentaje de escaneo de vulnerabilidades del nombre del sitio web

Se ha realizado escaneo de vulnerabilidades en algún momento	Porcentaje	No. Personas
Si	81,82%	9
No	18,18%	2
TOTAL	**100,00%**	**11**

Nota. Autoría propia

Figura 7

Porcentaje de escaneo de vulnerabilidades del nombre del sitio web



Nota. Autoría propia

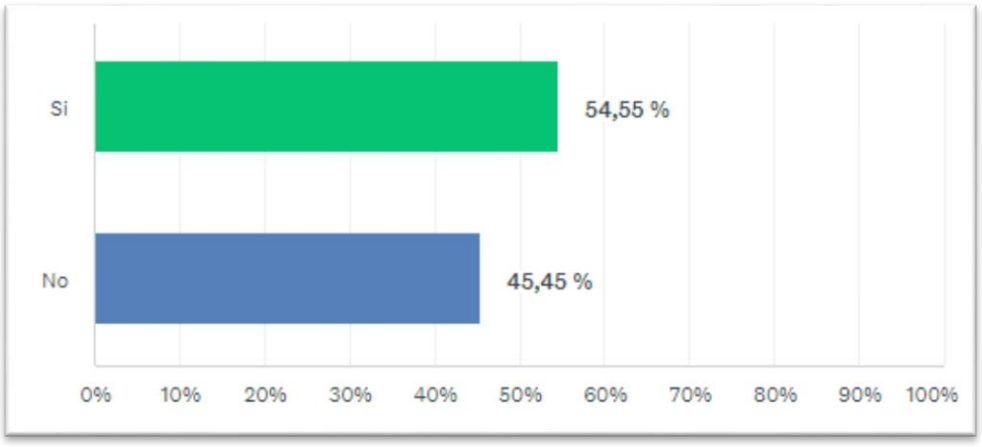
En la quinta pregunta ¿Conoce usted si los motores de búsqueda avanzada como Shodan, Censys y VirusTotal disponen de una API de desarrollo que permitan escanear las vulnerabilidades o puertos del nombre de su sitio web?, se puede observar en la Tabla 5 y Figura 8 que el 54.55% de los encuestados conocen de la existencia del API y el 45.45% no lo sabe, los motores de búsqueda deberían enfatizar en las API para mejorar los escaneos y que se realicen de forma automática.

Tabla 5
Conocimiento de la existencia de API en los motores de búsqueda

Conocimiento de la existencia de API en los motores de búsqueda	Porcentaje	No. Personas
Si	54,55%	6
No	45,45%	5
TOTAL	**100,00%**	**11**

Nota. Autoría propia

Figura 8
Porcentaje de conocimiento de la existencia de API en motores de búsqueda



Nota. Autoría propia

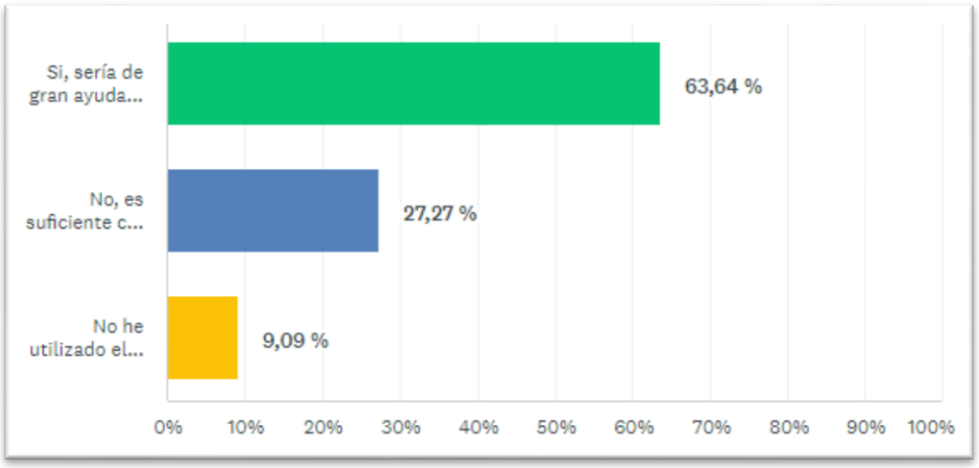
En la sexta pregunta ¿En base a su experiencia al escanear vulnerabilidades o puertos del nombre de su sitio web utilizando los motores de búsqueda mediante el API le sería de ayuda que los resultados del escaneo se consoliden en dashboards?, se observa en la Tabla 6 y Figura 9 en gran porcentaje del 63.64% que sería de gran ayuda visualizar las vulnerabilidades escaneadas en dashboards.

Tabla 6
Ayuda consolidar las vulnerabilidades en dashboards

Ayuda consolidar las vulnerabilidades en dashboards	Porcentaje	No. Personas
Si, sería de gran ayuda poder observar en dashboards los resultados.	63,64%	7
No, es suficiente con la información que se obtiene por el API	27,27%	3
No he utilizado el API de los motores de búsqueda avanzada	9,09%	1
TOTAL	**100,00%**	**11**

Nota. Autoría propia

Figura 9
Porcentaje de la Ayuda consolidar las vulnerabilidades en dashboards



Nota. Autoría propia

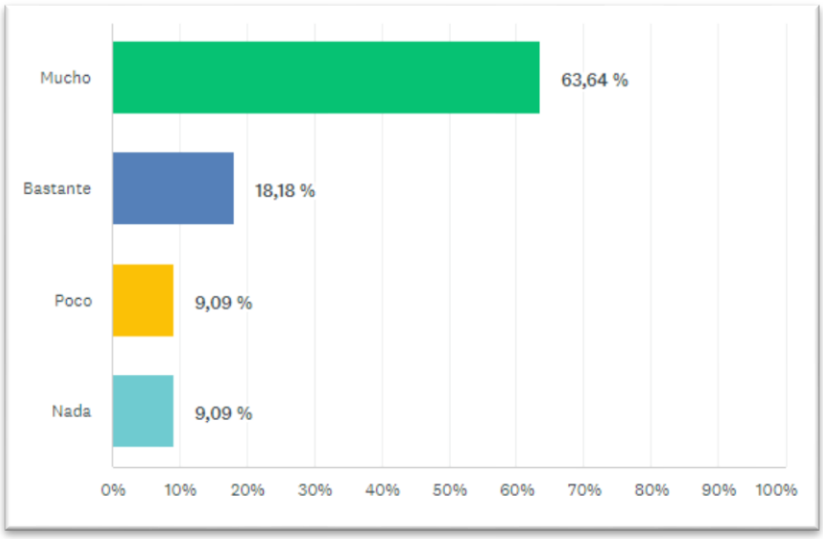
En la séptima pregunta ¿Qué tanto cree que le puede ayudar a la toma de decisiones para mitigar las vulnerabilidades o puertos escaneados presentados en dashboards?, se puede observar que consolidar las vulnerabilidades en dashboards ayudaría mucho a la toma de decisiones con el porcentaje de 63.64%, cómo se muestra en la Tabla 7 y Figura 10.

Tabla 7
Ayuda para la toma de decisiones sobre las vulnerabilidades encontradas

Ayuda para la toma de decisiones sobre las vulnerabilidades encontradas	Porcentaje	No. Personas
Mucho	63,64%	7
Bastante	18,18%	2
Poco	9,09%	1
Nada	9,09%	1
TOTAL	**100,00%**	**11**

Nota. Autoría propia

Figura 10
Ayuda para la toma de decisiones sobre las vulnerabilidades encontradas



Nota. Autoría propia

1.3.2. Escaneo de vulnerabilidades mediante API de los motores de búsqueda avanzada.

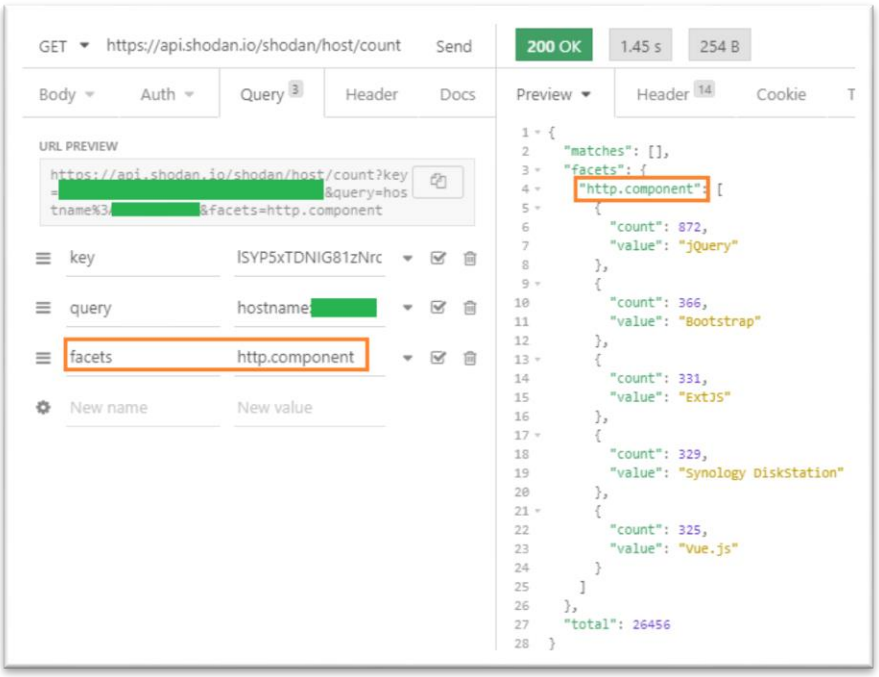
a. Shodan

Las propiedades de los elementos de información (facets) se pueden utilizar para obtener información adicional al filtro (Matherly, 2017) y utilizando los métodos correspondientes del API como contar los puertos expuestos, vulnerabilidades encontradas, datos de http, etc, como son las siguientes:

i. **Http.component**.- Con este facet se puede extraer los nombres de las tecnologías web utilizadas en el sitio web (Matherly, 2017) que se está realizando la búsqueda como se muestra en la Figura 11.

Figura 11

Facet http.content

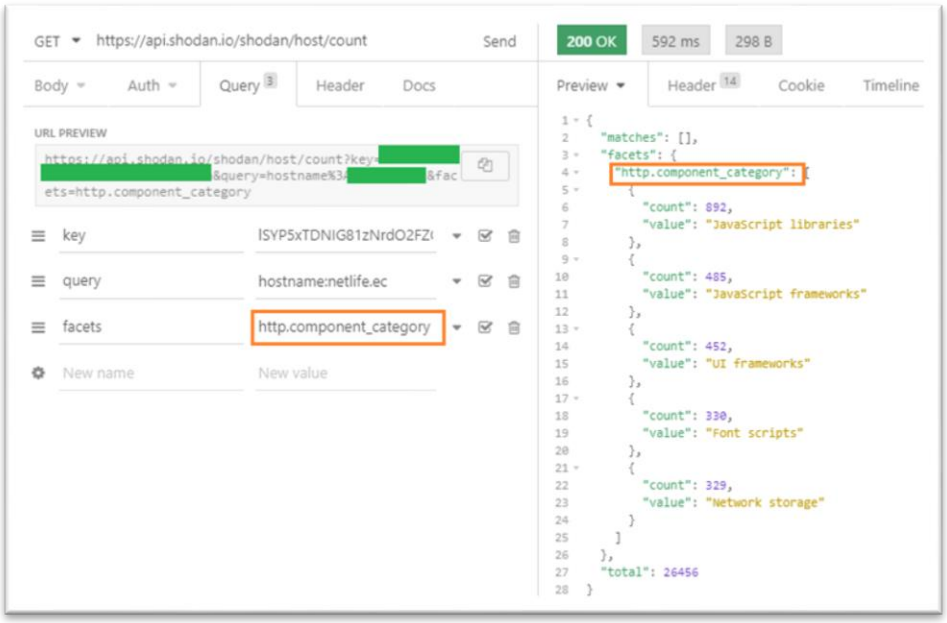


Nota. Autoría propia

ii. **Http.component_category**.- Con este facet se puede extraer las categorías de los componentes web utilizados en el sitio web (Matherly, 2017) que se realiza la búsqueda como se muestra en la Figura 12.

Figura 12

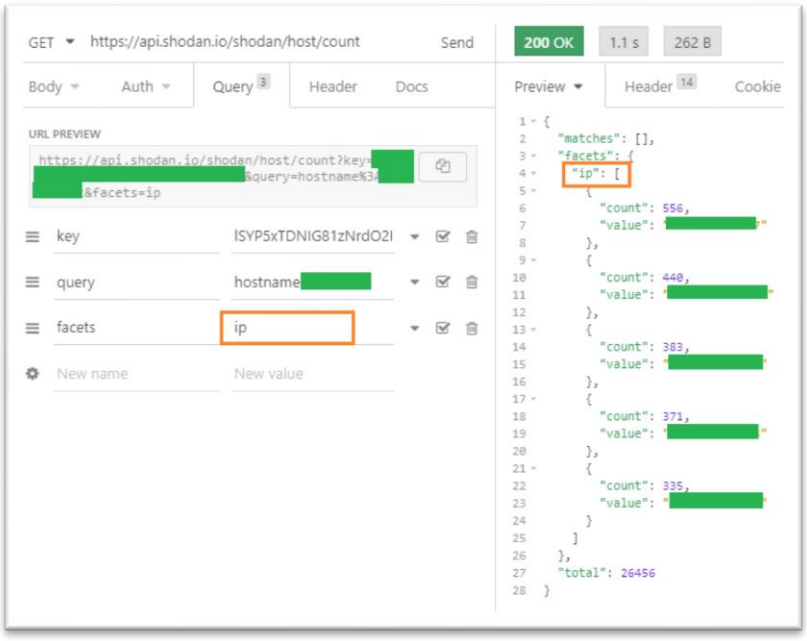
Facet http.component_category



Nota. Autoría propia

iii. **IP**.- Con este facet se puede extraer 5 IP con el API que se relacionen con la búsqueda del nombre del sitio web, cómo se muestra en la Figura 13.

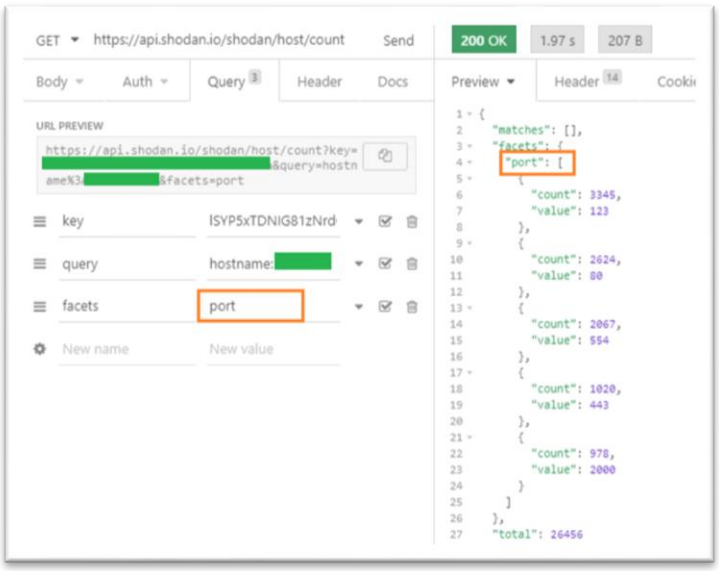
Figura 13
Facet IP



Nota. Autoría propia

iv. **Port**.- El facet port permite extraer los puertos que se encuentran expuestos y relacionados con la búsqueda relacionada al nombre del sitio web cómo se muestra en la Figura 14

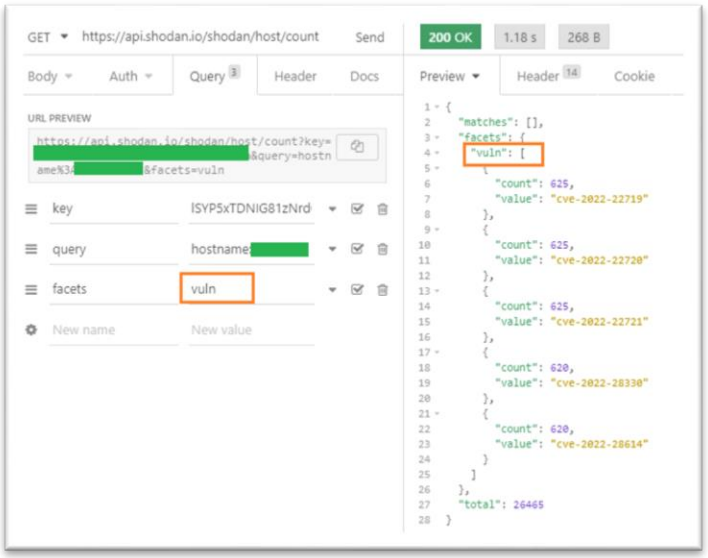
Figura 14
Facet port



Nota. Autoría propia

v. **Vuln**.- El facet vuln mediante el API muestra el top 5 de vulnerabilidades CVE relacionadas a la búsqueda del nombre del sitio web, cómo se indica en la Figura 15.

Figura 15
Facet vuln



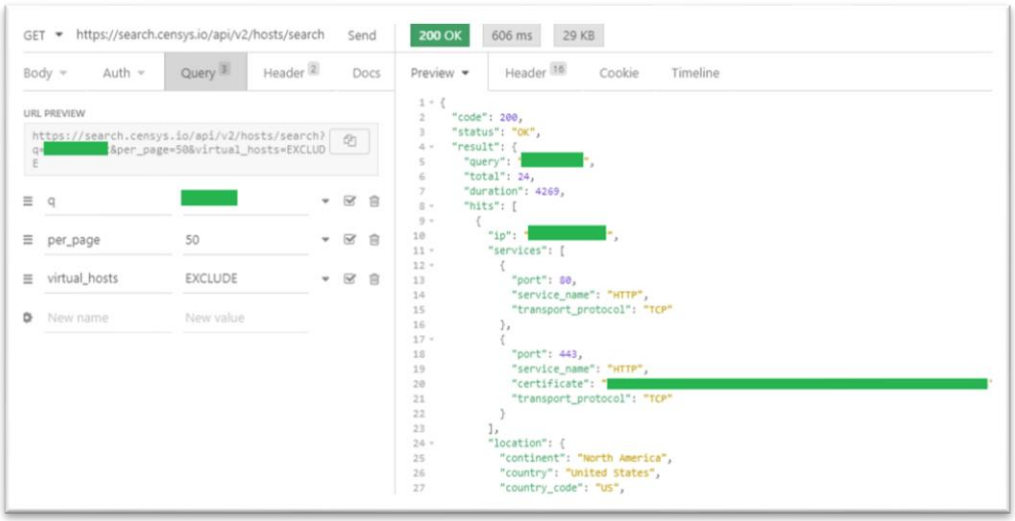
Nota. Autoría propia

b. Censys

Los métodos del API de Censys se encuentran alojados en el dominio https://search.censys.io y se puede obtener los puertos, las IP de los equipos que tengan referencia con la consulta del nombre del sitio web, los métodos utilizados fueron los siguientes:

i. **Search.-** Con el método search busca todo lo relacionado con la pregunta que en este caso es el nombre de sitio web, la paginación ya que puede traer varios datos por si se pasa el límite de la licencia free, como se muestra en la Figura 16.

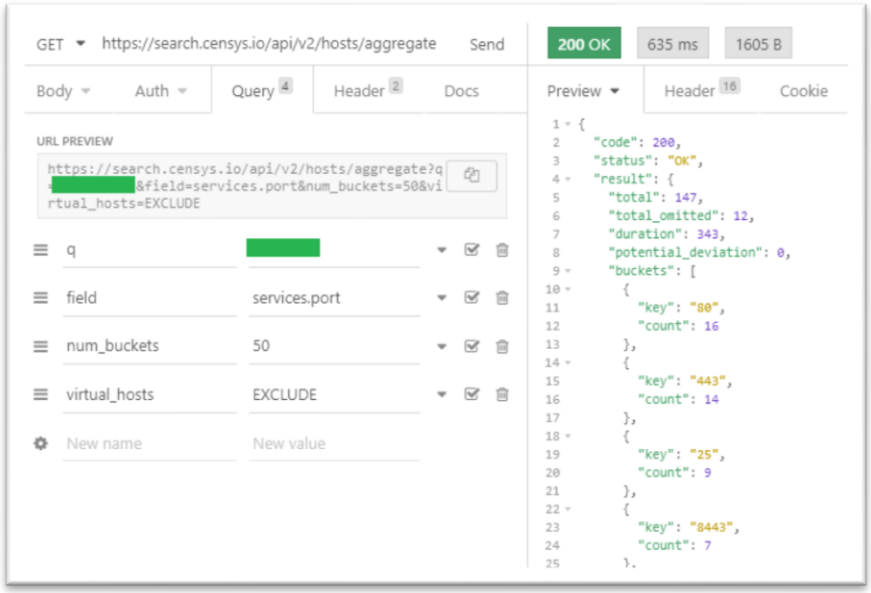
Figura 16
Método search



Nota. Autoría propia

ii. **Aggregate.-** con el método aggregate agrega los equipos que tengan relación con la consulta realizada con respecto al nombre del sitio web y en este caso el campo puerto, la respuesta contabiliza los datos obtenidos por puerto se muestra en la Figura 17.

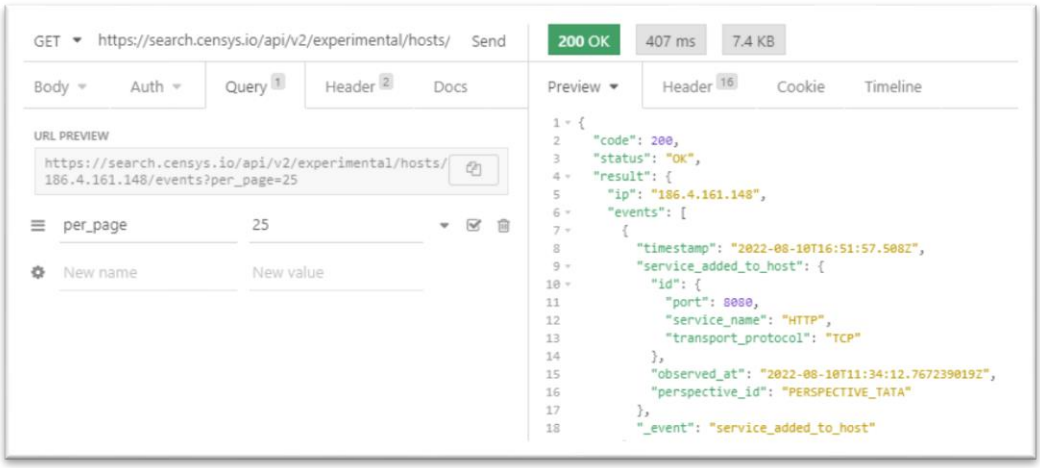
Figura 17
Método Aggregate



Nota. Autoría propia

iii. **Experimental.-** con el método experimental se puede observar los eventos que haya tenido alguna IP en específico, ya que la consulta se realiza con IP como se muestra en la Figura 18.

Figura 18
Método Experimental



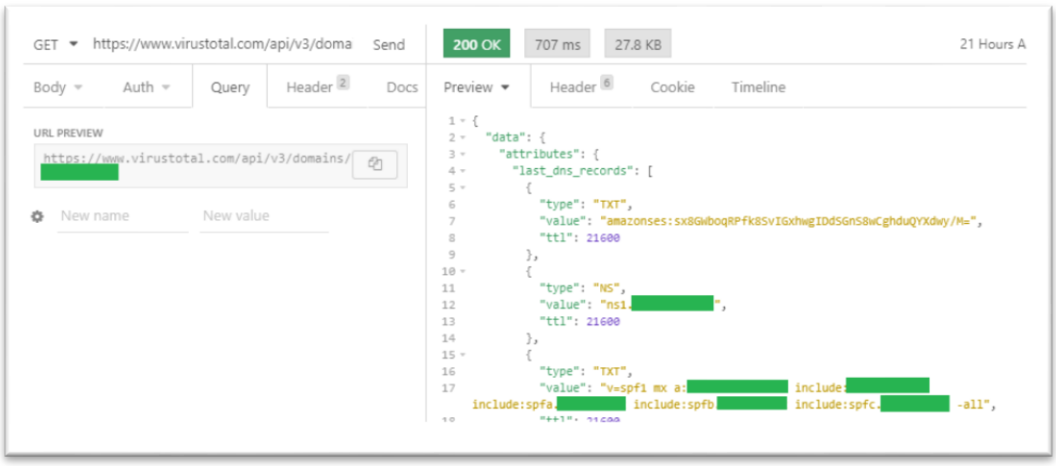
Nota. Autoría propia

c. VirusTotal

Los métodos del API de VirusTotal permiten escanear los nombres de sitios web y obtener información relevante con respecto a IP, puertos, certificados y análisis de antivirus que tiene la herramienta implementada, los métodos son los siguientes:

i. **Domain.-** Con este método se obtiene datos generales como escaneo de los antivirus que tiene embebida la herramienta, records DNS, datos informativos como el whois y certificados del nombre del sitio web que se realiza la consulta se muestra en la Figura 19.

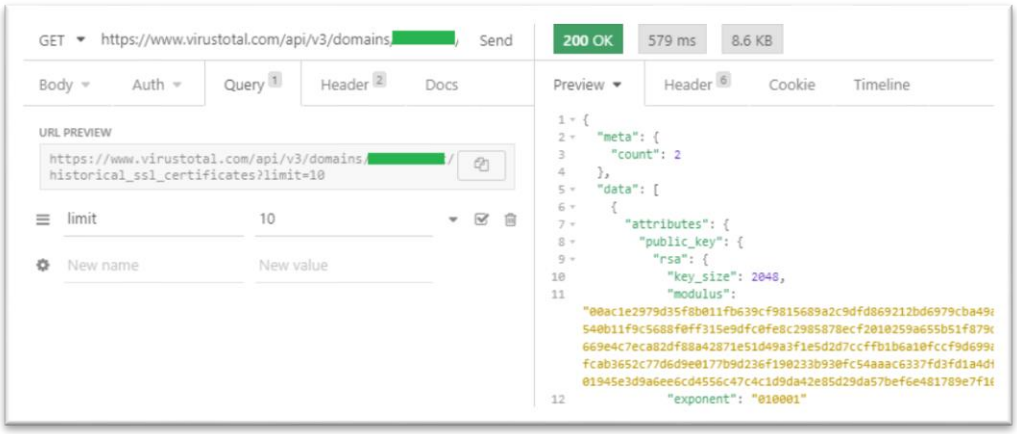
Figura 19
Método Domain



Nota. Autoría propia

ii. **Historical_ssl_certificates.-** con este método se puede observar los históricos principales de los certificados relacionados con la búsqueda realizada en este caso el nombre del sitio web se muestra en la Figura 20

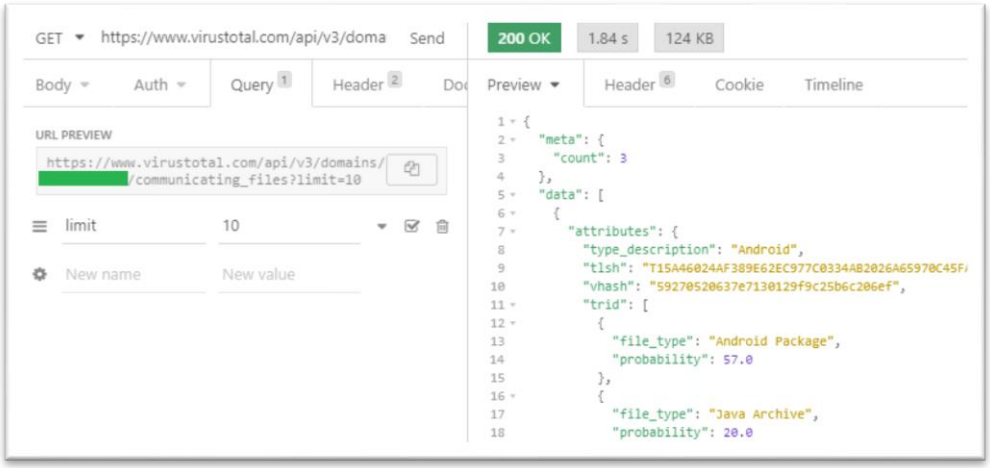
Figura 20
Método histórico de certificado SSL



Nota. Autoría propia

iii. **Communicating_files.-** muestra el escaneo de los archivos que se comunican con el nombre del sitio web que se envía en la consulta como se muestra en la Figura 21

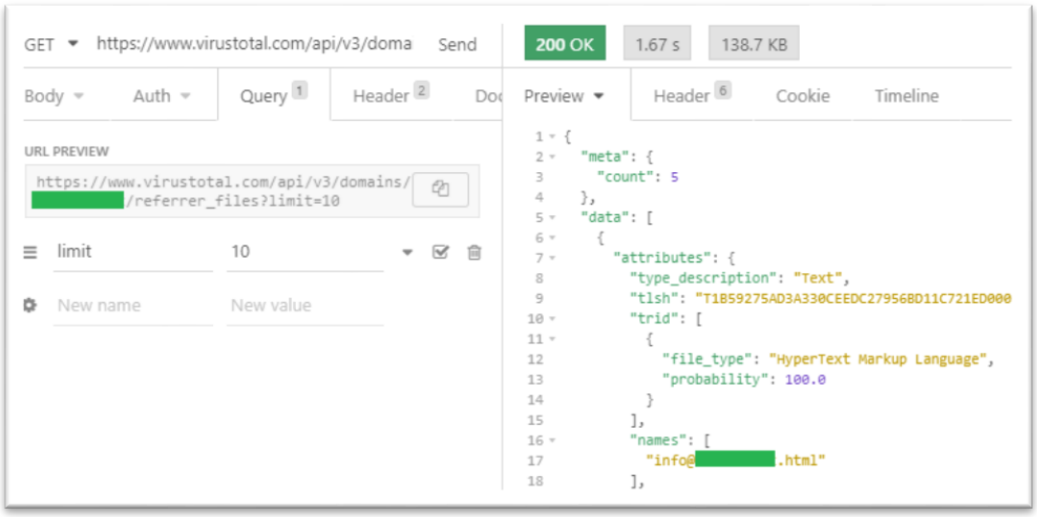
Figura 21
Método communicating_files



Nota. Autoría propia

iv. **Referrer_files.-** con este método se escanea los archivos que hacen referencia a la consulta del nombre de sitio web como se muestra en la Figura 22.

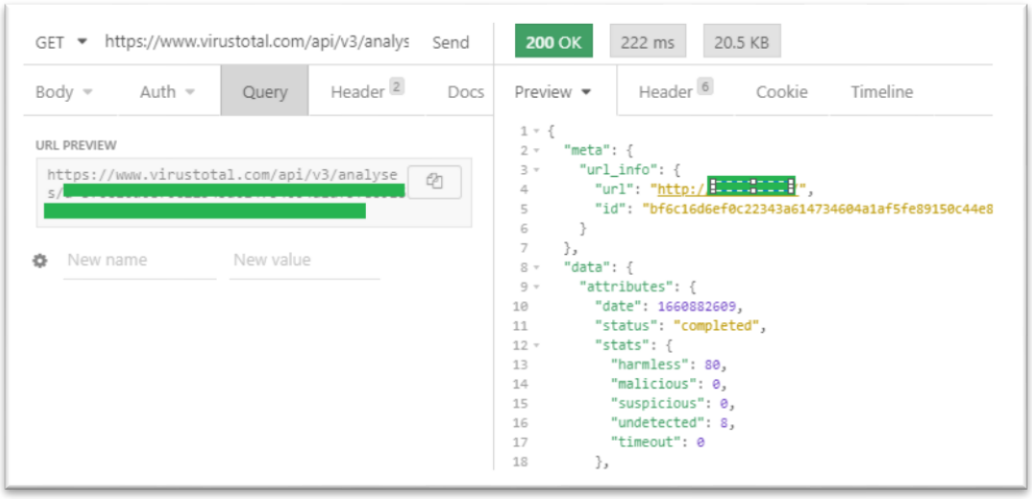
Figura 22
Método referrer_files



Nota. Autoría propia

v. **Analyses.-** con el método analyses el API devuelve información relevante del nombre del sitio web como la versión de php o del servidor web como se muestra en la Figura 23.

Figura 23
Método Analyses



Nota. Autoría propia

1.3.3. Comparación de los resultados obtenidos

Luego de haber realizado la encuesta al personal de diferentes ISP y el escaneo de los nombres de los sitios web de los principales proveedores mediante las API públicas, se ha podido obtener los siguientes resultados por cada herramienta.

Los datos de la encuesta muestra que algunos ISP si realizan en algún momento escaneo a los nombres de sus sitios web lo que indica que se preocupan por su seguridad y por la seguridad de los clientes, así también se puede observar que las herramientas de escaneo como Shodan, Censys y VirusTotal son herramientas muy útiles para los encuestados y que conocen de la existencia de su API.

En las encuestas se observa que los ISP en ocasiones creen que la información que manejan no está segura dentro del nombre de su dominio web lo que lleva al siguiente punto de escanear dichos nombres para evidenciar lo que se observa desde el Internet.

Con los escaneos realizados se puede observar que algunos datos que se obtiene de las API son muy similares en cuanto al tipo de información y también son diferentes ya que una de las herramientas tiene implementado análisis por antivirus, otra herramienta muestra las principales vulnerabilidades y exposiciones comunes y la otra herramienta puede mostrar eventos que puede haber tenido el nombre del sitio web, como se muestra a continuación.

a. Análisis de resultados obtenidos por la herramienta Shodan

Con el API de la herramienta Shodan se han tomado los principales facets para escanear a los nombre del sitio web de los ISP.

Facets http.component.- se observa las tecnologías web que han sido utilizadas para crear el sitio web, en la Tabla 8, se puede evidenciar que los cuatro ISP permiten observar las tecnologías que utilizan en sus sitios web, esta información puede ser utilizada por un atacante y buscar brechas de seguridad en esas tecnologías para luego explotarlas, CNT muestra pocas tecnologías y pocos dispositivos asociados a las tecnologías web utilizadas para sus sitios web.

Tabla 8
Shodan - Comparación de tecnologías web de los ISP

Proveedor de Internet	Facets http.component	Cantidad de hosts
Netlife	jQuery	872
	Bootstrap	366
	ExtJS	331
	Synology DiskStation	329
	Vue.js	325

Proveedor de Internet	Facets http.component	Cantidad de hosts
Puntonet	jQuery	839
	Modernizr	258
	Bootstrap	151
	Google Font API	111
	Font Awesome	75
CNT	PHP	1
	jQuery	1
	jQuery UI	1
Telconet	jQuery	150
	Bootstrap	75
	ExtJS	44
	Font Awesome	44
	Google Font API	32

Nota. Autoría propia

Facets port.- Se observa que el API muestra los puertos que se encuentran expuestos al Internet con la cantidad de dispositivos asociados al nombre del sitio web, según el escaneo realizado CNT es el ISP que menos puertos tiene expuestos con respecto al sitio web, mientras que los que tienen gran cantidad de puertos son los ISP Netlife y Puntonet como se muestra en la Tabla 9.

Tabla 9

Comparación de puertos y cantidad de hosts asociados

Proveedor de Internet	Facets port	Servicio	Cantidad de hosts
Netlife	123	NTP	3345
	80	HTTP	2624
	554	RTSP	2067
	443	HTTPS	1020
	2000	Cisco-SCCP	978
Puntonet	80	HTTP	1789
	22	SSH	1657
	443	HTTPS	1266
	2000	Cisco-SCCP	1139
	8080	HTTP	489
CNT	443	HTTPS	1

Proveedor de Internet	Facets port	Servicio	Cantidad de hosts
Telconet	22	SSH	1229
	80	HTTP	711
	443	HTTPS	508
	7547	CWMP	418

Nota. Autoría propia

Facets vuln.- en el escaneo realizado por el API, se observa que los nombres de dominio de los ISP presentan las principales vulnerabilidades CVE, con estos datos los ISP pueden tener una idea de las vulnerabilidades que tienen los sitios web y realizar las respectivas remediaciones, en la comparación CNT no muestra vulnerabilidades y Netlife es el que muestra mayor cantidad de equipos con vulnerabilidades como se muestra en el Tabla 10.

Tabla 10

Comparación de vulnerabilidades y cantidad de hosts involucrados

Proveedor de Internet	Facets vuln	Cantidad de hosts
Netlife	cve-2022-22719	625
	cve-2022-22720	625
	cve-2022-22721	625
	cve-2022-28330	620
	cve-2022-28614	620
Puntonet	cve-2022-28330	282
	cve-2022-28614	274
	cve-2022-28615	274
	cve-2022-29404	274
	cve-2022-30522	274
CNT	N/A	N/A
Telconet	cve-2022-28330	138
	cve-2022-28614	138
	cve-2022-28615	138
	cve-2022-29404	138
	cve-2022-22719	137

Nota. Autoría propia

b. Análisis de resultados obtenidos por la herramienta Censys

Con el API de Censys se obtiene los datos paginados eso quiere decir que se puede realizar la consulta indicando la cantidad de datos que se requiera

analizar, para la investigación se ha extraído los primero 5 valores con los siguientes métodos.

Método aggregate.- al escanear los nombres de dominio de los sitios web de los ISP agrupados por la búsqueda de puertos muestra que CNT presenta menos puertos expuestos al Internet al igual que un solo host relacionado a ese puerto, mientras que Puntonet presenta más host asociados a los puertos expuestos, como se muestra en la Tabla 11.

Tabla 11

Comparación de puertos expuestos y cantidad de host relacionados

Proveedor de Internet	Aggregate	Servicio	Cantidad de hosts
Netlife	80	HTTP	15
	443	HTTPS	13
	25	SMTP	7
	8443	HTTPS	6
	143	IMAP	5
Puntonet	443	HTTPS	37
	80	HTTP	30
	25	SMTP	20
	110	POP3	16
	587	SMTP	16
CNT	80	HTTP	1
Telconet	443	HTTPS	7
	25	SMTP	5
	110	POP3	5
	80	HTTP	4
	143	IMAP	4

Nota. Autoría propia

Método experimental.- en el escaneo se evidencia los puertos y servicios que otros ISP internacionales han observado con respecto a los nombres de dominio de cada ISP del Ecuador, por el API libre no se observa datos de CNT, es muy posible que no haya sido observado o que estos datos se puedan visualizar con un API de pago, Puntonet muestra puertos de servidores de correo y acceso ssh expuestos al Internet y que han sido observados como se muestra en la Tabla 12.

Tabla 12

Comparación de puertos y servicios que han recibido un evento

Proveedor de Internet	Puerto	Servicio	Protocolo	ISP que analiza	Evento
Netlife	80	HTTP	TCP	PERSPECTIVE_NTT	service_observed
	8070	HTTP	TCP	PERSPECTIVE_NTT	service_observed
	2022	SSH	TCP	PERSPECTIVE_HE	service_observed
	8080	HTTP	TCP	PERSPECTIVE_TATA	service_observed
	8080	HTTP	TCP	PERSPECTIVE_ORANGE	service_observed
Puntonet	995	POP3	TCP	PERSPECTIVE_HE	service_observed
	22	SSH	TCP	PERSPECTIVE_ORANGE	service_observed
	993	IMAP	TCP	PERSPECTIVE_TATA	service_observed
	8443	HTTP	TCP	PERSPECTIVE_ORANGE	service_observed
	8090	HTTP	TCP	PERSPECTIVE_HE	service_observed
CNT	N/A	N/A	N/A	N/A	N/A
Telconet	2444	UNKNOWN	TCP	PERSPECTIVE_NTT	service_observed
	2323	HTTP	TCP	PERSPECTIVE_HE	service_observed
	2000	UNKNOWN	TCP	PERSPECTIVE_NTT	service_observed
	8088	HTTP	TCP	PERSPECTIVE_HE	service_observed
	8883	UNKNOWN	TCP	PERSPECTIVE_HE	service_observed

Nota. Autoría propia

c. Análisis de resultados obtenidos por la herramienta VirusTotal

Con el API de VirusTotal se ha escaneado los nombres de dominio de los sitios web de los ISP con los métodos más relevantes, tomando en cuenta que esta herramienta escanea archivos con antivirus.

Método communicating_files.- el escaneo ha mostrado archivos de diferentes extensiones mismos que con la ayuda del antivirus que la herramienta tiene implementada indica una probabilidad de explotación, siendo Telconet y Netlife muestran las probabilidades más altas como se muestra en la Tabla 13.

Tabla 13

Comparación de tipos de archivos y probabilidad de explotación

Proveedor de Internet	Tipo de archivo	Probabilidad de Explotación
Netlife	Android Package	57
	Java Archive	20
	Sweet Home 3D design (generic)	15.5
	ZIP compressed archive	5.9
	PrintFox/Pagefox bitmap (640x800)	1.4

Proveedor de Internet	Tipo de archivo	Probabilidad de Explotación
Puntonet	Win16 NE executable (generic)	26.8
	Win32 Dynamic Link Library (generic)	25.0
	Win32 Executable (generic)	17.1
	Win16/32 Executable Delphi generic	7.9
	OS/2 Executable (generic)	7.7
CNT	Win16 NE executable (generic)	32.3
	Win32 Executable (generic)	28.9
	OS/2 Executable (generic)	13
	Generic Win/DOS Executable	12.8
	DOS Executable Generic	12.8
Telconet	Win64 Executable (generic)	40.3
	Win16 NE executable (generic)	19.3
	Win32 Executable (generic)	17.2
	OS/2 Executable (generic)	7.7
	Generic Win/DOS Executable	7.6

Nota. Autoría propia

Método referrer_files.- en el escaneo realizado se observa los archivos que tienen relación con el nombre de dominio del sitio web, se muestra el análisis de los colaboradores asociados a VirusTotal como se muestra en la Tabla 14 y Tabla 15

Tabla 14

Comparación de análisis de los socios de VirusTotal

Proveedor de Internet	Tag	harmless	type-unsupported	suspicious	confirmed-timeout	timeout	failure	malicious	undetected
Netlife	email	0	15	0	0	0	0	31	27
Puntonet	email	0	14	0	0	4	0	7	47
CNT	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Telconet	javascript	0	15	0	0	0	1	6	54

Nota. Autoría propia

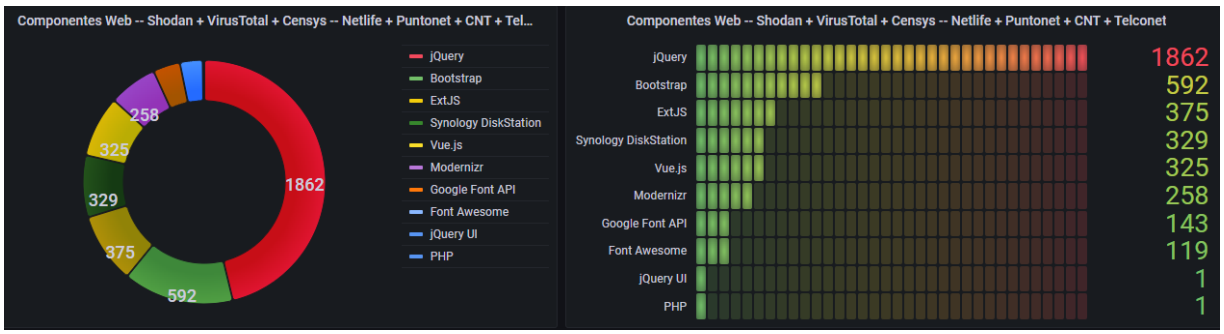
Tabla 15
Comparación de resultados del análisis de antivirus de la herramienta

Proveedor de Internet	Tag	Antivirus	Resultado
Netlife	email	Lionic	Hacktool.MSOffice.Generic.3!c
		McAfee	W97M/Downloader.ea
		CAT-QuickHeal	XML.Downloader.33357
		Cyren	W97M/Agent.gen
		ESET-NOD32	multiple detections
Puntonet	email	DrWeb	Exploit.Siggen3.28348
		ALYac	VBA.Heur.Bomber.1.BAEC0A0D.Gen
		Cyren	X97M/Agent.AIU.gen!Eldorado
		ESET-NOD32	GenScript.NDB
		TrendMicro-HouseCall	TrendMicro-HouseCall
CNT	N/A	N/A	N/A
Telconet	javascript	Ikarus	Trojan.JS.Cryxos
		Avast	JS:Facelike-B [PUP]
		Zillya	Trojan.FaceLiker.JS.2
		Microsoft	Trojan:Win32/Tnega!ml
		AVG	JS:Facelike-B [PUP]

Nota. Autoría propia

Con los datos obtenidos se han realizado dashboards que permitan visualizar y analizar el conjunto de los mismos y luego internamente puedan realizar las remediaciones necesarias como se muestra en la Figura 24, Figura 25 y Figura 26.

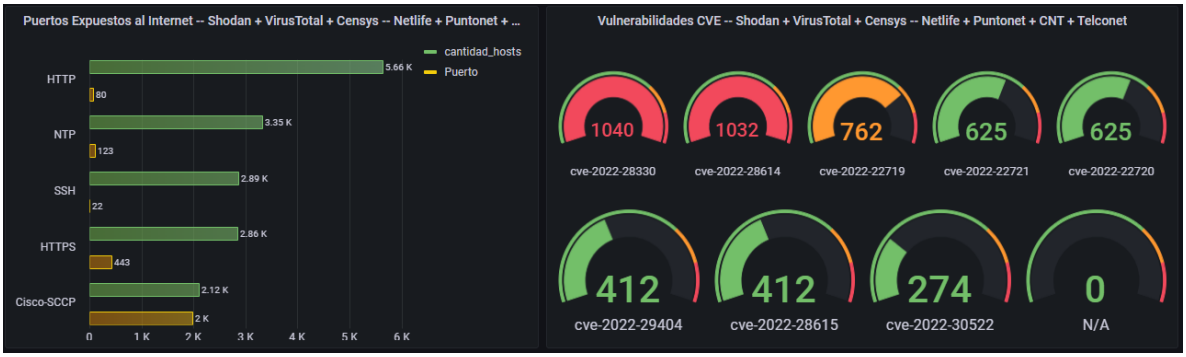
Figura 24
Componentes web vs número de equipos relacionados



Nota. Autoría propia

Figura 25

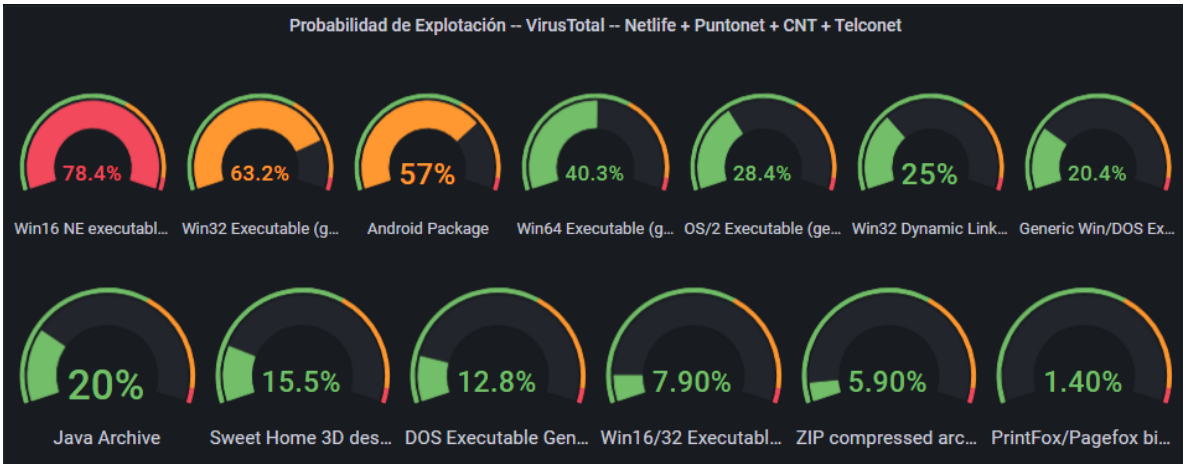
Puertos expuestos y CVE vs número de equipos relacionados



Nota. Autoría propia

Figura 26

Archivos vulnerables vs la probabilidad de explotación



Nota. Autoría propia

CAPÍTULO II: ARTÍCULO PROFESIONAL

2.1. Resumen

Esta investigación realiza la comparación de las principales vulnerabilidades o puertos expuestos de los nombres de sitios web de proveedores de Internet más relevantes del país, utilizando el API de tres herramientas de acceso público como son: Shodan, Censys y VirusTotal.

Cada herramienta tiene sus particularidades para poder contabilizar la cantidad de puertos, vulnerabilidades, escaneo de archivos relacionados con los nombres de dominio de sitios web mediante antivirus que tiene implementado como parte del funcionamiento la herramienta, esto no significa que los usuarios dueños de los nombres de sitios web deban omitir desarrollo de código seguro, implementación de firewalls o realizar escaneos constantes en búsqueda de nuevas brechas de seguridad ya que la tecnología sigue avanzando y los escaneos internos deben ser periódicos para asegurar tanto la información de la empresa como de los usuarios que utilizan el servicio.

Al realizar el escaneo periódicamente el usuario puede mitigar las vulnerabilidades encontradas o puertos expuestos antes de que sean explotados por un atacante cibernético en el caso que tenga el conocimiento necesario o implementar personal de seguridad informática especializado para mitigar los datos encontrados.

a. Palabras clave: shodan, censys, virustotal, API, vulnerabilidades

2.2. Abstract

This research compares the main vulnerabilities or exposed ports of the most relevant Internet provider website names in the country, using the API of three public access tools such as: Shodan, Censys and VirusTotal.

Each tool has its particularities to be able to count the number of ports, vulnerabilities, scanning of files related to the domain names of websites through antivirus that has been implemented as part of the tool's operation, this does not mean that the users who own the domain names Websites must skip developing secure code, implementing firewalls or performing constant scans for new security breaches as technology continues to advance and internal scans must be periodic to secure both the company's information and the users who use it the service.

By performing the scan periodically, the user can mitigate the vulnerabilities found or exposed ports before they are exploited by a cyber attacker if they have the necessary knowledge or deploy specialized computer security personnel to mitigate the data found.

a. Keywords: shodan, censys, virustotal, API, vulnerabilities

2.3. Introducción

En el año 2020 todo el mundo fue impactado por el virus mortal del SARS-COV-2, ocasionando que las personas no puedan salir a realizar compras, pagos de servicios, realicen teletrabajo o teleducación y esto ocasionó que la evolución de la tecnología avance a pasos gigantescos, este impacto se evidenció en que las empresas para poder subsistir durante la pandemia implementaron sitios web para que los usuarios puedan realizar las compras o pagos online, pero la mayoría de los sitios web por la premura de su implementación no se encuentran implementados con las debidas seguridades o se encuentran publicados en servidores que tiene muchos puertos abiertos que no son necesarios y publicados hacia el Internet, con esta información cualquier atacante puede utilizarla para obtener información, suplantar identidad, interferir con los servicios que brinde la empresa (Zelada, 2022). Las empresas pueden realizar un análisis interno de los nombres de sus sitios web mediante la utilización de motores de búsqueda especializados en vulnerabilidades y que son de uso público como Shodan, Censys y VirusTotal, para poder determinar las acciones que se debe seguir.

Shodan, Censys y VirusTotal son motores de búsqueda especializada en equipos conectados o expuestos al Internet, la ventaja que tienen estos motores es que puede obtener información por la API que disponen, solo con el registro en la plataforma, esta data se encuentra almacenada en la base de datos de los motores de búsquedas y facilitan la extracción, para los usuarios que realizan el análisis.

En los motores de búsqueda de Shodan y Censys se puede analizar nombres de sitios web e identificar los puertos expuestos y vulnerabilidades, la ventaja que se extraer la data mediante el API que ambos motores disponen, la desventaja de Shodan es que el API tiene un límite para los usuarios gratuitos pero es suficiente como para un primer análisis (Drago, 2016).

VirusTotal es un buscador especializado y también una herramienta ya que dentro de sus características tiene antivirus y motores de detección (Fernández, 2018), también dispone de una API que permite extraer la data y comparar con la información obtenida de las otras API.

En la actualidad se puede observar que las aplicaciones se comunican mediante API con otras aplicaciones sin necesidad que los desarrolladores tengan que volver a crear aplicaciones para validar pagos, publicar mensajes en redes sociales u obtener datos que

luego son utilizados para presentar análisis, etc, la comunicación entre las API se realiza mediante el protocolo http (*What Is an API?*, 2022).

Las API permiten la comunicación fluida entre aplicaciones aunque pueden tener sus restricciones mismas que son configuradas por los desarrolladores propietarios del API, estas restricciones en ocasiones es para limitar el número de usuarios que pueden utilizarla o cantidad de datos a consultar (Fernández, 2019), esto generalmente sucede cuando se vuelven populares en su uso y también para implementar nuevos servicios.

Al momento se utilizan las API REST ya que cumple con un estilo arquitectónico y la respuesta de los mensajes generalmente son en formato JavaScript Object Notation (JSON) que ayudan al desarrollador a entender la información que está obteniendo para luego extraerla con el lenguaje de programación que el desarrollador lo requiera (*What Is an API?*, 2022) como se muestra en la Figura 1.

2.3.1. Motor de búsqueda Shodan

En el caso de Shodan con una cuenta sin costo solo con registro se puede observar información entre los top 5, es decir solo los datos más relevantes, en el caso que se realice una búsqueda con muchos filtros o preguntas (query) solicita actualizar la cuenta a una de pago, pero si se puede realizar búsquedas individuales siempre y cuando los resultados no sean muy extensos.

2.3.2. Motor de búsqueda Censys

El motor de búsqueda Censys permite registrarse y generar un key sin costo que permite realizar varias consultas mediante el API hasta un límite que es reseteado cada mes, como se indica en la Figura 2.

2.3.3. Motor de búsqueda VirusTotal

El motor de búsqueda Virustotal, al igual que los otros motores antes mencionados genera un key sin costo con solo registrarse que permite realizar algunas búsquedas con restricciones por día y por mes como se indica en la Figura 3.

2.4. Metodología

El proceso de investigación que se utilizará para el problema planteado se basa en los siguientes puntos:

Diseño no experimental - transversal se utilizará para los nombres de los sitios web de los ISP ya se encuentran en funcionamiento y las vulnerabilidades y puertos serán mostrados en el instante de tiempo que se realice la consulta al API de los motores de

búsqueda avanzada para poder determinar las diferentes soluciones que los usuarios deben realizar o solicitar asesoría según sea el caso.

Muestreo: se plantea sea Intencional ya que se va a aplicar para los nombres de los sitios web de los ISP más conocidos en el país como netlife.ec, puntonet.ec, cnt.com.ec, telconet.net con el fin escanear las vulnerabilidades y los puertos que tengan expuestos al Internet y que los puedan visualizar en dashboards.

Comparativo: se mostrará en los paneles de la aplicación Grafana ya que los datos obtenidos por las API se almacenarán en una base de datos misma que luego se leerá y mostrará por el Grafana para que el usuario pueda interpretar la cantidad de puertos y vulnerabilidades con respecto a los nombres de sitios web y realice las mitigaciones correspondientes de acuerdo a los datos obtenidos.

La técnica que se plantea es la encuesta con cuestionarios estructurados para verificar si los ISP tienen conocimiento de lo que deberían tener expuesto al mundo sus nombres de sitios web, si conocen o no las vulnerabilidades de los mismos y si creen que es de utilidad la presentación consolidada y comparada en dashboards.

Con el resultado se espera tener un consolidado de las vulnerabilidades o puertos en dashboards, se plantea que el enfoque de la investigación sea cuantitativo con alcance descriptivo ya que se va a obtener las vulnerabilidades mediante las API de los motores de búsqueda avanzada como Shodan, Censys y VirusTotal, posteriormente se mostrarán los resultados obtenidos para que se puedan analizar de mejor forma la solución que se debe realizar.

2.5. Resultados – Discusión

La pandemia de SARS-COV-2 ha obligado al mundo a avanzar en tecnología para el comercio creando sitios web para ofrecer diferentes tipos de servicios, la implementación del Internet ha sido implementado en casi todos los lugares del planeta (Zelada, 2022), en muchas ocasiones los nombres de los sitios web no son tan seguros, para esta investigación se ha tomado como muestra los nombres de los sitios web de los ISP más conocidos en el Ecuador como son los siguientes: netlife.ec, puntonet.ec, cnt.com.ec, telconet.net para ser escaneados por las API de los motores de búsqueda avanzada como son: Shodan, Censys y VirusTotal, se presentará la comparación de las vulnerabilidades y puertos obtenidos de las API.

2.5.1. Situación actual de los ISP

Se ha realizado una encuesta a personal de uno de los ISP antes mencionados para analizar qué tanto conocen sobre las herramientas como los motores de búsqueda avanzada de vulnerabilidades y puertos del nombre de su sitio web, si conoce que se puede escanear utilizando el API de los motores de búsqueda y si le sería de utilidad poder visualizar los datos obtenidos por el API en dashboards, también es necesario conocer si realizan algún escaneo para lo cual se ha obtenido las siguientes estadísticas.

Como se puede observar en la Tabla 1 para la pregunta ¿Qué tanto conoce sobre las vulnerabilidades del nombre de su sitio web?, para el número de personas que han respondido la encuesta existe un gran porcentaje que conocen bastante las vulnerabilidades del nombre del sitio web obteniendo el 44.44%, pero también existen personas que no conocen de estas vulnerabilidades.

Tabla 1
Conocimiento de las vulnerabilidades

Conocimiento de Vulnerabilidades	Porcentaje	No. Personas
Bastante	44,44%	4
Mucho	22,22%	2
Poco	22,22%	2
Nada	11,11%	1
TOTAL	**100,00%**	**9**

Nota. Autoría propia

Para la segunda pregunta ¿Qué tan segura cree que se encuentra la información entregada por parte de sus clientes hacia usted como proveedor del servicio de Internet? Se puede observar en la Tabla 2 que el ISP cree que está muy segura y al mismo porcentaje poco segura, esto podría indicar que el ISP se encuentra consciente de que las vulnerabilidades no desaparecen por completo ya que si las mitigan al día siguiente pueden aparecer nuevas.

Tabla 2
Seguridad de la Información de clientes

Seguridad de la Información de clientes	Porcentaje	No. Personas
Muy segura	44,44%	4
Poco Segura	44,44%	4
Nada Segura	11,11%	1
TOTAL	**100,00%**	**9**

Nota. Autoría propia

En la tercera pregunta: Como proveedor del servicio de Internet indique los motores de búsqueda avanzados que conoce para el análisis de vulnerabilidades del nombre de su sitio web, se observa en la Tabla 3 que la mayoría de usuarios conocen por lo menos un de los motores de búsqueda y que la más utilizada es Shodan que se destaca con 54.55%

Tabla 3
Motores de búsqueda avanzada de vulnerabilidades

Motores de búsqueda avanzada de vulnerabilidades	Porcentaje	No. Personas
Shodan	54,55%	6
Censys	36,36%	4
VirusTotal	36,36%	4
Ninguna de las anteriores	36,36%	4
TOTAL	**100,00%**	**18**

Nota. Autoría propia

En la cuarta pregunta ¿Ha realizado en algún momento un escaneo de vulnerabilidades y puertos del nombre de su sitio web que se encuentran expuestos en el Internet?, se puede observar en la Tabla 4 que los ISP si realizan escaneo de vulnerabilidades y puertos expuestos al Internet de su respectivo nombre del sitio web con un 81.82%.

Tabla 4
Se ha escaneado en algún momento las vulnerabilidades del nombre del sitio web

Se ha realizado escaneo de vulnerabilidades en algún momento	Porcentaje	No. Personas
Si	81,82%	9
No	18,18%	2
TOTAL	**100,00%**	**11**

Nota. Autoría propia

En la quinta pregunta ¿Conoce usted si los motores de búsqueda avanzada como Shodan, Censys y VirusTotal disponen de una API de desarrollo que permitan escanear las vulnerabilidades o puertos del nombre de su sitio web?, se puede observar en la Tabla 5 que el 54.55% de los encuestados conocen de la existencia del API y el 45.45% no lo sabe, los motores de búsqueda deberían enfatizar en las API para mejorar los escaneos y que se realicen de forma automática.

Tabla 5
Conocimiento de la existencia de API en los motores de búsqueda

Conocimiento de la existencia de API en los motores de búsqueda	Porcentaje	No. Personas
Si	54,55%	6
No	45,45%	5
TOTAL	**100,00%**	**11**

Nota. Autoría propia

En la sexta pregunta ¿En base a su experiencia al escanear vulnerabilidades o puertos del nombre de su sitio web utilizando los motores de búsqueda mediante el API le sería de ayuda que los resultados del escaneo se consoliden en dashboards?, se observa en la Tabla 6 en gran porcentaje del 63.64% que sería de gran ayuda visualizar las vulnerabilidades escaneadas en dashboards.

Tabla 6
Ayuda consolidar las vulnerabilidades en dashboards

Ayuda consolidar las vulnerabilidades en dashboards	Porcentaje	No. Personas
Si, sería de gran ayuda poder observar en dashboards los resultados.	63,64%	7
No, es suficiente con la información que se obtiene por el API	27,27%	3
No he utilizado el API de los motores de búsqueda avanzada	9,09%	1
TOTAL	**100,00%**	**11**

Nota. Autoría propia

En la séptima pregunta ¿Qué tanto cree que le puede ayudar a la toma de decisiones para mitigar las vulnerabilidades o puertos escaneados presentados en dashboards?, se puede observar que consolidar las vulnerabilidades en dashboards ayudaría mucho a la toma de decisiones con el porcentaje de 63.64%, cómo se muestra en la Tabla 7.

Tabla 7
Ayuda para la toma de decisiones sobre las vulnerabilidades encontradas

Ayuda para la toma de decisiones sobre las vulnerabilidades encontradas	Porcentaje	No. Personas
Mucho	63,64%	7
Bastante	18,18%	2
Poco	9,09%	1
Nada	9,09%	1
TOTAL	**100,00%**	**11**

Nota. Autoría propia

2.5.2. Escaneo de vulnerabilidades mediante API de los motores de búsqueda avanzada.

a. Shodan

Las propiedades de los elementos de información (facets) se pueden utilizar para obtener información adicional al filtro (Matherly, 2017) y utilizando los métodos correspondientes del API como contar los puertos expuestos, vulnerabilidades encontradas, datos de http, etc, como son las siguientes:

i. **Http.component**.- Con este facet se puede extraer los nombres de las tecnologías web utilizadas en el sitio web (Matherly, 2017) que se está realizando la búsqueda como se muestra en la Figura 11.
ii. **Http.component_category**.- Con este facet se puede extraer las categorías de los componentes web utilizados en el sitio web (Matherly, 2017) que se realiza la búsqueda como se muestra en la Figura 12.
iii. **IP**.- Con este facet se puede extraer 5 IP con el API que se relacionen con la búsqueda port permite extraer los puertos que se encuentran expuestos y relacionados con la búsqueda relacionada al nombre del sitio web cómo se muestra en la Figura 13.
iv. **Port**.- El facet port permite extraer los puertos que se encuentran expuestos y relacionados con la búsqueda relacionada al nombre del sitio web cómo se muestra en la Figura 14.
v. **Vuln**.- El facet vuln mediante el API muestra el top 5 de vulnerabilidades CVE relacionadas a la búsqueda del nombre del sitio web, cómo se indica en la Figura 15.

b. Censys

Los métodos del API de Censys se encuentran alojados en el dominio https://search.censys.io y se puede obtener los puertos, las IP de los equipos que

tengan referencia con la consulta del nombre del sitio web, los métodos utilizados fueron los siguientes:

i. **Search.-** Con el método search busca todo lo relacionado con la pregunta que en este caso es el nombre de sitio web, la paginación ya que puede traer varios datos por si se pasa el límite de la licencia free, como se muestra en la Figura 16.
ii. **Aggregate.-** con el método aggregate agrega los equipos que tengan relación con la consulta realizada con respecto al nombre del sitio web y en este caso el campo puerto, la respuesta contabiliza los datos obtenidos por puerto se muestra en la Figura 17.
iii. **Experimental.-** con el método experimental se puede observar los eventos que haya tenido alguna IP en específico, ya que la consulta lo realiza con IP se muestra en la Figura 18.

c. VirusTotal

Los métodos del API de VirusTotal permiten escanear los nombres de sitios web y obtener información relevante con respecto a IP, puertos, certificados y análisis de antivirus que tiene la herramienta implementada, los métodos son los siguientes:

i. **Domain.-** Con este método se obtiene datos generales como escaneo de los antivirus que tiene embebida la herramienta, records DNS, datos informativos como el whois y certificados del nombre del sitio web que se realiza la consulta se muestra en la Figura 19.
ii. **Historical_ssl_certificates.-** con este método se puede observar los históricos principales de los certificados relacionados con la búsqueda realizada en este caso el nombre del sitio web se muestra en la Figura 20.
iii. **Communicating_files.-** muestra el escaneo de los archivos que se comunican con el nombre del sitio web que se envía en la consulta como se muestra en la Figura 21.
iv. **Referrer_files.-** con este método se escanea los archivos que hacen referencia a la consulta del nombre de sitio web como se muestra en la Figura 22.
v. **Analyses.-** con el método analyses el API devuelve información relevante del nombre del sitio web como la versión de php o del servidor web como se muestra en la Figura 23.

2.5.3. Comparación de los resultados obtenidos

Luego de haber realizado la encuesta al personal de diferentes ISP y el escaneo de los nombres de los sitios web de los principales proveedores mediante las API públicas, se ha podido obtener los siguientes resultados por cada herramienta.

Los datos de la encuesta muestra que algunos ISP si realizan en algún momento escaneo a los nombres de sus sitios web lo que indica que se preocupan por su seguridad y por la seguridad de los clientes, así también se puede observar que las herramientas de escaneo como Shodan, Censys y VirusTotal son herramientas muy útiles para los encuestados y que conocen de la existencia de su API.

En las encuestas se observa que los ISP en ocasiones creen que la información que manejan no está segura dentro del nombre de su dominio web lo que lleva al siguiente punto de escanear dichos nombres para evidenciar lo que se observa desde el Internet.

Con los escaneos realizados se puede observar que algunos datos que se obtiene de las API son muy similares en cuanto al tipo de información y también son diferentes ya que una de las herramientas tiene implementado análisis por antivirus, otra herramienta muestra las principales vulnerabilidades y exposiciones comunes y la otra herramienta puede mostrar eventos que puede haber tenido el nombre del sitio web, como se muestra a continuación.

a. Análisis de resultados obtenidos por la herramienta Shodan

Con el API de la herramienta Shodan se ha tomado los principales facets para escanear a los nombre del sitio web de los ISP.

Facets http.component.- se observa las tecnologías web que han sido utilizadas para crear el sitio web, en la Tabla 8, se puede evidenciar que los cuatro ISP permiten observar las tecnologías que utilizan en sus sitios web, esta información puede ser utilizada por un atacante y buscar brechas de seguridad en esas tecnologías para luego explotarlas, CNT muestra pocas tecnologías y pocos dispositivos asociados a las tecnologías web utilizadas para sus sitios web.

Tabla 8

Shodan - Comparación de tecnologías web de los ISP

Proveedor de Internet	Facets http.component	Cantidad de hosts
Netlife	jQuery	872
	Bootstrap	366
	ExtJS	331
	Synology DiskStation	329
	Vue.js	325
Puntonet	jQuery	839
	Modernizr	258
	Bootstrap	151
	Google Font API	111
	Font Awesome	75
CNT	PHP	1
	jQuery	1
	jQuery UI	1
Telconet	jQuery	150
	Bootstrap	75
	ExtJS	44
	Font Awesome	44
	Google Font API	32

Nota. Autoría propia

Facets port.- Se observa que el API muestra los puertos que se encuentran expuestos al Internet con la cantidad de dispositivos asociados al nombre del sitio web, según el escaneo realizado CNT es el ISP que menos puertos tiene expuestos con respecto al sitio web, mientras que los que tienen gran cantidad de puertos son los ISP Netlife y Puntonet como se muestra en la Tabla 9.

Tabla 9

Comparación de puertos y cantidad de hosts asociados

Proveedor de Internet	Facets port	Servicio	Cantidad de hosts
Netlife	123	NTP	3345
	80	HTTP	2624
	554	RTSP	2067
	443	HTTPS	1020
	2000	Cisco-SCCP	978

Proveedor de Internet	Facets port	Servicio	Cantidad de hosts
Puntonet	80	HTTP	1789
	22	SSH	1657
	443	HTTPS	1266
	2000	Cisco-SCCP	1139
	8080	HTTP	489
CNT	443	HTTPS	1
Telconet	22	SSH	1229
	80	HTTP	711
	443	HTTPS	508
	7547	CWMP	418

Nota. Autoría propia

Facets vuln.- en el escaneo realizado por el API, se observa que los nombres de dominio de los ISP presentan las principales vulnerabilidades CVE, con estos datos los ISP pueden tener una idea de las vulnerabilidades que tienen los sitios web y realizar las respectivas remediaciones, en la comparación CNT no muestra vulnerabilidades y Netlife es el que muestra mayor cantidad de equipos con vulnerabilidades como se muestra en el Tabla 10.

Tabla 10

Comparación de vulnerabilidades y cantidad de hosts involucrados

Proveedor de Internet	Facets vuln	Cantidad de hosts
Netlife	cve-2022-22719	625
	cve-2022-22720	625
	cve-2022-22721	625
	cve-2022-28330	620
	cve-2022-28614	620
Puntonet	cve-2022-28330	282
	cve-2022-28614	274
	cve-2022-28615	274
	cve-2022-29404	274
	cve-2022-30522	274
CNT	N/A	N/A

Proveedor de Internet	Facets vuln	Cantidad de hosts
Telconet	cve-2022-28330	138
	cve-2022-28614	138
	cve-2022-28615	138
	cve-2022-29404	138
	cve-2022-22719	137

Nota. Autoría propia

b. Análisis de resultados obtenidos por la herramienta Censys

Con el API de Censys se obtiene los datos paginados eso quiere decir que se puede realizar la consulta indicando la cantidad de datos que se requiera analizar, para la investigación se ha extraído los primero 5 valores con los siguientes métodos.

Método aggregate.- al escanear los nombres de dominio de los sitios web de los ISP agrupados por la búsqueda de puertos muestra que CNT presenta menos puertos expuestos al Internet al igual que un solo host relacionado a ese puerto, mientras que Puntonet presenta más host asociados a los puertos expuestos, como se muestra en la Tabla 11.

Tabla 11

Comparación de puertos expuestos y cantidad de host relacionados

Proveedor de Internet	Aggregate	Servicio	Cantidad de hosts
Netlife	80	HTTP	15
	443	HTTPS	13
	25	SMTP	7
	8443	HTTPS	6
	143	IMAP	5
Puntonet	443	HTTPS	37
	80	HTTP	30
	25	SMTP	20
	110	POP3	16
	587	SMTP	16
CNT	80	HTTP	1

Proveedor de Internet	Aggregate	Servicio	Cantidad de hosts
Telconet	443	HTTPS	7
	25	SMTP	5
	110	POP3	5
	80	HTTP	4
	143	IMAP	4

Nota. Autoría propia

Método experimental.- en el escaneo se evidencia los puertos y servicios que otros ISP internacionales han observado con respecto a los nombres de dominio de cada ISP del Ecuador, por el API libre no se observa datos de CNT, es muy posible que no haya sido observado o que estos datos se puedan visualizar con un API de pago, Puntonet muestra puertos de servidores de correo y acceso ssh expuestos al Internet y que han sido observados como se muestra en la Tabla 12.

Tabla 12

Comparación de puertos y servicios que han recibido un evento

Proveedor de Internet	Puerto	Servicio	Protocolo	ISP que analiza	Evento
Netlife	80	HTTP	TCP	PERSPECTIVE_NTT	service_observed
	8070	HTTP	TCP	PERSPECTIVE_NTT	service_observed
	2022	SSH	TCP	PERSPECTIVE_HE	service_observed
	8080	HTTP	TCP	PERSPECTIVE_TATA	service_observed
	8080	HTTP	TCP	PERSPECTIVE_ORANGE	service_observed
Puntonet	995	POP3	TCP	PERSPECTIVE_HE	service_observed
	22	SSH	TCP	PERSPECTIVE_ORANGE	service_observed
	993	IMAP	TCP	PERSPECTIVE_TATA	service_observed
	8443	HTTP	TCP	PERSPECTIVE_ORANGE	service_observed
	8090	HTTP	TCP	PERSPECTIVE_HE	service_observed
CNT	N/A	N/A	N/A	N/A	N/A
Telconet	2444	UNKNOWN	TCP	PERSPECTIVE_NTT	service_observed
	2323	HTTP	TCP	PERSPECTIVE_HE	service_observed
	2000	UNKNOWN	TCP	PERSPECTIVE_NTT	service_observed
	8088	HTTP	TCP	PERSPECTIVE_HE	service_observed
	8883	UNKNOWN	TCP	PERSPECTIVE_HE	service_observed

Nota. Autoría propia

c. Análisis de resultados obtenidos por la herramienta VirusTotal

Con el API de VirusTotal se ha escaneado los nombres de dominio de los sitios web de los ISP con los métodos más relevantes, tomando en cuenta que esta herramienta escanea archivos con antivirus.

Método communicating_files.- el escaneo ha mostrado archivos de diferentes extensiones mismos que con la ayuda del antivirus que la herramienta tiene implementada indica una probabilidad de explotación, siendo Telconet y Netlife muestran las probabilidades más altas como se muestra en la Tabla 13.

Tabla 13

Comparación de tipos de archivos y probabilidad de explotación

Proveedor de Internet	Tipo de archivo	Probabilidad de Explotación
Netlife	Android Package	57
	Java Archive	20
	Sweet Home 3D design (generic)	15.5
	ZIP compressed archive	5.9
	PrintFox/Pagefox bitmap (640x800)	1.4
Puntonet	Win16 NE executable (generic)	26.8
	Win32 Dynamic Link Library (generic)	25.0
	Win32 Executable (generic)	17.1
	Win16/32 Executable Delphi generic	7.9
	OS/2 Executable (generic)	7.7
CNT	Win16 NE executable (generic)	32.3
	Win32 Executable (generic)	28.9
	OS/2 Executable (generic)	13
	Generic Win/DOS Executable	12.8
	DOS Executable Generic	12.8
Telconet	Win64 Executable (generic)	40.3
	Win16 NE executable (generic)	19.3
	Win32 Executable (generic)	17.2
	OS/2 Executable (generic)	7.7
	Generic Win/DOS Executable	7.6

Nota. Autoría propia

Método referrer_files.- en el escaneo realizado se observa los archivos que tienen relación con el nombre de dominio del sitio web, se muestra el análisis de los colaboradores asociados a VirusTotal como se muestra en la Tabla 14 y 15

Tabla 14

Comparación de análisis de los socios de VirusTotal

Proveedor de Internet	Tag	harmless	type-unsupported	suspicious	confirmed-timeout	timeout	failure	malicious	undetected
Netlife	email	0	15	0	0	0	0	31	27
Puntonet	email	0	14	0	0	4	0	7	47
CNT	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Telconet	javascript	0	15	0	0	0	1	6	54

Nota. Autoría propia

Tabla 15

Comparación de resultados del análisis de antivirus de la herramienta

Proveedor de Internet	Tag	Antivirus	Resultado
Netlife	email	Lionic	Hacktool.MSOffice.Generic.3!c
		McAfee	W97M/Downloader.ea
		CAT-QuickHeal	XML.Downloader.33357
		Cyren	W97M/Agent.gen
		ESET-NOD32	multiple detections
Puntonet	email	DrWeb	Exploit.Siggen3.28348
		ALYac	VBA.Heur.Bomber.1.BAEC0A0D.Gen
		Cyren	X97M/Agent.AIU.gen!Eldorado
		ESET-NOD32	GenScript.NDB
		TrendMicro-HouseCall	TrendMicro-HouseCall
CNT	N/A	N/A	N/A
Telconet	javascript	Ikarus	Trojan.JS.Cryxos
		Avast	JS:Facelike-B [PUP]
		Zillya	Trojan.FaceLiker.JS.2
		Microsoft	Trojan:Win32/Tnega!ml
		AVG	JS:Facelike-B [PUP]

Nota. Autoría propia

CONCLUSIONES

Luego de la investigación realizada se evidencia las principales vulnerabilidades relacionadas con versiones inseguras de Apache con su respectivo CVE como por ejemplo se enumera algunos datos: cve-2022-22720, cve-2022-28615, cve-2022-29404, de igual forma algunos virus identificados por el antivirus de la herramienta por ejemplo: JS:Facelike-B [PUP], Trojan:Win32/Tnega!ml, Trojan.JS.Cryxos

Las API de los motores de búsqueda avanzada en su versión libre, que fue la utilizada para la investigación se evidencia que todos los nombres de los sitios web de los ISP tienen por lo menos una vulnerabilidad entre las más representativas son vulnerabilidades de apache, virus troyanos, puertos expuestos que son asociadas a la IP que resuelve el nombre de dominio o los archivos que tiene el sitio web, con el uso del API libre, la herramienta Shodan permite principalmente realizar el conteo de las principales vulnerabilidades en su top cinco, mientras que las API de Censys y VirusTotal permite extraer mayor información.

En el escaneo de vulnerabilidades realizado con Shodan, Censys y VirusTotal se identifica que algunos ISP tienen expuestos al Internet puertos que no suelen ser necesarios publicar como el puerto de acceso remoto ssh o puertos de correo electrónico pop3 e imap,

Se realizan tablas comparativas de los datos obtenidos mediante el API de los motores de búsqueda y así presentar la información de forma legible y clara de los datos que se pueden obtener como primer punto en un auto análisis de vulnerabilidades a nivel de pequeñas y grandes empresas.

Con la herramienta VirusTotal se evidencia que los nombres de dominio de los sitios web pueden contener documentos relacionados con el sitio web, mismos que, al ser escaneados por los antivirus de la herramienta identificaron que tienen alguna vulnerabilidad como virus y con la herramienta Shodan lista las vulnerabilidades CVE, con estos datos se puede suponer que si el usuario utiliza el sitio web del proveedor y descarga algún documento a sus equipos electrónicos que haya sido catalogado como malicioso, podrían ser víctimas de la infección de virus y de igual forma si un delincuente explota alguna de las vulnerabilidades encontradas podría apoderarse de la información de los clientes como nombres completos, dirección domiciliaria, número de cédula y número telefónico.

RECOMENDACIONES

Luego de la investigación realizada es recomendable que cada ISP realice un escaneo de vulnerabilidades y puertos expuestos al Internet cada cierto tiempo para exponer sólo lo que sea necesario y así asegurar la información de la empresa y de los clientes.

Para realizar un autoanálisis fue de gran ayuda utilizar el API sin costo pero ya a nivel empresarial se recomienda gestionar una licencia de pago para realizar análisis más seguidos ya que como se mostró en los resultados no suelen responder al API todos los nombres de dominio.

Se recomienda a los ISP realizar auto escaneos de vulnerabilidades y puertos de los sitios web antes de que sea utilizado por el usuario final con el fin de precautelar la información de los clientes y publicar al Internet solo lo indispensable para el correcto funcionamiento.

Se recomienda a los ISP que instalen en los servidores software de antivirus para que constantemente se encuentren actualizados, realizar auto escaneos con otros motores de búsqueda avanzada, tomando en cuenta que crearse una cuenta sin costo para generar un key para el API no es complicado pero si es necesario contratar personal especializado en el campo de seguridad informática que pueda interpretar los datos obtenidos brindando soluciones y generando sitios web más seguros.

BIBLIOGRAFÍA

ALVARADO CHANG. (2020). *ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR.2(1).* https://revistacientificaistjba.edu.ec/images/home/documentos/Mayo_2020/2.pdf

Avances de la Ciberseguridad y el Cibercrimen desde la realidad de Ecuador [Parte 2/4]. (2021, noviembre 25). LISA Institute. https://www.lisainstitute.com/blogs/blog/avances-ciberseguridad-cibercrimen-ecuador

Coutin García, C. A. (2019). *Análisis de vulnerabilidades mediante pruebas de penetración avanzada Pentesting al sitio web oficial de la Alcaldía del municipio de Quibdó – Chocó*. http://repository.unad.edu.co/handle/10596/26950

Chen, Y., Lian, X., Yu, D., Lv, S., Hao, S., & Ma, Y. (2020). *Exploring Shodan From the Perspective of Industrial Control Systems. IEEE Access,* 8, 75359–75369*.* https://doi.org/10.1109/ACCESS.2020.2988691

Eskandari, S., Leoutsarakos, A., Mursch, T., & Clark, J. (2018). *A first look at browser-based Cryptojacking* (arXiv:1803.02887). arXiv. http://arxiv.org/abs/1803.02887

Fernández, R. J. R., & Hernáiz, J. M. (2018). *Modelización del protocolo Tor y extracción de características de servicios ocultos.* 53.

Fernández, Y. (2019, agosto 23). *API: Qué es y para qué sirve.* Xataka. https://www.xataka.com/basics/api-que-sirve

Harrell, C. R., Patton, M., Chen, H., & Samtani, S. (2018). *Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions. 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), 148–153.* https://doi.org/10.1109/ISI.2018.8587380

Jurado Pallarés, G. (2021). *Plataforma de Monitorización y Descubrimiento de Vulnerabilidades* [B.S. thesis].

Matherly, J. (2017). *Complete Guide to Shodan*. 97.

Mulero Palencia, S. (2021). *Vulnerabilidades en edificios inteligentes.* http://openaccess.uoc.edu/webapps/o2/handle/10609/127648

O'Hare, J., Macfarlane, R., & Lo, O. (2019). *Identifying Vulnerabilities Using Internet-Wide Scanning Data. 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3),* 1–10. https://doi.org/10.1109/ICGS3.2019.8688018

Samarasinghe, N., & Mannan, M. (2017). *Short Paper: TLS Ecosystems in Networked Devices vs. Web Servers. En A. Kiayias (Ed.), Financial Cryptography and Data Security (Vol. 10322, pp. 533–541). Springer International Publishing*. https://doi.org/10.1007/978-3-319-70972-7_30

Vulnerabilidades de sitios web gubernamentales en Ecuador: Un estudio exploratorio pre-muestral - ProQuest. (2019, noviembre 9). https://www.proquest.com/openview/6d12f06cb84b7490cbbcbee7c41e6d3c/1?pq-origsite=gscholar&cbl=1006393

What is an API? (2022, junio 2). https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces

Zelada, S. (2022). *COVID 19: Un acelerador de la transformación digital | Deloitte Perú | Tecnología*. Deloitte Perú. Recuperado el 10 de agosto de 2022, de https://www2.deloitte.com/pe/es/pages/technology/articles/COVID19-un-acelerador-de-la-transformacion-digital.html

ANEXO 1

FORMATO DE ENCUESTA

Encuesta

Universidad Israel	**UNIVERSIDAD TECNOLÓGICA ISRAEL** Maestría en Seguridad Informática

1. Como proveedor de servicio de Internet. ¿Qué tanto conoce sobre las vulnerabilidades del nombre de su sitio web?

   O Mucho

   O Bastante

   O Poco

2. ¿Qué tan segura cree que se encuentra la información entregada por parte de sus clientes hacia usted como proveedor del servicio de Internet?

   O Muy segura

   O Poco Segura

   O Nada Segura

3. Como proveedor del servicio de Internet indique los motores de búsqueda avanzados que conoce para el análisis de vulnerabilidades del nombre de su sitio web.

   ☐ Shodan

   ☐ Censys

   ☐ VirusTotal

   ☐ Ninguna de las anteriores

4. ¿Ha realizado en algún momento un escaneo de vulnerabilidades y puertos del nombre se su sitio web que se encuentran expuestos en el Internet?

   O Si

   O No

5. ¿Conoce usted si los motores de búsqueda avanzada como Shodan, Censys y VirusTotal disponen de una API de desarrollo que permitan escanear las vulnerabilidades o puertos del su dominio web?

   O Si

   O No

6. ¿En base a su experiencia al escanear vulnerabilidades o puertos de su dominio web utilizando los motores de búsqueda mediante el API le sería de ayuda que los resultados del escaneo se consoliden en dashboards?

   - O Si, sería de gran ayuda poder observar en dashboards los resultados.
   - O No, es suficiente con la información que se obtiene por el API
   - O No he utilizado el API de los motores de búsqueda avanzada

7. Como proveedor de servicio de Internet. ¿Qué tanto cree que le puede ayudar a la toma de decisiones para mitigar las vulnerabilidades o puertos escaneados presentados en dashboards?

   - O Mucho
   - O Bastante
   - O Poco