URKUND

Urkund Analysis Result

Analysed Document: urkund19.docx (D44244662)
Submitted: 11/19/2018 10:56:00 PM
Submitted By: razup@unemi.edu.ec
Significance: 1 %

Sources included in the report:

hromerom_M1.830_20171_PEC4 - Memoria final_8217517.txt (D34658569)
http://www.cvedetails.com/vulnerability-list/vendor_id-11936/product_id-41377/version_id-229259/Tp-link-Tl-wr741n-Firmware-3.11.7.html

Instances where selected sources appear:

3

INTRODUCCIÓN

Muchas personas en la actualidad no conocemos la forma de llamar a la interconexión de nuestros objetos o cosa (es decir de una cosa a otras cosas, servicios o personas a través de internet), a esto se le llama internet de las cosas (IoT). IoT nos ayuda con herramientas para incrementar el desempeño en muchas áreas como salud, logística, industria, seguridad, agricultura y medio ambiente.

Las tecnologías digitales evolucionan a través de los tiempos es así como las organizaciones están examinando dicha evolución. El estudio de grandes volúmenes de información (datos) afecta los procesos empresariales y la forma en que se determinan sus acciones; esto lo revelan las redes sociales mediante las interacciones y consumos de los clientes; las aplicaciones móviles y el almacenamiento en la nube son importantes para ofrecer servicios.

El Internet de las Cosas (IoT) asocia diferentes productos a través de sensores así crea nuevas posibilidades tanto para crear valor como para reducir costos, ya que son clave para la evolución de los suministros.

Para Latino América, se estima un crecimiento del 21% en el tráfico de Internet; 6,7% en usuarios de Internet; un 8% en conexiones de dispositivos (CAGR de 2015 a 2020). CITATION Cis16 \l 3082 (Cisco, 2016).

El desarrollo de propuestas de valor basadas en el IoT demanda conocimiento y experiencia en tecnología. Para las organizaciones no tecnológicas resulta difícil brindar una solución completa basada en el IoT en forma independiente. Se recomienda construir un ecosistema de aliados y co-desarrollar con ellos CITATION Kra17 \l 12298 (Kranz, 2017). Debido al IoT, la industria está evolucionando rápidamente a un mundo de ecosistemas de alianzas y co-creación con los clientes. Se trata de una transición compleja y estratégica tanto para vendedores como para usuarios de las soluciones basadas en tecnología y esto resulta en un ecosistema abierto de proveedores de soluciones IoT basadas en estándares CITATION Kra17 \l 12298 (Kranz, 2017). CITATION Wei15 \l 12298 (Weill & Woerner , 2015) destacan que las organizaciones no solo fracasan en tomar las oportunidades dadas por la digitalización, sino que no logran adaptar sus modelos de negocios para reflejar las características económicas y los mecanismos subyacentes de la digitalización. Es decir, para aprovechar las oportunidades se requiere un liderazgo que entienda las oportunidades y los recursos y las capacidades necesarias.

En los últimos años se ha observado un gran avance tecnológico y el servicio de Internet no es la excepción, dando como resultado el término “Internet de las cosas” (IoT, por sus siglas en inglés)CITATION Fig14 \l 12298 (Figuerola, 2014).

A pesar de que se pronostica un acelerado crecimiento de IoT en todas las áreas, donde se encuentra más maduro es en el ámbito de los vestibles (wearables) ya que existe una gran cantidad de productos que se han estado comercializando y evolucionando desde hace varios años CITATION Luq16 \l 12298 (Luque, 2016).

Son muchos los dispositivos vestibles que existen actualmente: lentes, gorras, relojes, bandas, ropa, zapatos, joyas, cinturones, cascos, etc.; sin embargo, los más utilizados son los que se usan en la muñeca CITATION Luq16 \l 12298 (Luque, 2016).

(Figuerola, 2014; Rahman, Daud, & Mohamad, 2016) mencionan que para el año 2020 la cantidad de dispositivos conectados en total será de 50 mil millones, mientras que CITATION YuS15 \l 12298 (Yu, Sekar, Seshan, Agarwal, & Xu, 2015), argumentan que, para el mismo año, habrá 25 mil millones de dispositivos sólo de IoT. Este gran incremento en el número de dispositivos conlleva un gran reto para la seguridad, ya que por lo general son productos novedosos que ofrecen una funcionalidad específica y muchos fabricantes descuidan las características de seguridad, debido a la competencia por llegar primero al mercado y que su producto sea fácil de usar CITATION YuS15 \l 12298 (Yu, Sekar, Seshan, Agarwal, & Xu, 2015).

CAPÍTULO 1

PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del Problema

En la actualidad en cada hogar por lo menos tenemos un dispositivo inteligente, dichos equipos tienen sus vulnerabilidades las cuales vamos a analizar, se utilizó el primer motor de búsqueda del mundo para dispositivos conectados a Internet (SHODAN).

De acuerdo con el análisis, en el último mes un 61% de las amenazas detectadas por el servicio de Ciberalarma se deben al uso de aplicaciones potencialmente peligrosas (PUAs); el 15% a hacking; cerca de un 12% a troyanos, y un 4% a programas que muestran publicidad, banners o pop-ups (adware). Sin embargo, "aunque un 67% de los hogares admite haber tenido un problema de fraude online, solo un 19% está protegido con un servicio de antifraude", explica Miguel Ángel González Losada, CEO de Virtual Care. Asimismo, un 27% de los usuarios desconoce si tiene protegida su WiFi; un 30% se conecta a redes públicas de cualquier tipo, y un 29% se descarga apps de fuentes desconocidas. CITATION Cib18 \l 3082 (Ciberalarma, 2018)

Un estudio realizado por HP revela que un 70% de los dispositivos de IoT no cifran sus comunicaciones, el 70% permiten a un atacante identificar las cuentas de usuario válidas, el 60% de los que tienen interfaz de usuario son vulnerables a distintos ataques como secuencias de comandos en sitios cruzados (XSS). Considerando que estos dispositivos recopilan una gran cantidad de información sensible para los usuarios, esto se vuelve un gran riesgo de seguridad. CITATION Rah16 \l 3082 (Rahman, Daud, & Mohamad, 2016)

Otras fuentes también inciden en casi los mismos porcentajes es decir en cada hogar en el mundo al menos un equipos está infectado por algún virus, el mismo puede traer como consecuencia el acceso a información que manejemos en la red de nuestra casa, oficina, etc.

El análisis de los estudios primarios permitió identificar que el principal problema de seguridad en IoT se encuentra en la fase de comunicación, convergiendo hacia temas de cifrado, de los cuales se detectaron: falta de un estándar de cifrado y descifrado, falta de

algoritmos ligeros de cifrado que permitan implementarse en dispositivos con poca capacidad de procesamiento, fuga de información, pérdida de confidencialidad, comunicaciones no protegidas, rastreo de paquetes, etc., el total de estudios primarios seleccionados y el análisis completo, se pueden consultar en CITATION Mar16 \l 3082 (Martínez, Mejía, & Muñoz, 2016).

1.2 Sistematización

¿Cuántos dispositivos aparecen conectados a internet según Shodan?

¿Cuáles son los tipos de vulnerabilidades que presentan los diferentes dispositivos?

¿Qué medidas debemos de tomar para corregir la vulnerabilidad?

1.3 Objetivos

Objetivo General

Analizar las diferentes vulnerabilidades de los dispositivos conectados a internet en el Ecuador visibles desde el motor de búsqueda Shodan.

Objetivos Específicos

• Consultar en Shodan los dispositivos conectados a Internet en el Ecuador.

• Determinar y analizar por los modelos de las marcas de los dispositivos, cuales son los tipos de vulnerabilidades que los mismos poseen.

• Visualizar el código de vulnerabilidad de los modelos de las marcas de los dispositivos para saber si ya el error esta resulto por el fabricante.

1.4 Justificación del Problema

Esta investigación se la realizo para así poder analizar ciertas vulnerabilidades que pueden tener nuestros equipos ya que tenemos un problema con relación a la masificación. Tenemos graves errores de seguridad, muchas empresas tienen la responsabilidad de cuidar esos datos y que no se difundan.

Dar a conocer que muchas veces la culpa de que nuestra información no esté segura es nuestra responsabilidad ya que decidimos ahorrar dinero cuando compramos estos aparatos que muchos no cuentan con garantía de seguridad. Muchas veces pensamos que solo hackers maliciosos y que son “profesionales” pueden ser una amenaza para estos dispositivos pero no es así ya que si alguna persona que este inmiscuida en este “campo” puede seguir dichos defectos ya que si no cuentan con una correcta implementación pueden ser susceptible de ser atacado.

Las brechas de seguridad que desconocemos pueden afectar a nuestro sistema ya que por el hardware que hemos adquirido puede ser vulnerable por las medidas de seguridad no son adecuadamente estrictas. Un ejemplo es el caso de los primeros lectores de huellas para

móviles Samsung que tenían una brecha de seguridad que permitían a otras aplicaciones acceder a ellas.

Se ha llegado a pensar en el mundo que solo nuestros Smartphone, Pcs, Smart TV son las que se conectan a internet pero que decimos de la cámara de seguridad instalada en nuestro hogar, empresa, los relojes o las pulseras, nuestros electrodomésticos, alarmas, GPS, hasta incluso nuestras mascotas; por ello el llamado internet de las cosas seguirá evolucionando y con ello sus vulnerabilidades.

CAPÍTULO 2

MARCO TEÓRICO CONCEPTUAL

2.1 Antecedentes

Origen de la IoT

Según CITATION Bru17 \l 12298 (Cendón, 2017) detalla de la siguiente manera el origen de la IoT

El Internet de las Cosas, el famoso Internet of Things o IoT, está de moda. Conectar cualquier objeto a Internet y con ello crear infinidad de nuevas aplicaciones ha levantado grandes expectativas. Y aunque parece que es un concepto que nos ha acompañado desde hace muchísimo tiempo dada su omnipresencia en cualquier artículo o discusión tecnológica de hoy en día, la realidad es que es bastante reciente.

Fue en 2009 cuando Kevin Ashton, profesor del MIT en aquel entonces, usó la expresión Internet of Things (IoT) de forma pública por primera vez, y desde entonces el crecimiento y la expectación alrededor del término ha ido en aumento de forma exponencial. Fue en el RFID journal cuando Ashton acuñó públicamente el término. Aunque él mismo ha comentado que la expresión era de uso corriente en círculos internos de investigación desde 1999, si bien no se hizo público de forma notoria hasta entonces. CITATION Bru17 \l 12298 (Cendón, 2017)

“Si tuviésemos ordenadores que fuesen capaces de saber todo lo que pudiese saberse de cualquier cosa –usando datos recolectados sin intervención humana– seríamos capaces de hacer seguimiento detallado de todo, y poder reducir de forma importante los costes y malos usos. Sabríamos cuando las cosas necesitan ser reparadas, cambiadas o recuperadas, incluso si están frescas o pasadas de fecha. El Internet de las Cosas tiene el potencial de cambiar el mundo como ya lo hizo Internet. O incluso más.”

CITATION Kev09 \l 3082 (Ashton, 2009)

Raro es el artículo periodístico sobre nuevas tecnologías o transformación digital que no incluya alguna mención sobre el IoT, ya sea ésta de forma directa o tangencial. Y es que es un hecho que la capacidad de poder conectar cualquier objeto es un concepto que despierta de forma inusual la imaginación.

CITATION Bru17 \l 12298 (Cendón, 2017)

Si queremos entender en su totalidad el origen y el alcance del IoT sería un error centrarse únicamente en la actividad de los últimos años. Es conveniente recular y echar un vistazo al pasado analizando cómo las distintas evoluciones tecnológicas nos han traído de forma irremediable a este punto. CITATION Bru17 \l 12298 (Cendón, 2017)

Del Mont-Blanc Al IoT

Porque el origen de los objetos conectados no es algo de hace pocas décadas, en realidad se remonta hasta los albores tecnológicos del siglo XIX, en lo que se consideran los primeros experimentos de telemetría de la historia. El primero del que se tiene constancia fue el llevado a cabo en 1874 por científicos franceses. Estos instalaron dispositivos de información meteorológica y de profundidad de nieve en la cima del Mont Blanc. A través de un enlace de radio de onda corta, los datos eran transmitidos a París. Otros experimentos, ya en el siglo XX, se realizaron desde iniciativas originadas en países como Rusia o Estados Unidos, ayudando al crecimiento de la telemetría y llevándola a un uso extensivo impulsado por la evolución de distintas tecnologías de telecomunicación.

CITATION Bru17 \l 12298 (Cendón, 2017)

La idea de poder conectar los objetos y de que éstos fuesen inteligentes ya se plasmó en aquella época en los pensamientos y escritos de científicos tan notables como Nikola Tesla o Alan Turing. Sus palabras, leídas desde una perspectiva histórica, cobran ahora sentido y demuestran cuan adelantados a su tiempo fueron.

CITATION Bru17 \l 12298 (Cendón, 2017)

En 1926,

Nikola Tesla en una entrevista a la revista Colliers anticipó de forma sorprendente el crecimiento de la conectividad a nivel global y la miniaturización tecnológica:

“Cuando lo inalámbrico esté perfectamente desarrollado, el planeta entero se convertirá en un gran cerebro, que de hecho ya lo es, con todas las cosas siendo partículas de un todo real y rítmico… y los instrumentos que usaremos para ellos serán increíblemente sencillos comparados con nuestros teléfonos actuales. Un hombre podrá llevar uno en su bolsillo”

CITATION Nik26 \l 3082 (Tesla, 1926)

Recordemos que Nikola Tesla, entre otros descubrimientos, fue uno de los padres de las comunicaciones inalámbricas. Su visión siempre fue más allá del propio descubrimiento tecnológico y postuló de forma premonitoria alguna de sus aplicaciones, principalmente en dos: la interconexión de todo en lo que él denominó un “gran cerebro” y la simplicidad de los terminales que usamos para ello, avanzando cómo los ordenadores personales, y más tarde los teléfonos inteligentes y cualquier tipo de dispositivo, dispondrán de una conexión a este “gran cerebro” que hoy en día conocemos como Internet.

CITATION Bru17 \l 12298 (Cendón, 2017)

Premonitorias también fueron las palabras de Alan Turing en 1950 en su artículo en el Computing Machinery and Intelligence in the Oxford Mind Journal, en el cual ya avanzó la necesidad futura de dotar de inteligencia y capacidades de comunicación a los dispositivos sensores:

"...también se puede sostener que es mejor proporcionar la máquina con los mejores órganos sensores que el dinero pueda comprar, y después enseñarla a entender y hablar inglés. Este proceso seguirá el proceso normal de aprendizaje de un niño"

CITATION Ala50 \l 3082 (Turing, 1950)

Pero a pesar de estos postulados y la visión tan temprana que supieron transmitir estos y otros científicos, la inmadurez tecnológica de la época hizo que todo esto quedase como entelequias irrealizables. No fue hasta la década de los 60 y, sobre todo, los 70 cuando se crearon los primeros protocolos de comunicaciones que definirían la base de lo que hoy es Internet. Este desarrollo se realizó dentro del seno de la red ARPANET, en el Departamento de Defensa de EEUU. Aunque también cabe destacar que durante muchos años, estos protocolos fueron exclusivamente de uso militar y académico. CITATION Bru17 \l 12298 (Cendón, 2017)

El avance de esta red de redes fue lento durante las décadas de los 70 y 80 por varios motivos, siendo el principal la falta de comunicaciones rápidas y de bajo coste a medias y largas distancias lo cual facilitó la creación de redes heterogéneas, totalmente incompatibles entre sí. Nos encontramos pues en esta época con un ecosistema de silos de equipos conectados de forma local. Y no fue hasta mediados de los 90 que el Internet comercial y universal comenzó su expansión definitiva. Los silos se interconectaron mediante un protocolo de comunicaciones, el famoso TCP/IP, base de Internet, y las implementaciones no estándar comenzaron su declive. De esta forma, la red militar y académica que una vez fue ARPANET, se convirtió en INTERNET y con ello, en el origen de infinidad de nuevos modelos sociales y de negocio. CITATION Bru17 \l 12298 (Cendón, 2017)

Y fue ante la popularización de esta incipiente Internet que la idea de conectar objetos mediante esta red empezó pronto a popularizarse. Ya en 1990 John Romkey, en el evento Interop en EEUU, creó el primer objeto conectado a Internet: una tostadora que se podía encender o apagar en remoto. La conectividad fue a través del ya mencionado protocolo TCP/IP y el control se realizó mediante SNMP (Simple Network Management Protocol), protocolo de gestión de red, que se usó para controlar el encendido y apagado del electrodoméstico.

CITATION Bru17 \l 12298 (Cendón, 2017)

A pesar de suponer una revolución en la forma de entender las redes, las comunicaciones que Internet ofrecía en el origen de su expansión mundial eran principalmente cableadas. Esto, unido a que el coste del hardware era aún elevado, hizo que las ideas que podían llevar a implementar objetos conectados prácticamente pasasen inadvertidas durante años.

CITATION Bru17 \l 12298 (Cendón, 2017)

La revolución vino de la mano de la popularización de conectividad inalámbrica, ya fuese celular o WiFi, durante el inicio del siglo XXI. Esta permitió por fin presenciar una primera explosión en el crecimiento de los objetos conectados. Y este crecimiento se ha constatado especialmente en la última década, donde se han venido sucediendo nuevos conceptos como el WSN (Wireless Sensor Networks) o M2M (Machine to Machine), para finalmente dar paso al IoT que todos conocemos.

CITATION Bru17 \l 12298 (Cendón, 2017)

Esta historia aún no está terminada. Nos encontramos en plena efervescencia evolutiva dentro del IoT. Este es un relato que ha empezado con las tecnologías existentes en su momento, pero que se está escribiendo con nuevas redes, nuevos protocolos y nuevos dispositivos. Aún estamos en una fase de coexistencia y de crecimiento.

En futuros artículos comentaré estos aspectos. De momento quedémonos con la historia que ha llevado a la telemetría y a Internet a confluir en lo que hoy conocemos como el IoT. CITATION Bru17 \l 12298 (Cendón, 2017)

Evolución de la IoT

IoT revolucionará la manera en que las personas y las organizaciones interactúan con el mundo físico, la interacción con dispositivos domésticos, automóviles, plantas industriales, etc., sufrirá grandes modificaciones. También permitirá que muchos servicios como salud, educación y gestión de recursos, puedan ser mejorados para comodidad del cliente CITATION XuW14 \l 12298 (Xu, Wendt, & Potkonjak, 2014).

A pesar de que se pronostica un acelerado crecimiento de IoT en todas las áreas, donde se encuentra más maduro es en el ámbito de los vestibles (wearables) ya que existe una gran cantidad de productos que se han estado comercializando y evolucionando desde hace varios años CITATION Luq16 \l 12298 (Luque, 2016).

Son muchos los dispositivos vestibles que existen actualmente: lentes, gorras, relojes, bandas, ropa, zapatos, joyas, cinturones, cascos, etc.; sin embargo, los más utilizados son los que se usan en la muñeca CITATION Luq16 \l 12298 (Luque, 2016).

FUNDAMENTOS TEÓRICOS

DIFERENCIA ENTRE INTERNET Y WEB

Antes de que podamos ver la importancia de IoT, es necesario comprender las diferencias que existen entre Internet y World Wide Web (o web), términos que suelen utilizarse indistintamente. Internet es la capa física o la red compuesta de switches, routers y otros equipos. Su función principal es transportar información de un punto a otro, de manera veloz, confiable y segura. La web, por otro lado, es una capa de aplicaciones que opera sobre la superficie de Internet. Su rol principal es proporcionar una interfaz que permite utilizar la información que fluye a través de Internet.CITATION CIS \l 3082 (CISCO)

IOT (INTERNET OF THINGS)

Internet de las cosas, revolución tecnológica que posibilita que Internet alcance el mundo real de los objetos físicos, convirtiendo objetos comunes en “cosas inteligentes” conectadas a Internet. CITATION Fer15 \l 3082 (Fermín Pérez & Guerra Guerra, 2015)

CLASIFICACIÓN DE LOS DISPOSITIVOS DE IOT Tabla 1. Clasificación de IoT

Ámbito Dispositivos Vestibles Relojes, lentes, bandas fitness y de salud, anillos, pulseras, ropa, cinturones, etc. Domótica Alarmas, cerraduras, cámara, refrigeradores, televisores, manejo automático de luces, control de temperatura, automatización de cortinas, riesgo de macetas y jardines, etc. Industriales Variedad de sensores para monitorizar y controlar producción, monitorizar inventario, monitorizar estado físico y ubicación de los empleados, etc. Automotriz GPS, sensores en llantas para ahorrar combustible, seguros automáticos en puertas, encendido inteligente, estacionamiento automático conducción automática, etc. Ciudades inteligentes Detectores de velocidad para monitorizar tráfico, sensores en las estructuras de los edificios para monitorizar su estado, cámaras de vigilancia, sensores para monitorizar el uso de bicicletas, estacionamientos inteligentes, sensores para medir la congestión de tráfico y redirigirlo en tiempo real para agilizarlo, vigilancia mediante drones, etc. Fuente: Juan-Manuel Martínez; Jezreel Mejía; Mirna Muñoz; et al. (2017)

SHODAN

Shodan recopila información sobre todos los dispositivos conectados directamente a Internet. Si un dispositivo está conectado directamente a Internet, Shodan lo consulta para obtener información diversa disponible públicamente. Los tipos de dispositivos que se indexan pueden variar enormemente: desde computadoras de escritorio pequeñas hasta plantas de energía nuclear y todo lo que se encuentre en el medio. CITATION Sho \l 3082 (Shodan)

COMANDOS UTILZADOS EN SHODAN

Según Shodan utiliza los siguientes comandos para filtrar las búsquedas:

Comandos de Ubicación

Los comandos “country”, “state” y “city”, permiten acortar por ubicación geográfica las búsquedas. Por ejemplo; “country:US”, “state:LA”, “city:Denver”, “postal:12345”. Utilizando cualquiera de estos filtros es factible buscar dispositivos por ubicación geográfica. También siendo factible combinar filtros individuales si se requiere. CITATION Cab17 \l 12298 (Caballero Quezada, 2017)

Figura 1. Búsqueda por comandos de ubicación Fuente: Shodan Comandos de Red

Los comandos “org”, “net”, “hostname” y “port” permiten acortar las búsquedas utilizando filtros basados en red. “org” busca organizaciones individuales por nombre, “net” busca por direcciones IP individuales o un rango completo de red. “hostname” permite escanear Internet completa por dominios individuales, se puede utilizar parte del FDQN, como “bing” o el sitio

web completo como “www. sony. com”. “port” busca sistemas por puertos abiertos. Por ejemplo; “org:Bing”, “net:192.168.0.50”, “hostname:sony.com”, “port:3309”. CITATION Cab17 \l 12298 (Caballero Quezada, 2017)

Figura 2. Búsqueda por comandos de red Fuente: Shodan Comandos de Página Web

Los filtros “title” y “html” permiten acortar las búsquedas utilizando los filtros basados en páginas web. El filtro “title” es probablemente uno de los parámetros de búsqueda más obviados. Se puede escanear Internet completo o un dominio completo buscando por palabras clave en el título. El filtro “html” permite escanear por una palabra específica o cadena en el código html de la página web. CITATION Cab17 \l 12298 (Caballero Quezada, 2017)

Figura 3. Búsqueda por comandos de Páginas web Fuente: Shodan

Comandos de Software

Los filtros “os”, “product” y “version” permiten acortar las búsquedas utilizando filtros basados en software. Por ejemplo; “os:Linux”, “product:Apache” y “version:1.6.8”. Estos permiten buscar por sistema operativo, tipo de producto y versión de software CITATION Cab17 \l 12298 (Caballero Quezada, 2017).

Figura 4. Búsqueda por comandos de software Fuente: Shodan

Probablemente la manera más popular para buscar en Shodan es utilizando la búsqueda de palabra clave en el cuerpo. Si se conoce el tipo de servidor del sistema objetivo utilizando el nombre de un servidor incorporado, y se desea buscar por únicamente páginas web “200 OK”, entonces la búsqueda por palabra clave en el cuerpo es aquella a utilizar CITATION Cab17 \l 12298 (Caballero Quezada, 2017).

• 200 OK: No requerirán autenticación

• 401 Unauthorized: Requerirá autenticación con user y password

• 403 Forbidden: El acceso es denegado con independencia de la autenticación

Figura 5. Búsqueda por palabra clave Fuente: Shodan

Shodan nos permite ver máximo dos páginas porque si no nos muestra un error, indicándonos que compremos una membresía.

Figura 6. Muestra de error Fuente: Shodan

DEFINICIONES DE LAS VULNERABILIDADES

En el artículo presentado por CITATION Fra13 \l 12298 (Franco, Perea, & Tovar, 2013), indica que se presentan algunas definiciones y conceptos necesarios para situar la propuesta en su justo contexto. Por lo tanto en esta sección se definen términos tales como Base de datos

Nacional de Vulnerabilidades (NVD), código de vulnerabilidades y amenazas comunes (CVE), Sistema común de puntuación de vulnerabilidades (CVSS), la Identificación de servicios.

NVD: Base de datos nacional de vulnerabilidades

NVD (National Institute of Standards and Technology, 2011) es un repositorio estandarizado del gobierno de los Estados Unidos en el cual se encuentra almacenada información acerca de la gestión de vulnerabilidades. Estos datos permiten la automatización de la gestión de vulnerabilidades y la toma de medidas de seguridad. NVD incluye bases de datos con listas de control de seguridad, fallos de seguridad relacionados con software, errores de configuración, nombres de productos y métricas de impacto. En la actualidad cada día se adiciona a la NVD un promedio de 12 nuevas vulnerabilidades. La información sobre estas vulnerabilidades puede ser accedida a través de diferentes fuentes de datos proporcionadas en formato XML cuya actualización es continua. (p.15)

CVE (Common Vulnerabilities and Exposures)

El código CVE (vulnerabilidades y amenazas comunes) es un identificador que se asigna a cada vulnerabilidad que se conoce públicamente con el fin de que pueda ser identificada de forma unívoca (The MITRE Corporation, 2011). Este código fue creado por la corporación MITRE y permite que los usuarios puedan conocer de forma objetiva las vulnerabilidades de un sistema computacional. Los identificadores CVE se presentan en el formato CVE-AÑO-NUMERO y están acompañados de una breve descripción de la vulnerabilidad o amenaza y un grupo de referencias pertinentes. (p.16)

CVSS: Sistema común de puntuación de vulnerabilidades

CVSS (Mell et al., 2007) es un sistema de puntuación de vulnerabilidades diseñado con el fin de proporcionar un método abierto y estandarizado para la clasificación de vulnerabilidades en tecnologías de la información. Con esto ayuda a las organizaciones a priorizar y coordinar una respuesta concertada para la mitigación de vulnerabilidades de TIC. Adicionalmente CVSS provee a profesionales en seguridad informática, ejecutivos y usuarios finales un lenguaje común para discutir la severidad de las vulnerabilidades de seguridad. (p.16)

CVSS utiliza tres tipos de métricas: Base, temporal, ambiental. La primera representa la característica fundamental de la vulnerabilidad que no varía con el tiempo ni el ambiente; la segunda representa las características que cambian con el tiempo pero no varían entre ambientes de trabajo; la tercera representa las características de las vulnerabilidades que solo son relevantes para un entorno específico. Las tres métricas de CVSS están en un rango de 0 a 10 y se utilizan para determinar la severidad de las vulnerabilidades. (p.16)

Identificación de servicios

Es una técnica de enumeración utilizada para obtener información acerca de un sistema computacional dentro de una red y de los servicios que se ejecutan en sus puertos. Esta técnica suele ser utilizada por administradores para determinarlos sistemas y servicios en sus redes; sin embargo los atacantes informáticos la utilizan para conocer las versiones de los

servicios activos en los equipos de red (Franco et al., 2012) y determinar si existen exploits para estos (Mcclure et al., 2005). (p.16)

CWE (Common Weakness Enumeration)

CWE (Enumeración de debilidad común) es una lista de tipos de debilidades de software dirigida a desarrolladores y profesionales de la seguridad. Fue creada al igual que CVE para unificar la descripción de las debilidades de seguridad de software en cuanto a arquitectura, diseño y código se refiere. Se puede ver como un catálogo de debilidades documentadas que se suelen cometer programando, y que podría derivar en vulnerabilidades. Es muy utilizada por distintas herramientas de seguridad encargadas de identificar estas debilidades y para promover la identificación de las vulnerabilidades, mitigación y su prevención. CITATION Umb14 \l 12298 (Schiavo, 2014)

CAPÍTULO 3

METODOLOGÍA

Nuestro tema: “Internet de las cosas – Análisis de vulnerabilidades de dispositivos que se pueden visualizar en SHODAN: Caso de Estudio Ecuador” se ha planteado los objetivos y referencias buscadas que están relacionada con el mismo nuestra investigación seria de tipo descriptiva y documental.

Se realizó una investigación descriptiva ya que analizaron datos recopilados en Shodan y documental ya que se revisaron artículos web relacionados al tema.

La investigación se ha desglosado de la siguiente manera:

Fase 1:

Se comenzó la elaboración del presente trabajo de investigación se limitó el área geográfica que se utilizó al momento de la consulta de los datos que fue Ecuador.

Fase 2:

Luego de tener delimitada el área geográfica que se utilizó para el estudio, se procedió a realizar la búsqueda de la información en Shodan que es un motor de búsqueda que nos permite conocer cierta información sobre dispositivos conectados a internet, tales como: números aproximados de equipos interconectados que existen, marca y modelo del mismo, y después se hizo una investigación por marca y por modelo de equipos se obtuvo resultado de los mismos.

Fase 3:

Con los datos que nos salieron en los reportes que Shodan nos proporcionó se buscó si los equipos consultados daban algún tipo de vulnerabilidad.

Fase 4:

Luego se encontró por el CVE y CWE la descripción de los códigos y si hubo alguna actualización para corregir el error en el equipo que contenía la vulnerabilidad.

CAPÍTULO 4

DESARROLLO DEL TEMA

El presente trabajo de investigación se lo realizó para la búsqueda de vulnerabilidades en los dispositivos que se conectan a internet, para poder realizar la misma se procedió a crear una cuenta en el motor de búsqueda Shodan, luego de eso se procedió a la búsqueda por posibles vulnerabilidades como contraseña por default, o la marca del dispositivo, o modelos del mismo, también por el nombre del país usando los filtros correspondientes que se mostraran a continuación.

Para crear la cuenta en Shodan se ingresó a la página web www.shodan.io y se siguieron los pasos descritos:

1. Se da clic en iniciar sesión o registrarse.

2. Luego en registro y se llenan los campos solicitados, y se hace clic en el botón crear.

3. Al correo electrónico indicado en el campo va a llegar un correo de activación se da clic en el link para que la cuenta se active.

4. Nos llega un mensaje con la bienvenida a Shodan y ahora se utiliza Shodan

5. En Shodan con el usuario y la contraseña que creada se ingresa a una interfaz así

Figura 7. Página web de Shodan Fuente: Shodan

Luego que se creó la cuenta en la barra de navegación de Shodan se encontró la barra de búsqueda en la cual se procedió a buscar la información necesaria.

Se utilizaron las palabras default password y se observó los resultados, pero como se ha visto aparecieron resultados de todo el mundo.

Figura 8. Búsqueda por default password Fuente: Shodan

Es por eso que hizo el uso de los comandos para filtrado esto nos ayudó a la búsqueda hacia algo en específico, se usó un comando ubicación en este caso Ecuador se utilizó country:ec y luego se dio clic en crear reporte, envió a nuestro correo.

Figura 9. Búsqueda por filtro ec Fuente: Shodan

Los números que salieron en Shodan son de diversos dispositivos pero en muchos de los casos no mostró los modelos de los mismos y el trabajo se lo enfoco en varios modelos que presentaron vulnerabilidades para aquello los modelos que salieron se buscó en el siguiente link https://www.cvedetails.com si tenía algún tipo de vulnerabilidad y para la enumeración de debilidad común por el código que nos mostró CVE se observó en CWE https://cwe.mitre.org.

ROUTER Se realizo la busqueda por router y mostrò 3,141 dispositivos y el top de dichos dispositivos eran los siguientes: Tabla 2. Top Productos y Ciudades -Router TOP PRODUCTOS TOP CIUDADES TP-LINK WR740N / TL-WR741ND 1,520 Ambato 1,457 TP-LINK WR841N 789 Quito 493 Huawei Home Gateway 376 Guayaquil 185 D-link 295 Cuenca 70 Fuente: Elaboración propia

Figura 10. Búsqueda por router country: ec Fuente: Elaboración propia TPLINK Empresa fabricante de productos incluyen redes de comunicación inalámbrica, routers, routers portátiles, routers 3G/4G, switches, adaptadores Powerline, cámaras IP y servidores de impresión. TP-LINK WR740N / TL-WR741ND

Figura 11. Búsqueda por TP-LINK WR740N / TL-WR741ND country: ec Fuente: Elaboración propia Hallazgo Tabla 3. Hallazgo de vulnerabilidad TP-LINK WR740N / TL-WR741ND Vulnerabilidad: CVE-2017-14250 Publicado: 2017-10-31 Link: www.cvedetails.com/vulnerability-list/vendor_id-11936/product_id-41377/version_id-229259/Tp-link-Tl-wr741n-Firmware-3.11.7.html Descripción: En

0: http://www.cvedetails.com/vulnerability-list/vendor_id-11936/product_id-41377/version_id-229259/Tp-link-Tl-wr741n-Firmware-3.11.7.html 73%

TP-LINK TL-WR741N / TL-WR741ND 150M Wireless Lite N Router con versión de firmware 3.11.7 Build 100603 Rel.56412n y versión de hardware: WR741N v1 / v2 00000000,

el parámetro SSID en la "Configuración inalámbrica" no está validado correctamente. Es posible inyectar código malicioso: >/script< >H1< BUG / * >/script< >a href=XXX.com<. La segunda carga útil bloquea el cambio de la configuración inalámbrica. Se requiere un reinicio de fábrica. CWE - 20: Cuando el software no valida la entrada correctamente, un atacante puede crear la entrada en una forma que el resto de la aplicación no espera. Esto conducirá a que partes del sistema reciban entradas no intencionadas, lo que puede resultar en un flujo de control alterado, control arbitrario de un recurso o ejecución de código arbitrario. Link CWE: https://cwe.mitre.org/data/definitions/20.html Fuente: Elaboración propia TP-LINK WR841N

Figura 12. Búsqueda por TP-LINK WR841N country: ec Fuente: Elaboración propia Hallazgo Tabla 4. Hallazgo de vulnerabilidad TP-LINK WR841N Vulnerabilidad: CVE-2018-11714 Publicado: 2018-06-04 Link: https://www.cvedetails.com/vulnerability-list/vendor_id-11936/product_id-30820/version_id-250264/Tp-link-Tl-wr840n-Firmware-0.9.1-3.16.html Descripción: Se descubrió un problema en TL-WR841N v13 00000013 0.9.1 4.16 v0001.0 Build 170622 Rel.64334n. Este problema se debe a un manejo inadecuado de la sesión en la carpeta / cgi / o en un archivo / cgi. Si un atacante envía un encabezado de Referer: http://192.168.0.1/mainFrame.htm", no se requiere autenticación para ninguna acción. CWE - 384: 1. Una aplicación web autentica a un usuario sin invalidar primero la sesión existente, por lo que continúa utilizando la sesión ya asociada con el usuario. 2. Un atacante puede forzar un identificador de sesión conocido en un usuario para que, una vez que el usuario se autentique, el atacante tenga acceso a la sesión autenticada. 3. La aplicación o el contenedor

utiliza identificadores de sesión predecible. En la explotación genérica de vulnerabilidades de reparación de sesión, un atacante crea una nueva sesión en una aplicación web y registra el identificador de sesión asociado. El atacante luego hace que la víctima se asocie, y posiblemente se autentique, contra el servidor que usa ese identificador de sesión, lo que le da acceso al atacante a la cuenta del usuario a través de la sesión activa. Link: https://cwe.mitre.org/data/definitions/384.html Fuente: Elaboración propia HUAWEI Es una marca que nos trae diferentes tipos de dispositivos: router, switch, Smartphone, tablets, smartwatch, cámaras, etc; en el reporte vimos que nos salía al buscar por huawei pero vimos un modelo en específico que es Huawei Home Gateway es el router que buscamos.

Figura 13. Búsqueda por Huawei Home Gateway country:ec Fuente: Elaboración propia Hallazgo Tabla 5. Hallazgo de vulnerabilidad Huawei HG532 Vulnerabilidad: CVE-2017-17215 Publicado: 2018-03-20 Link: www.cvedetails.com/vulnerability-list/vendor_id-5979/product_id-44511/version_id-241155/year-2018/Huawei-Hg532-Firmware--.html Descripción: Huawei HG532 con algunas versiones personalizadas tiene una vulnerabilidad de ejecución remota de código. Un atacante autenticado podría enviar paquetes maliciosos al puerto 37215 para lanzar ataques. La explotación exitosa podría llevar a la ejecución remota de código arbitrario. CWE - 20: Cuando el software no valida la entrada correctamente, un atacante puede crear la entrada en una forma que el resto de la aplicación no espera. Esto conducirá a que partes del sistema reciban entradas no intencionadas, lo que puede resultar en un flujo de control alterado, control arbitrario de un recurso o ejecución de código arbitrario. Link CWE: https://cwe.mitre.org/data/definitions/20.html Fuente: Elaboración propia D-LINK Es una marca que nos trae diferentes tipos de dispositivos: router, switch, cámaras, etc. Se analizó por D-link-Dir-600 B1.

Figura 14. Búsqueda por D-link-Dir-600 country:ec Fuente: Elaboración propia

Hallazgo Tabla 6. Hallazgo de vulnerabilidad D-link-Dir-600 Vulnerabilidad: CVE-2017-12943 Publicado: 2017-08-18 Link: www.cvedetails.com/vulnerability-list/vendor_id-899/product_id-39542/year-2017/D-link-Dir-600-B1-Firmware.html Descripción: Los dispositivos D-Link DIR-600 Rev Bx con el firmware v2.x permiten a los atacantes remotos leer las contraseñas a través de un modelo / __ show_info.php? REQUIRE_FILE = ataque de recorrido de ruta absoluta, como se demuestra al descubrir la contraseña del administrador. CWE - 22: Muchas operaciones de archivos están destinadas a realizarse dentro de un directorio restringido. Al usar elementos especiales como ".." y "/" separadores, los atacantes pueden escapar fuera de la ubicación restringida para acceder a archivos o directorios que se encuentran en otras partes del sistema. Uno de los elementos especiales más comunes es la secuencia "../", que en la mayoría de los sistemas operativos modernos se interpreta como el directorio principal de la ubicación actual. Esto se conoce como recorrido de la ruta relativa. La trayectoria del camino también cubre el uso de rutas de acceso absolutas como "/ usr / local / bin", que también puede ser útil para acceder a archivos inesperados. Esto se conoce como camino de recorrido absoluto. En muchos lenguajes de programación, la inyección de un byte nulo (el 0 o NUL) puede permitir a un atacante truncar un nombre de archivo generado para ampliar el alcance del ataque. Por ejemplo, el software puede agregar ".txt" a cualquier ruta de acceso, lo que limita al atacante a archivos de texto, pero una inyección nula puede

eliminar esta restricción. Link CWE: https://cwe.mitre.org/data/definitions/22.html Fuente: Elaboración propia

CAMARAS Las cámaras IP son las que se utilizan para la seguridad tanto en el hogar como en compañías. Se realizo la busqueda por router y mostro 318 dispositivos y el top de dichos dispositivos eran los siguientes:

Figura 15. Búsqueda por Camera country:ec Fuente: Elaboración propia

Tabla 7. Top Productos y Ciudades de Cámara TOP PRODUCTOS TOP CIUDADES NETWAY IP 149 Quito 100 Avtech 30 Guayaquil 46 D-Link DCS-5300 1 Cuenca 29 Axis P5635-E PTZ 1 Manta 4 Fuente: Elaboración propia

AVTECH-AVN801-DVR Hallazgo Tabla 8. Hallazgo de vulnerabilidad de Avtech-Avn801-Dvr Vulnerabilidad: CVE-2013-4981 Publicado: 2014-03-03 Link: https://www.cvedetails.com/vulnerability-list/vendor_id-8500/product_id-27162/version_id-161176/Avtech-Avn801-Dvr-Firmware-1017-1003-1009-1003.html Descripción: Desbordamiento de búfer en cgi-bin / user / Config.cgi en AVTECH AVN801 DVR con firmware 1017-1003-1009-1003 y anteriores, y posiblemente otros dispositivos, permite que los atacantes remotos provoquen una denegación de servicio (fallo del dispositivo) y posiblemente ejecuten arbitrariamente código a través de una cadena larga en el parámetro Network.SMTP.Receivers. CWE - 119: Ciertos idiomas permiten el direccionamiento directo de las ubicaciones de memoria y no garantizan automáticamente que estas ubicaciones sean válidas para el búfer de memoria al que se hace referencia. Esto puede hacer que las operaciones de lectura o escritura se realicen en ubicaciones de memoria que pueden estar asociadas con otras variables, estructuras de datos o datos internos del programa. Como resultado, un atacante puede ejecutar código arbitrario, alterar el flujo de control deseado, leer información confidencial o causar que el sistema se bloquee. Link CWE: https://cwe.mitre.org/data/definitions/119.html Fuente: Elaboración propia D-Link DCS-5300 Hallazgo Tabla 9. Hallazgo de vulnerabilidad de Dlink-Dcs-5300 Vulnerabilidad: CVE-2012-5319 Publicado: 2012-10-08 Link: https://www.cvedetails.com/vulnerability-list/vendor_id-9740/product_id-23387/Dlink-Dcs-5300.html Descripción: Vulnerabilidad de falsificación de solicitud entre sitios (CSRF) en setup / security.cgi en D-Link DCS-900, DCS-2000 y DCS-5300 permite a atacantes remotos secuestrar la autenticación de administradores para solicitudes que cambian la contraseña del administrador a través del rootpass parámetro. CWE - 352:

un atacante podría engañar a un cliente para que realice una solicitud no intencional al servidor web, que se tratará

> como Una solicitud auténtica. Esto puede hacerse a través de una URL, carga de imagen, XMLHttpRequest, etc. y puede resultar en la exposición de datos o la ejecución de código no

deseado. Link CWE: https://cwe.mitre.org/data/definitions/352.html Fuente: Elaboración propia

CAPÍTULO 5

CONCLUSIONES

Se observó que en el Ecuador existen miles de dispositivos conectados a internet pero en Shodan en muchos casos no presentan cuál es su marca o su modelo, luego se continuó la investigación viendo el top de productos y fue más sencillo encontrar las vulnerabilidades de los equipos.

Se visualizó varios equipos que presentan vulnerabilidad de años anteriores como 2002 en adelante hasta la actualidad y dichos dispositivos muchas veces presentan más de una vulnerabilidad, la investigación se realizó por la última vulnerabilidad encontrada es así como se puede observar que la mayoría muchos permiten a atacantes remotos secuestrar la autenticación de administradores para solicitudes que cambian la contraseña del administrador, que provoquen una denegación de servicio (fallo del dispositivo), leer las contraseñas, acceder con usuario y contraseña por default, entre otras.

Siempre el comprador debe buscar en la red si no hay alguna actualización de firmware ya que los fabricantes al observar algún tipo de vulnerabilidad tratan de corregirlo inmediatamente pero es él es quien tiene la responsabilidad de actualizar su dispositivo.

En un artículo consultado menciona que muchas ocasiones que el usuario por ahorrar dinero compra equipos “baratos” pero estos muchas veces son los que más tipos de inseguridades pueden presentar al momento de salvaguardar los datos.

Ahora con estas herramientas se puede conseguir toda esta información que es útil para la seguridad de los datos que se proporcionan en internet pero no tan solo se lo puede utilizar para esto sino que personas malintencionadas lo pueden utilizar para poder acceder a la información en el caso de no tener las debidas medidas de seguridad.

Como recomendación se tiene que concientizar al usuario con respecto a la seguridad de los equipos hacia el internet y poder capacitarlo en configuraciones básicas debido a los múltiples ataques por la filtración de información los ataques suelen pasar más en corporaciones pero eso no quiere decir que al usuario del hogar también le pueda suceder.

, 15

Hit and source - focused comparison, Side by Side:

Left side: As student entered the text in the submitted document.
Right side: As the text appears in the source.

Instances from: hromerom_M1.830_20171_PEC4 - Memoria final_8217517.txt

2	100%	2: hromerom_M1.830_20171_PEC4 - Memoria final_8217517.txt 100%
Cuando un servidor web está diseñado para recibir una solicitud de un cliente sin ningún mecanismo para verificar que se envió intencionalmente, entonces		The source document can not be shown. The most likely reason is that the submitter has opted to exempt the document as a source in Urkund's Archive.

3	76%	3: hromerom_M1.830_20171_PEC4 - Memoria final_8217517.txt 76%
como Una solicitud auténtica. Esto puede hacerse a través de una URL, carga de imagen, XMLHttpRequest, etc. y puede resultar en la exposición de datos o la ejecución de código no		The source document can not be shown. The most likely reason is that the submitter has opted to exempt the document as a source in Urkund's Archive.

Instances from: http://www.cvedetails.com/vulnerability-list/vendor_id-11936/product_id-41377/version_id-229259/Tp-link-Tl-wr741n-Firmware-3.11.7.html

1	73%
TP-LINK TL-WR741N / TL-WR741ND 150M Wireless Lite N Router con versión de firmware 3.11.7 Build 100603 Rel.56412n y versión de hardware: WR741N v1 / v2 00000000,	

1: http://www.cvedetails.com/vulnerability-list/vendor_id-11936/product_id-41377/version_id-229259/Tp-link-Tl-wr741n-Firmware-3.11.7.html	73%
TP-LINK TL-WR741N / TL-WR741ND 150M Wireless Lite N Router with Firmware Version 3.11.7 Build 100603 Rel.56412n and Hardware Version: WR741N v1/v2 00000000,	