Universidad de Buenos Aires

Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Internet de las cosas desde una perspectiva de Ciberseguridad

Autor: Esp. Ing. Jorge Ismael Campoverde Armijos
Tutor del Trabajo Final: Dr. Pedro Hecht

Año de presentación: 2019

Cohorte del cursante: 2018

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales de Maestría vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Jorge Ismael Campoverde Armijos
Nro. Documento 1104527278
DNI (Argentina): 95699339

Resumen

El presente Trabajo Final de Maestría se enfoca en un estudio desde una perspectiva de Ciberseguridad sobre una de las tecnologías informáticas que se encuentra en auge como es el internet de las cosas.

El estado actual de la Ciberseguridad con respecto de la tecnología IoT es bastante precario y eso no es un secreto para nadie, debido a múltiples problemas, ya sea por de falta de jurisdicción y regulaciones a las compañías que crean los dispositivos de esta tecnología, y una falta importante de estandarización, que dificultad llevar un control y vigilancia efectivo de los billones de dispositivos.[1]

De acuerdo con cifras de la consultora Frost & Sullivan, en el mercado latinoamericano existen aproximadamente 313 millones de dispositivos IoT conectados y para el 2023 estiman que crecerá rápidamente hasta los 995 millones de dispositivos , si el mercado llega a esa cifra en el 2023, representará un crecimiento anual del 26,7% entre el 2017 y el 2023 de acuerdo al Gerente de Investigación ICT para América Latina.[2]

La primera parte del trabajo consiste en una introducción acerca de los ambientes y dispositivos que se usan en la tecnología del internet de las cosas desde un punto de vista de ciberseguridad y la relevancia de la tecnología IoT como objetivo de posibles amenazas que comprometan la privacidad de los usuarios y organizaciones que hacen uso de la misma , lo cual permite tener una visión holística de la utilización de IoT para la ejecución de Ciberataques y saber cómo evitarlos.

La segunda parte de este trabajo, se fundamenta en el desarrollo de 4 casos de estudio, a través de los cuales se describe los diferentes vectores de ataques que se pueden realizar a dispositivos IoT basados en la Metodología OWASP 2017[3]; los casos prácticos están enfocado en la explotación de diferentes tipos de vulnerabilidades que existen en un ambiente de IoT, demostrando así como se puede obtener acceso a información sensible que está expuesta a internet.

El objetivo final del presente trabajo final de maestría radica en el estudio de los principales vectores de ataque a los que son vulnerables los dispositivos de IoT y los mecanismos de seguridad que se deben considerar

para la implementación de medidas de seguridad ´para prevenir y mitigar los riesgos a los que están expuestos los dispositivos de IoT.

El alcance de este trabajo comprenderá la investigación de los componentes que conformar la tecnología del IoT, cuáles son los estándares y protocolos de comunicación , y la elaboración de 4 casos de estudio a través de los cuales se puedan analizar los diferentes vectores de ataque que existen en un ambiente de IoT y de esta manera brindar recomendaciones para la mitigación de estas vulnerabilidades y saber el estado de madurez de los dispositivos con respecto a la ciberseguridad según la metodología OWASP 2017.

Palabras clave: Internet de las cosas, Ciberseguridad, Ciber terroristas, Vectores Ataque, Botnets

INDICE GENERAL

DECLARACIÓN JURADA DE ORIGEN DE LOS CONTENIDOS I
RESUMEN II
INDICE GENERAL IV
ÍNDICE DE FIGURAS VI
ÍNDICE DE TABLAS VIII
AGRADECIMIENTO IX
INTRODUCCIÓN 1
CAPITULO I: INTERNET DE LAS COSAS: DEFINICIÓN 4
1.1 ANTECEDENTES 4
1.2 DEFINICIÓN 4
1.3 ARQUITECTURA 6
1.3.1 Definición ..... ¡Error! Marcador no definido.
1.3.2 Desafíos de seguridad a la arquitectura de IoT **9**
1.4 COMPONENTES PARA LA IMPLEMENTACIÓN DE IOT 14
1.4.1 Sensores **14**
1.4.2 Redes **15**
1.4.3 Análisis inteligente **15**
1.4.4 Acciones inteligentes **16**
CAPITULO 2: ESTÁNDARES Y PROTOCOLOS DE COMUNICACIÓN ... 17
2.1 INTRODUCCIÓN 17
2.1.1 Plataforma **18**
2.1.2 Conectividad: **18**
2.1.3 Modelo de negocio: **18**
2.1.4 Aplicaciones determinantes: **19**
2.2 PROTOCOLOS DE COMUNICACIÓN 19
2.2.2 Entorno Industrial: **20**
2.2.3 Protocolo de enlace de datos de IoT **22**
2.2.4 Protocolos en la capa de Red y Encapsulamiento **24**
2.2.5 Protocolos en la capa de Sesión **25**
2.2.5 Protocolos en la capa de Aplicación **26**
CAPITULO 3: CIBERSEGURIDAD 27
3.1 DEFINICIÓN 27
3.2 RETOS DE LA CIBERSEGURIDAD EN IOT 27

3.2.1 Fin de la autenticación de doble factor. 29
3.2.2 Ransomware y minado de monedas a través de Cryptohacking 30
3.2.3 Internet de las Cosas, en la mira de los ciberdelincuentes. 32
3.2.4 Machine Learning y Big Data 34
3.2.5 Casas Inteligentes 35
3.2.6 Botnets 37

CAPITULO 4: CASOS DE ESTUDIO: VECTORES DE ATAQUE A DISPOSITIVOS IOT 41

4.1 SHODAN COMO VECTOR DE ATAQUE 41
4.2 CONSIDERACIONES DE SEGURIDAD EN DISPOSITIVOS IOT 42
4.2.1 CASO DE ESTUDIO #1: ATAQUE A ROUTERS 46
4.2.1.1 Ataques de fuerza bruta 46
4.2.1.2 Explotando vulnerabilidades en routers remotos 55
4.2.2 CASO DE ESTUDIO #2: ATACANDO EQUIPOS DE LA RED INTERNA DE UNA ORGANIZACIÓN 61
4..2.2.1 Explotando versiones vulnerables de servicios 61
4.2.3 CASO DE ESTUDIO #3: ATACANDO CONTROLADORES DE ACCESO VERTX 68
4.2.4 CASO DE ESTUDIO #4: CRIPTOMINING CON BOTNETS. 72

CONCLUSIONES 81
BIBLIOGRAFÍA 82

Índice de Figuras

Figura 1. El paradigma del internet de las cosas, como resultado de la convergencia de diferentes visiones. [13] 6

Figura 2. Arquitectura general de IoT [14] 6

Figura 3. Arquitectura básica del IoT[15] 7

Figura 4. Arquitectura estándar de comunicaciones IoT [12] 8

Figura 5. Modelo de referencia IoT [18] 9

Figura 6. Componentes de IoT [20] 14

Figura 7 . Ambiente Heterogéneo de Estándares de IoT [25] 17

Figura 8. Protocolos en Entorno Doméstico[28] 19

Figura 9. Entorno Industrial[29] 20

Figura 10. Modelo de referencia de alto nivel de un entorno industrial [30] 22

Figura 11 WirelessHart Arquitectura [31] 23

Figura 12 . Arquitectura MQTT [31] 25

Figura 13 Arquitectura AMQP [31] 26

Figura 14. Empresas que piensan que es necesario variar el presupuesto de Ciberseguridad para los próximos tres años [35] 29

Figura 15. Esquema de Doble Factor de Autentificación. [37] 30

Figura 16. Ejemplo de un Ransomware [38] 31

Figura 17. Estadística del robo de Criptomonedas [38]. 31

Figura 18. IoT y Ciberseguridad [39] 32

Figura 19. Estadística de dispositivos conectados hasta el 2025 [39] 33

Figura 20. Botnets [45] 37

Figura 21. Ciclo de vida de una botnet [46] 39

Figura 22. Riesgos de Seguridad , Owasp 2017 [3] 43

Figura 23. Metodología CEH [50] 47

Figura 24. Resultado de la búsqueda del modelo del router en Shodan 47

Figura 25. Panel de Login del Router 48

Figura 26. Descubriendo Usuario y Password del router 49

Figura 27. Credenciales Obtenidas Inválidas 49

Figura 28. Ataque de fuerza bruta con un diccionario diferente 50

Figura 29. Credenciales Obtenidas Inválidas 50

Figura 30. Resultado de la ejecución del comando 51

Figura 31. Resultado de la ejecución del comando 51

Figura 32. Servicio de Telnet Ejecutándose 52

Figura 33. Credenciales obtenidas a través de fuerza bruta 52

Figura 34. Acceso correcto al router a través de telnet 53

Figura 35. Archivos del router 53

FIGURA 36. EJECUCIÓN DEL FRAMEWORK ROUTERSPLOIT 56
FIGURA 37. VULNERABILIDADES ENCONTRADAS EN EL ROUTER 57
FIGURA 38. EJECUCIÓN EXITOSA DEL XPLOIT Y OBTENCIÓN DE LA CONTRASEÑA 58
FIGURA 39. CONSOLA DE ADMINISTRACIÓN DEL ROUTER 59
FIGURA 40. DISPOSITIVOS ENCONTRADOS EN LA RED Y LOS SERVICIOS QUE ESTÁN EJECUTANDO 62
FIGURA 41. CONFIGURACIÓN DE PARÁMETROS NECESARIOS PARA LA EJECUCIÓN DEL EXPLOIT 63
FIGURA 42. EJECUCIÓN DEL LISTENER PARA LA CREACIÓN DE LA SHELL INTERACTIVA 64
FIGURA 43. VERIFICACIÓN DE PRIVILEGIOS EN LA SHELL OBTENIDA. 64
FIGURA 44. SISTEMA DE ARCHIVOS DE LA MÁQUINA COMPROMETIDA 65
FIGURA 45. DESCUBRIENDO INFORMACIÓN CONFIDENCIAL EN LA MÁQUINA VULNERADA 65
FIGURA 46. INGRESO AL PANEL DE SENSORES, A TRAVÉS DE LAS CREDENCIALES OBTENIDAS 66
FIGURA 47. RESULTADOS DE LA EJECUCIÓN DE EYESHODAN 69
FIGURA 48. CONFIGURACIONES DE RED DEL CONTROLADOR 70
FIGURA 49 , PANEL DE SERVICIOS 70
FIGURA 50. DESCURBIENDO SERVICIOS ACTIVOS EN EL DISPOSITIVO 71
FIGURA 51 CONEXIÓN POR SSH A EL CONTROLADO HID 71
FIGURA 52 . CLONADO DEL REPOSITORIO DE LA BOTNET EN EL SERVIDOR LINUX 73
FIGURA 53 INSTALACIÓN DE LOS REQUERIMIENTOS PARA LA BOTNET 74
FIGURA 54. ARRANCANDO EL SERVIDOR DE LA BOTNET 74
FIGURA 55. OPCIONES DE LA BOTNET CON LOS DISPOSITIVOS INFECTADOS 75
FIGURA 56 EJECUCIÓN DEL CLIENTE Y CREACIÓN DEL PAYLOAD PRUEBATESIS.PY 75
FIGURA 57 ARCHIVO PRUEBATESIS.PY 76
FIGURA. 58 EJECUCIÓN DEL ARCHIVO PRUEBATESIS.PY EN LA MÁQUINA WINDOWS 77
FIGURA 59 SESIÓN OBTENIDA EN LA BOTNET 77
FIGURA 60 . SHELL REVERSA DE LA MÁQUINA INFECTADA EN LA BOTNET 78
FIGURA 61 DATOS DE CONEXIÓN DE MINERGATE 79
FIGURA 62. MÁQUINA INFECTADA MINANDO EN SEGUNDO PLANO 79
FIGURA 63 RENTABILIDAD DE MONERO 80

Índice de tablas

TABLA 2 PROTOCOLOS DE COMUNICACIÓN 20
TABLA 4. FILTROS DE SHODAN[49] 42
TABLA 5. VECTORES DE ATAQUE SEGÚN OWASP 2017 [3] 45
TABLA 6. VECTOR DE ATAQUE A2:2017 BROKEN AUTHENTICACION [3] 55
TABLA 7 MEDIDAS DE PREVENCIÓN Y MITIGACIÓN[3] 60
TABLA 8 VECTOR DE ATAQUE A9:2017 USING COMPONENTES WITH KNOWN VULNERABILITIES[3] 67

Agradecimiento

Esta tesis está dedicada a mi padre, quien me enseñó que el mejor conocimiento que se puede tener es el que se aprende por sí mismo. También está dedicado a mi madre, quien me enseñó que incluso la tarea más grande se puede lograr si se hace un paso a la vez.

Introducción

El Internet de las cosas de aquí en adelante (IoT), es un paradigma novedoso que está ganando terreno rápidamente en el escenario de las modernas telecomunicaciones inalámbricas. La idea básica de este concepto es la presencia generalizada que nos rodea de una variedad de cosas u objetos, como etiquetas de identificación por radiofrecuencia (RFID), sensores, actuadores, teléfonos móviles, etc, que a través de esquemas de direccionamiento únicos, son capaces de interactuar entre sí y cooperar con sus vecinos para alcanzar objetivos comunes [4].

En el año de 1988, Mark Weiser acuñó la frase "computación ubicua", que se conoce como un concepto donde la informática está disponible en cualquier lugar y en cualquier tiempo, el término “Internet of Things" fue acuñado por primera vez por Kevin Aston en 1999 [5].

El estado actual de la Ciberseguridad con respecto de la tecnología IoT es bastante precario y eso no es un secreto para nadie, debido a múltiples problemas, ya sea por de falta de jurisdicción y regulaciones a las compañías que crean los dispositivos de esta tecnología, además de una falta importante de estandarización, lo que dificulta llevar un control y vigilancia efectivo de los billones de dispositivos. [6]

Conectar cualquier objeto a Internet y con ello crear infinidad de nuevas aplicaciones ha levantado grandes expectativas, 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. [7] La Idea esencial de IoT consiste en utilizar sensores y controles de distintos objetos y diferentes plataformas ,para reunir y analizar los datos sobre el ambiente que se está trabajando [8] , es así que el número de dispositivos IoT se encuentra en constante crecimiento, por la razón de que estos dispositivos son usados en prácticamente cualquier área de negocio, es así que al existir ambientes de TI[1] cada vez más complejos y con una enorme cantidad de eventos generados, es una necesidad primordial encontrar una solución a través de la cual se pueda

[1] Tecnologías de la Información

asegurar estos equipos para que no puedan ser vulnerados por ciber terroristas.

El gran poder de Internet de las cosas viene con la gran responsabilidad de la seguridad, siendo la tecnología más novedosa, los desarrollos e innovaciones se están produciendo a una gran velocidad, pero la seguridad de IoT aún está por ponerse al día ya que se ha venido creando nuevos dispositivos pero no dándoles la seguridad que les corresponde, por lo tanto las repercusiones de seguridad son graves y en ocasiones amenazan la vida (autos inteligentes), es por esta razón que no hay forma de que las empresas que desarrollan estos dispositivos puedan darse el lujo de descuidar la seguridad de sus productos.

El objetivo general del presente trabajo es establecer mecanismos de seguridad que se deben considerar para la implementación IoT en una organización y estudiar los diferentes vectores de ataque a los que son vulnerables estos dispositivos.

El alcance de este trabajo comprenderá la investigación de los componentes que conformar la tecnología del IoT, cuáles son los estándares y protocolos de comunicación , y la elaboración de 4 casos de estudio a través de los cuales se puedan analizar los diferentes vectores de ataque que existen en un ambiente de IoT y de esta manera brindar recomendaciones para la mitigación de estas vulnerabilidades y saber el estado de madurez de los dispositivos con respecto a la Ciberseguridad según la metodología OWASP 2017.

La primera parte de este trabajo está conformada por el capítulo los tres primeros capítulos y consiste en una introducción acerca de los ambientes y dispositivos que se usan en la tecnología del internet de las cosas desde un punto de vista de ciberseguridad y la relevancia de la tecnología IoT como objetivo de posibles amenazas que comprometan la privacidad de los usuarios y organizaciones que hacen uso de la misma , lo cual permite tener una visión holística de la utilización de IoT para la ejecución de Ciberataques y saber cómo evitarlos.

La segunda parte de este trabajo, consiste en el desarrollo de 4 casos de estudio, a través de los cuales se describe los diferentes vectores de ataques que se pueden realizar a dispositivos IoT basados en la Metodología OWASP 2017[3]; los casos prácticos están enfocado en la explotación de diferentes tipos de vulnerabilidades que existen en un ambiente de IoT, demostrando así como se puede obtener acceso a información sensible que está expuesta a internet.

La hipótesis planteada en este estudio, es verificar que existen las medidas adecuadas de seguridad en los dispositivos de IoT que están expuestos a internet , para así asegurar la confidencialidad e integridad de la información.

CAPITULO I: Internet de las Cosas: Definición

1.1 Antecedentes

Para hablar acerca del Internet de las Cosas nos tenemos que remontar al año 1927, cuando Nikola Tesla conformó la base de las comunicaciones inalámbricas y de radio, pero la primera conexión entre computadoras se realizó en el año 1969 con la red ARPANET, que fue creada por el departamento de Defensa de Estados Unidos y esta fue la red que fue interconectado computadoras y creando nuevas redes.

En el año 1979 se implantó el protocolo TCP/IP y Tim Berners-Le en 1990 implemento con éxito la primera comunicación entre un cliente HTTP y un servidor de internet [9]. El uso del protocolo IP para conectar a internet dispositivos que no son computadoras no es una idea del siglo XX, el primer dispositivo fue una tostadora conectada vía IP que se podía encender y apagar a través de internet, esta se presentó en una conferencia sobre internet realizada en el año de 1990. De la misma manera en la Universidad Carnegie Mellon en Estados Unidos conectó una máquina de refresco y una cafetera la misma que estuvo conectada hasta el 2001. Desde una perspectiva amplia, la confluencia de diferentes tendencias tecnológicas y de mercado está permitiendo interconectar dispositivos más pequeños de forma económica y sencilla:[10].

El término IoT fue empleado por primera vez por Kevin Ashton que impartió una conferencia en Procter and Gamble (1999) donde dijo “Necesitamos internet de las cosas, una forma estandarizada para equipos para entender el mundo real.” [9] , Ashton acuñó este término para ilustrar el poder de conectar a Internet las etiquetas de identificación por radio frecuencia (RFID)[2] que se utilizaban en las cadenas de suministro corporativas para contar y realizar un seguimiento de las mercancías sin necesidad de la intervención humana[10].

1.2 Definición

Según la definición de Gardner , el internet de las cosas se relaciona con dispositivos conectados entre sí a través de diferentes métodos y canales de comunicación , estos dispositivos son capaces de comunicarse y transmitir

[2] Identificación de Radio Frecuencia

datos entre sí , las rutas de comunicación y transmisión varían según el dispositivo de IoT y su propósito.[11].

El internet de las cosas se basa en la infraestructura de la iniciativa de normas globales (IoT – GSI[3]) de la unión internacional de telecomunicaciones , esta infraestructura abarca dispositivos como computadoras de escritorio , laptops, tabletas y teléfonos inteligentes conectados a través de múltiples protocolos de comunicación como bluetooh , Zigbee (protocolo de comunicación inalámbrico) ,LoRawAN (red de área amplia de gran alcance) y SIGFOX.[12].

Sin lugar a dudas, la principal fortaleza de la idea de IoT es el gran impacto que tendrá en varios aspectos de la vida cotidiana y el comportamiento de los usuarios potenciales.

Desde el punto de vista de un usuario privado, los efectos más evidentes de la introducción de IoT serán visibles tanto en el ámbito laboral como en el doméstico, en este contexto, la domótica, la vida asistida, la salud electrónica, el aprendizaje mejorado, son solo algunos ejemplos de los posibles escenarios de aplicación. Se debe tener en cuenta que IoT es más que simplemente agregar sensores, se trata de crear dispositivos y sistemas inteligentes, para lo cual se desarrollaron tres visiones principales:

- **Visión orientada a las cosas:** El enfoque está en los dispositivos físicos que se conectan a la red y sus sensores.
- **Visión orientada a internet:** El enfoque está en el protocolo que se será utilizado para conectar todos estos dispositivos, por ejemplo, el protocolo de internet.
- **Visión orientada a semántica:** Esta es la más abstracta de las tres visiones , se centra en la cantidad de dispositivos o tipos de dispositivos que se encuentran interconectados , y buscar la manera de almacenar y direccionar las comunicaciones de estos dispositivos.[13]

La figura 1 tomada del artículo “El internet de las cosas: encuesta”, nos muestra estas tres perspectivas y los componentes de cada una en detalle.

[3] Iniciativa de Estándares Globales

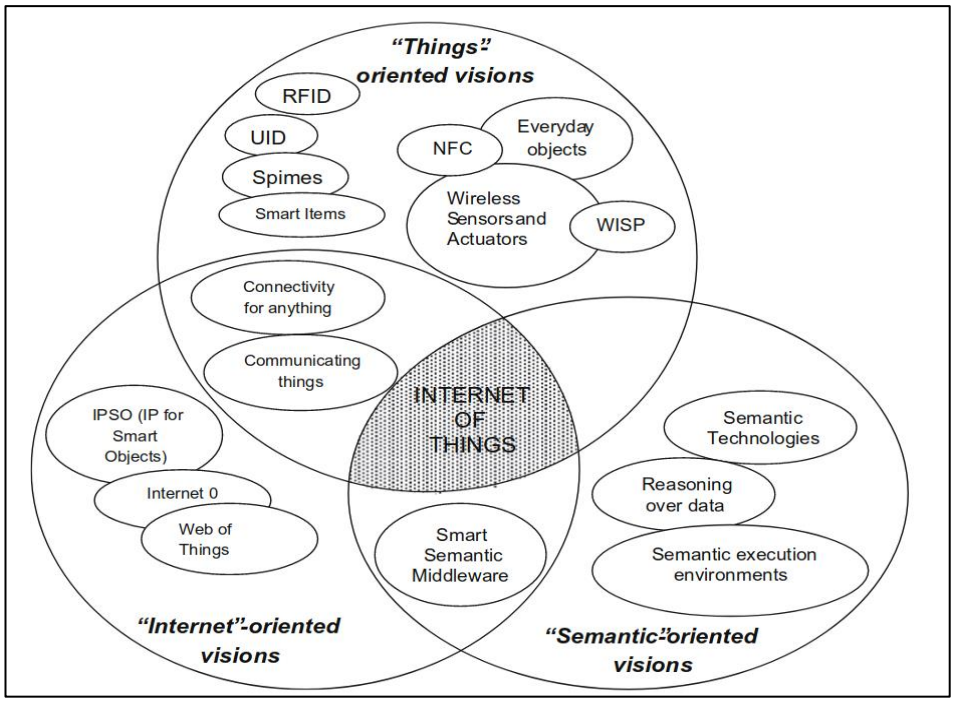


Figura 1. El paradigma del internet de las cosas, como resultado de la convergencia de diferentes visiones. [13]

1.3 Arquitectura

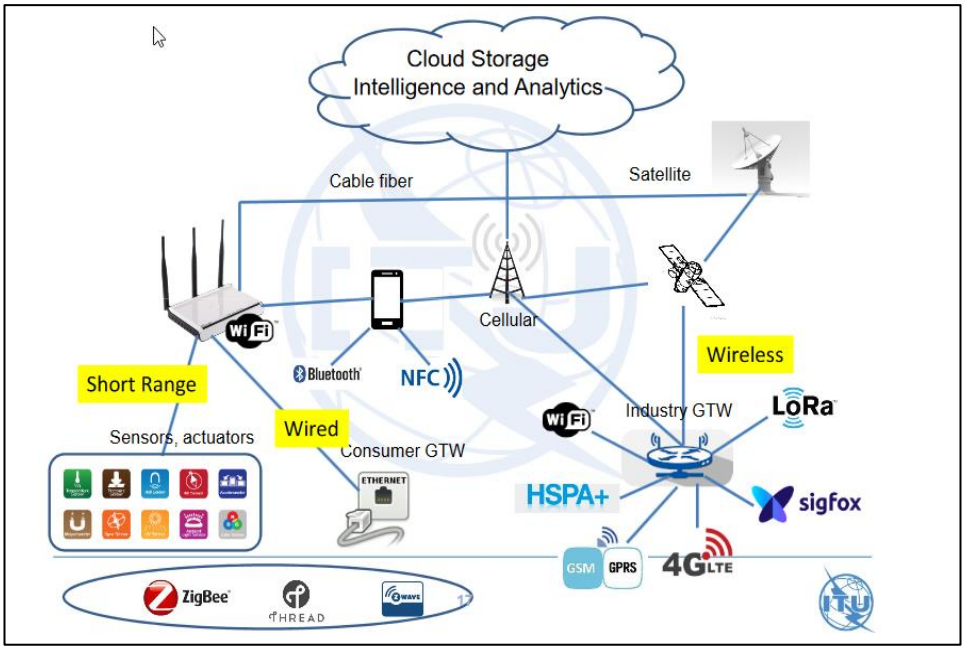


Figura 2. Arquitectura general de Iot [14]

La arquitectura de ordenadores se refiere a toda una estructura y a los detalles necesarios para que sea funcional, es decir, cubre sistemas informáticos, microprocesadores, circuitos y programas del sistema. En el contexto de IoT

se describe cómo los componentes físicos recogen los datos, los procesan e intercambian, y el formato en que lo hacen.

Por lo General se describen las arquitecturas atendiendo a diferentes capas, cada una de las cuales tiene su función específica, y dispone de sus propios protocolos que se definen como los lenguajes a través de los cuales se comunican los diferentes componentes.

La arquitectura básica de IoT se encuentra dividida en 5 capas como se muestra en la figura 3

Figura 3. Arquitectura básica del IoT[15]

- Capa de Negocio: En esta capa se resuelven todos los problemas de más alto nivel de abstracción, como los modelos de negocio, la privacidad de los datos de usuario, y se gestionan las aplicaciones y en general todo el modelo IoT.
- Capa de aplicación: La función de la capa de aplicación es el desarrollo de todo tipo de aplicaciones en función del objetivo que tenga y de los datos recogidos por la capa de percepción.
- Capa de procesamiento: Esta capa es la responsable de recoger las propiedades físicas de los objetos (temperatura, humedad, localización, etc) mediante sensores y convertir la información en señales digitales para poder transmitirlas por la red.
- Capa de red: Esta capa tiene como función principal enviar los datos recogidos por la capa de percepción hacia su destino mediante la red a través de 3G, 4G, Wifi, Bluetooth, ZigBee u otras tecnologías.

- Capa de Percepción: En esta capa se encuadran los diferentes sensores encargados de recoger información del entorno. Aquí se identifican otros dispositivos inteligentes del entorno. [16][15].

La base de la arquitectura en los dispositivos de IoT está fundamentada en poder distribuir objetos y dispositivos conectados por todo el entorno, esto implica que la información adquirida pueda provenir de diferentes lugares y a su vez, procesada por máquinas o servidores diferentes.

Uno de los grandes problemas que nos encontramos al intentar conectar diferentes tipos de dispositivos, es la estandarización de protocolos de comunicación, ya que cada fabricante aplica su propia tecnología lo que implica que muchas veces los dispositivos no puedan comunicarse entre ellos, en IoT el intercambio de datos debe ser entre cualquier objeto de manera bidireccional. [17]

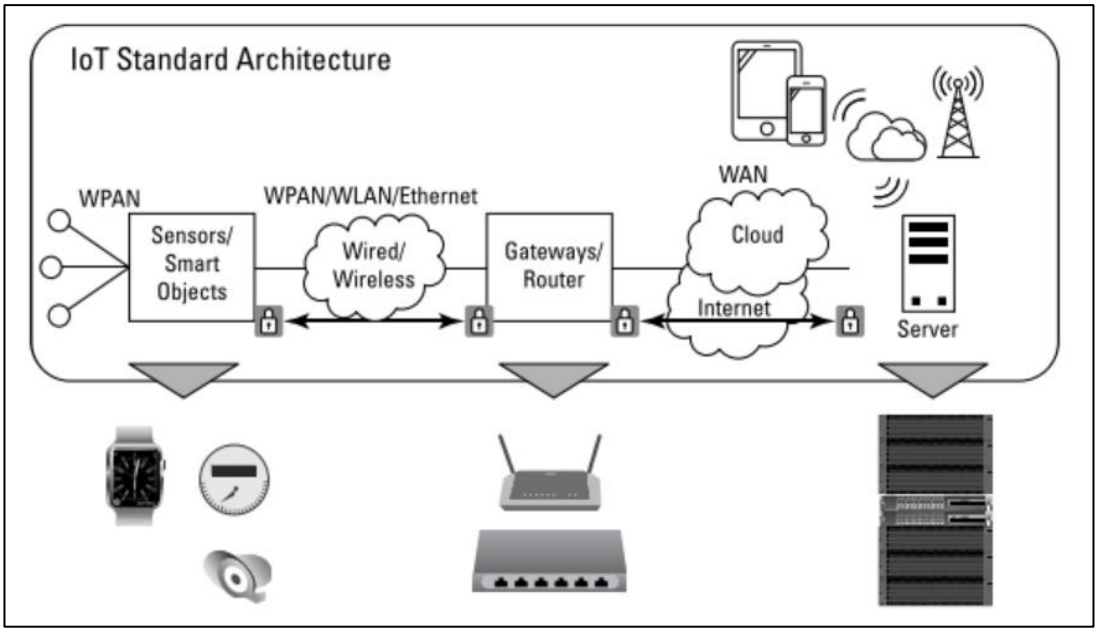


Figura 4. Arquitectura estándar de comunicaciones IoT [12]

La figura 3 ilustra una arquitectura de comunicaciones que consta de sensores objetos inteligentes, dispositivos inteligentes, Gateway, centro de datos y servicios de BackEnd.

- Sensores: Son los encargados de recibir y enviar datos.
- Objetos Inteligentes: Son dispositivos capaces de trabajar por sí solos, sin depender de la manipulación constante del ser humano.

- Wireless: Es el término usado para describir las telecomunicaciones en las cuales las ondas electromagnéticas llevan la señal sobre parte o toda la trayectoria de la comunicación entre dispositivos.
- Cloud: La computación en la nube hace que los recursos del sistema informático, especialmente el almacenamiento y la potencia de cómputo, estén disponibles sin la administración activa directa del usuario.

1.3.2 Desafíos de seguridad a la arquitectura de IoT

Cuando se piensa en el entorno de Internet de las cosas, la protección contra amenazas y vulnerabilidades externas debe considerarse tan importante como en un entorno normal de TIC. La razón de esto es la gran cantidad de dispositivos y entornos de IoT que podrían usarse para construir las redes de bot o para cualquier otra actividad hostil. [11]. Es por esto que antes de revisar los desafíos seguridad de IoT, se debe analizar cómo se encuentra está formado un modelo de referencia de IoT, el cual se muestra en la figura 5

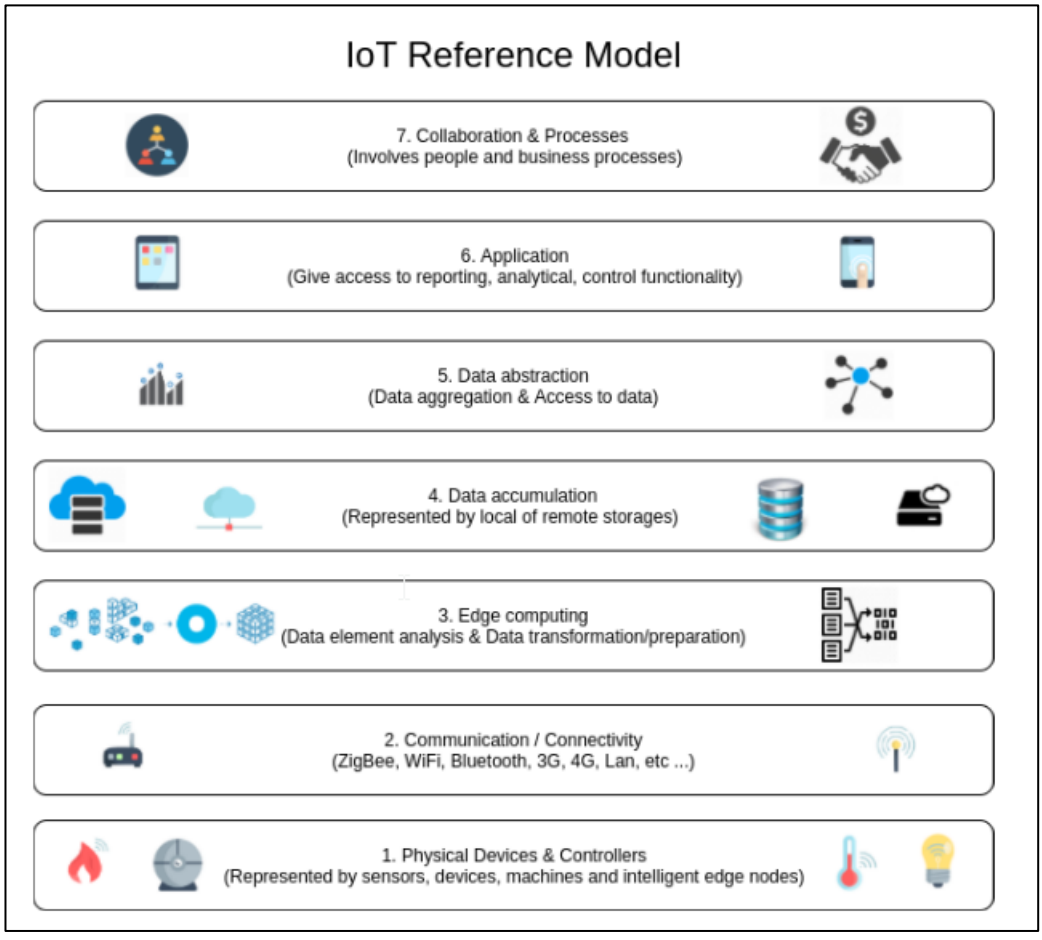


Figura 5. Modelo de referencia IoT [18]

Para aprovechar al máximo los beneficios de IoT, es necesario tener en cuenta los diferentes vectores de ataque a los cuales es susceptible este modelo de referencia teniendo en cuenta cada una de las capas del mismo.

Ataques externos

Uno de los principales problemas que hay que abordar en lo que corresponde a riesgos de seguridad de IoT, es el almacenamiento de los datos en la nube, aquí la principal preocupación es la confianza del proveedor de servicios en la nube, ya que ahí se almacenan todos los datos enviados por los sensores o dispositivos inteligentes. Las organizaciones descargan deliberadamente datos sensibles para obtener los servicios, pero desconocen la ubicación donde se procesarán sus datos o donde son almacenados, hasta inclusive existe la preocupación de que esos datos puedan ser vendidos por terceros sin el consentimiento de la organización.

Ataques de agujero de gusano

El ataque de agujero de gusano es muy popular en redes ad hoc[4], IoT conecta objetos estacionarios y objetos dinámicos, que van desde relojes de pulsera y refrigeradores hasta vehículos, el enlace que une estos objetos también es heterogéneo el cual puede ser cableado o inalámbrico. Este tipo de ataque en especial es muy difícil de detectar ya que el atacante cambia el nodo al que llegan los datos por otro y los reenvía al nodo que el administra.

Ataque selectivo de reenvío

Los nodos maliciosos eligen los paquetes y los descartan; es decir, selectivamente filtrar ciertos paquetes y permiten el resto. Los paquetes descartados pueden llevar necesarios datos sensibles para su posterior procesamiento.

Ataque de bruja

El nodo malicioso aprovecha la falla de un nodo legítimo. Cuando el nodo legítimo falla, el enlace real se desvía a través de la red maliciosa para toda su comunicación futura, lo que resulta en pérdida de datos. [19]

[4] Una red inalámbrica ad hoc (WANET) o una red móvil ad hoc (MANET) es un tipo descentralizado de red inalámbrica

Denegación de servicio distribuida (DDoS)

DDoS, un ataque iniciado y continuado por algunos cientos o incluso miles de atacantes, comienza rellenando paquetes de tráfico no deseado con un tamaño enorme para capturar y agotar completamente los recursos de memoria. Un ataque de denegación de servicio DDoS puede abrumar al objetivo al no disponer de recursos, por lo que los usuarios autorizados no pueden acceder a los servicios normales lo que produce una falla de disponibilidad.[19]

1.3.2.1 Desafíos de seguridad en la capa de aplicación

Los mayores riesgos de seguridad en la capa de aplicación pueden ser representados por los siguientes cuatro grupos:

1. **Autenticación:** Permite la integración de diferentes dispositivos IoT de diferentes contextos. Durante el proceso de autenticación, es necesario autenticar a los pares de enrutamiento utilizados para la transferencia o intercambio de datos junto con la autenticación del nodo de datos de origen. En consecuencia, podemos afirmar que la implementación de claves y la gestión de claves son desafíos básicos en la autenticación de IoT. La autenticación de nodos siempre es necesaria para una implementación buena y segura, ya que proporciona prevención contra el acceso ilegal de nodos.
2. **Autorización:** Aborda el problema de seguridad del acceso ilegal a los nodos al especificar los derechos de acceso a desde diferentes recursos. Los datos siempre deben estar protegidos de manera segura y accesibles solo para usuarios autorizados. Como cada nodo IoT admite técnicas limitadas para la verificación de acceso, siempre es un desafío proporcionar un mecanismo de autorización apropiado que sea beneficioso y tolere a los nodos con diferentes capacidades.
3. **Agotamiento de recursos**: Uno de los desafíos resultantes de los ataques, cuyo objetivo es drenar la energía del nodo IoT objetivo a través de bucles de enrutamiento o extendiendo rutas de transferencia de paquetes. Cada nodo puede ser atacado y comprometido físicamente, en consecuencia, puede usarse para realizar actividades maliciosas dentro de la red. Por lo tanto, el desafío principal ocurre cuando uno de los nodos

se ve comprometido y, como resultado, las técnicas criptográficas no son más útiles ya que el atacante tiene acceso a las claves y los esquemas de cifrado a través del nodo comprometido.

4. **Establecimiento de confianza:** Es un aspecto importante de cada sistema IoT porque a menudo manejan datos confidenciales, almacenan, transfieren, procesan de forma recurrente la recuperación y toman decisiones sobre este tipo de datos. Proporcionar un modelo de confianza a nivel de aplicación para seguir las pautas de integridad y confidencialidad de los datos establece un desafío fundamental para la seguridad de los datos confidenciales [18]

1.3.2.2 Desafíos de seguridad en capa de red

La comunicación puede describirse como un proceso de intercambio de datos entre los dispositivos IoT o entre diferentes capas. Con la enorme heterogeneidad de los sistemas IoT por falta de estandarización, toda la infraestructura de comunicación siempre es amplia y vulnerable a la pérdida de privacidad.

Los principales ataques se detallan a continuación:

1. **Meet-in-the-middle (MiTM)[5].** Es una técnica clásica de criptoanálisis que se aplica a muchas construcciones. La idea es que el atacante construya patrones que se propaguen desde ambos extremos hasta la mitad del cifrado, en algunos casos mediante adivinación de clave parcial. Si los eventos no coinciden en el medio, la conjetura de clave fue incorrecta y puede descartarse. Dicho ataque se ha aplicado al DES de 7 y al criptoanálisis estructural de cifrado.
2. **Ataque Sieve-in-the-Middle (SitM)**: Se considera como una versión mejorada del ataque MitM. Se representa SitM como una nueva mejora genérica de los algoritmos MitM, que permite atacar un mayor número de rondas. Proponen calcular los bits de entrada y salida de la casilla S media particular en lugar de buscar colisiones.

[5] Meet-in-the-middle es un ataque conocido que puede reducir exponencialmente la cantidad de permutaciones de fuerza bruta necesarias para descifrar el texto que ha sido cifrado por más de una clave. Tal ataque hace que sea mucho más fácil para un intruso obtener acceso a los datos.

3. Eavesdropping: Consiste en interceptar y registrar la información entre dos nodos interconectados. Siempre ocurre en la capa de red en el IoT y representa una forma de análisis de datos [5]. A pesar de que tal técnica puede ser usada para evitar colisiones y mejorar el rendimiento de los sistemas IoT [18]

1.3.2.3 Desafíos de seguridad en la capa de datos

Si observamos la taxonomía de los sistemas IoT, es muy importante saber cómo respaldar la seguridad y la privacidad de los datos de extremo a extremo. Siempre debemos asegurarnos de la autenticidad, integridad y confidencialidad de los datos recopilados o transferidos a través de dispositivos IoT heterogéneos.

Complejidad en el manejo de datos: Una interacción entre los actores, dispositivos y componentes de los sistemas IoT puede dar como resultado la acumulación de una gran cantidad de datos, que difícilmente se pueden administrar y proteger. En consecuencia, si los datos no pueden controlarse incluso en las etapas de generación y acumulación, no hay opciones para garantizar un control adecuado del flujo de datos en el sistema.

Consentimiento del usuario para envío de datos: En muchos casos, las operaciones de procesamiento de datos podrían estar cubiertas por el usuario, lo que influye en la transparencia de los datos personales para el propietario. Por ejemplo, los dispositivos portátiles como los relojes inteligentes pueden recopilar y distribuir información personal de los usuarios con sensores incorporados, sin la aprobación o consentimiento de los mismos. Es por eso que se debe proporcionar un nuevo mecanismo de consentimiento sobre el uso de estos datos.

Creación de patrones de comportamiento y perfiles

A pesar del hecho de que los datos podrían recopilarse por medio de información aislada y separada, aún podrían analizarse y podrían revelarse aspectos específicos de los hábitos de un individuo. Pero generar ese conocimiento a partir de los datos de los usuarios podría conducir a la extracción de los patrones de vida y comportamiento aún más detallados y completos del usuario. Si el sistema IoT no pudiera garantizar la privacidad

del comportamiento de los usuarios o evitar la detección de patrones ocultos, esto ejercerá presión sobre la privacidad de los usuarios. [18]

1.4 Componentes para la implementación de IoT

Para la implementación de una arquitectura de IoT se debe tener en cuenta varios componentes, lo cual no es un proceso sencillo por muchas razones, incluida la naturaleza compleja de los distintos componentes del ecosistema de IoT. Para comprender la dificultad de este proceso, examinaremos los cinco componentes que se necesitan para la implementación de IoT:

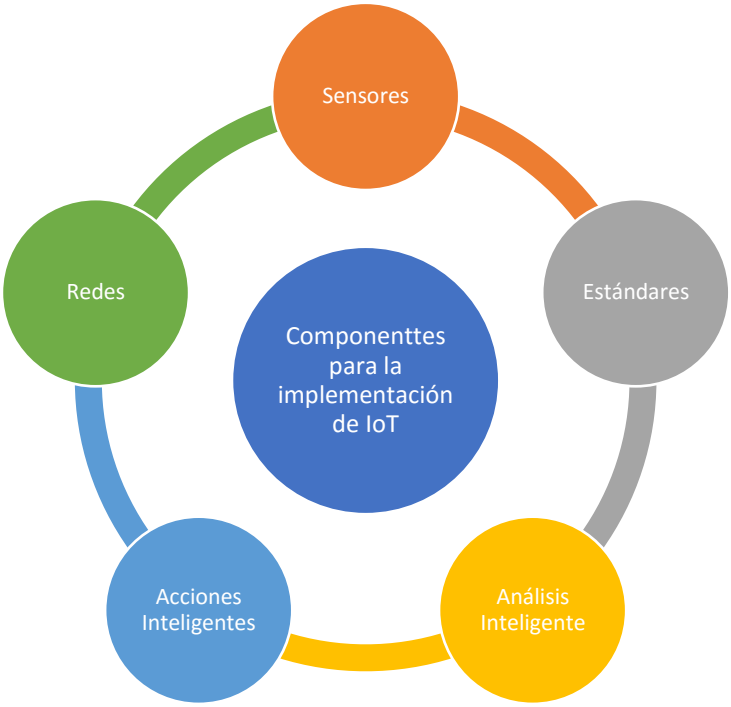


Figura 6. Componentes de Iot [20]

1.4.1 Sensores

El propósito principal de los sensores es recopilar datos medibles de una máquina, dispositivo o entorno ambiental. [11]

Los sensores son uno de los bloques de construcción clave de la Internet de las cosas que se puede implementar en todas partes, desde campos de batalla militares hasta viñedos. Un sensor es un dispositivo electrónico que detecta sentidos o medidas estímulos físicos y responde a ellos de una manera específica. Convierte las señales de los estímulos en una forma analógica o digital, de modo que los datos sin procesar sobre los parámetros detectados puedan ser leídos por máquinas y humanos. Los sensores también se pueden implantar debajo de la piel humana, en un bolso o en un

vestido. Algunos pueden tener un tamaño tan pequeño como cuatro milímetros, pero los datos que recopilan se pueden recibir a cientos de kilómetros de distancia. Los sensores complementan los sentidos humanos y se han convertido en indispensables en una gran cantidad de industrias, desde el cuidado de la salud hasta la construcción, los sensores tienen la ventaja clave de que pueden anticipar las necesidades humanas en función de la información recopilada sobre su contexto. [21]

1.4.2 Redes

El segundo componente para la implementación de IoT es la transmisión de las señales recogidas por los sensores a través de redes a los diferentes elementos de una red típica, como routers y hubs en distintas topologías. Cuando se habla de dispositivos IoT, existen básicamente dos opciones diferentes disponibles, red cableada con conexiones de cobre o fibra y conexiones inalámbricas con diferentes tipos de métodos y protocolos de conexión.[11] .

Las diferentes partes de las redes se pueden conectar a los sensores mediante tecnologías como Wi-Fi, Bluetooth, Wi-Fi de bajo consumo, Wi-Max, Ethernet normal, Long Term Evolution (evolución a largo plazo, o LTE) y la reciente y prometedora tecnología Li-Fi (que utiliza la luz como medio de comunicación entre las diferentes partes de una red típica, incluidos los sensores).

1.4.3 Estándares

La tercera fase en el proceso de implementación incluye la suma de todas las actividades en materia de gestión, tramitación y almacenamiento de los datos recopilados por los sensores. Es una de las fases más importantes ya que en esta fase es como se trata los datos recolectados. Los retos a los que se enfrenta la adopción de normas es que deben existir métodos para el manejo de datos no estructurados, cuestiones de seguridad y privacidad.[20]

1.4.3 Análisis inteligente

La cuarta fase de la implantación del Internet de las Cosas consiste en extraer conocimiento de los datos para su análisis. El análisis está impulsado por tecnologías cognitivas, inteligencia artificial y software de análisis de código abierto, lo que permite procesar distintas formas de información como

la visión y la voz, abriendo la puerta para una comprensión en profundidad de los flujos ininterrumpidos de datos en tiempo real. [20]

1.4.4 Acciones inteligentes

Las acciones inteligentes se pueden expresar como interfaces M2M (máquina a máquina) y M2H (máquina a humano), que son factores que impulsan la adopción de acciones inteligentes en IoT , en contexto esto se refiere a máquinas que “influyen” en las acciones humanas mediante un fundamento de comportamiento-científico y herramientas de aprendizaje profundo como machine learning. [22]

CAPITULO 2: Estándares y Protocolos de Comunicación

2.1 Introducción

El propósito de este capítulo es redactar un documento de referencia orientado técnicamente con el objetivo estratégico de representar los requisitos de estandarización para las aplicaciones de IoT, los estándares existentes, y los protocolos de comunicación [23].

Un estándar puede definirse en términos generales como el consenso de diferentes agentes para realizar ciertas actividades clave de acuerdo con las reglas acordadas, mientras que un estándar de tecnología puede verse como un conjunto de especificaciones para el que todos los objetos ,procesos, o procedimientos puedan llegar a un acuerdo sobre un formato tecnológico homogéneo a través del cual los dispositivos puedan comunicarse, este concepto se ilustra en la figura 7 [24].

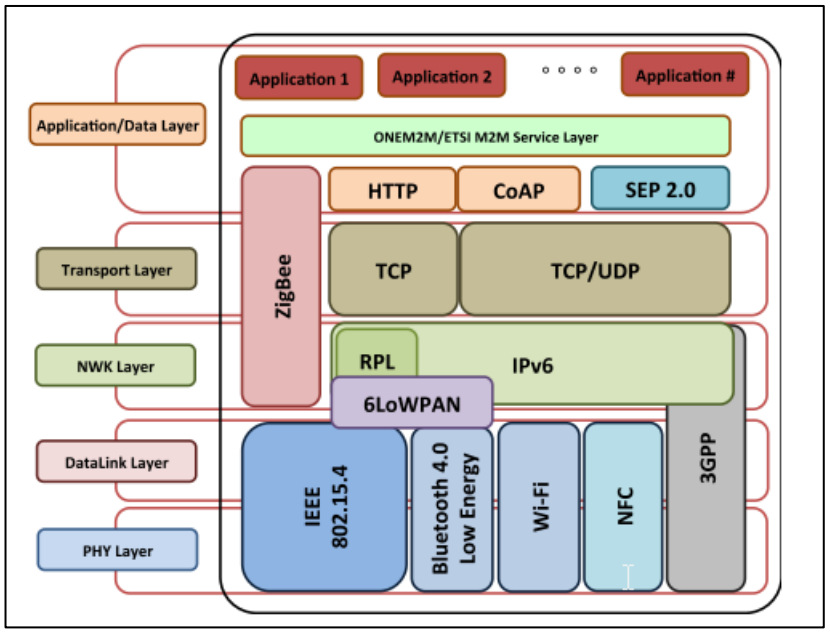


Figura 7 . Ambiente Heterogéneo de Estándares de IoT [25]

Entre los estándares más importantes ya desarrollados tenemos:

- Common Weakness Enumeration (CWE 2018): Este estándar describe posibles debilidades en la arquitectura y el diseño de IoT
- Common Attack Pattern Enumeration and Classification (2018): Es una fuente de recursos para identificar los métodos de ataque

- El Centro de recursos de seguridad informática (2018): Este proporciona información sobre el estándar de seguridad informática del gobierno de los Estados Unidos para acreditar módulos criptográficos
- Common Criteria (N.d.) proporciona información para el desarrollo de la certificación de seguridad informática para la industria de las tarjetas inteligentes basada en el estándar internacional ISO / IEC 15408. [11]

Es así que para para poder homogenizar una estandarización se necesita dividir los componentes de IoT en 4 categorías: plataforma, conectividad, modelo de negocio y aplicaciones determinantes.

2.1.1 Plataforma

Esta categoría incluye la forma y el diseño de los productos, las herramientas de análisis encargadas de la transmisión segura de los datos procedentes de todos los productos, y la escalabilidad, que significa la adopción generalizada de protocolos como IPv6[6] en todos los mercados.

2.1.2 Conectividad:

Esta categoría incluye todos los elementos necesarios para la comunicación de los dispositivos que día a día los consumidores utilizan, como por ejemplo dispositivos portátiles, coches inteligentes, hogares inteligentes y, a más alto nivel, ciudades inteligentes.

2.1.3 Modelo de negocio:

Esta categoría representa el resultado final para empezar a invertir en IoT, y usar esta tecnología en negocio. Sin modelos de negocio sólidos para IoT tendremos otra burbuja: este modelo debe cumplir todos los requisitos de todos los tipos de comercio electrónico. Una capa de servicio estándar mundial abierta basada en el futuro estándar ONEM2M abrirá la posibilidad de que una amplia gama de empresas y jugadores ingresen al campo empresarial con diferentes conjuntos de posibles modelos comerciales.

El proveedor de servicios puede enfocarse inicialmente en dominios específicos utilizando una capa de servicio estandarizada y aún tener la posibilidad de extender el negocio hacia un nuevo campo si es necesario. [25]

[6] Esta nueva versión del Protocolo de Internet está destinada a sustituir al estándar IPv4, la misma cuenta con un límite de direcciones de red, lo cual impide el crecimiento de la red.

2.1.4 Aplicaciones determinantes:

En esta categoría esta cualquier aplicación que tiene tres funciones: controlar “cosas”, recoger “datos” y analizar “datos”. Estas funciones están interrelacionadas y se necesitan que todas ellas funcionen para que el modelo tenga una correcta estandarización [22].

2.2 Protocolos de Comunicación

Los dispositivos IoT utilizados tanto en entornos industriales, como en el entorno doméstico, pueden compartir aspectos de kernel (Linux, FreeRTOS, Windows Embedded, siendo el primero de ellos el más utilizado) y servicios de bajo nivel (*Real-Time Management, Context Discovery Management*), pero en términos de comunicación son muy diferentes. A continuación se explican algunos de los protocolos utilizados a nivel doméstico e industrial.[26]

2.2.1 Entorno doméstico:

Figura 8. Protocolos en Entorno Doméstico[27]

Los dispositivos del hogar también son parte del IoT y en su mayoría se conectan a Internet a través del router del hogar. Esto incluye todo tipo de dispositivos domésticos, desde luces, interruptores, sensores de movimiento, termostatos hasta cerraduras y cortinas automáticas. Mediante la conexión WiFi al router, los smartphones también se convierten en paneles de control online y dispositivos de control para aplicaciones *S*mart home[7]. Existen multitud de empresas que fabrican estos dispositivos y cada una tiene su propio protocolo de comunicación, en la tabla 2 se presentan los más importantes.

[7] Se aplica este término a las Casas Inteligentes

PROTOCOLO	DESCRIPCIÓN
AllJoyn	Es un estándar de código abierto, que facilita la comunicación entre dispositivos y aplicaciones, para todo tipo de protocolos de la capa de transporte.
HomePlug y HomeGrid	Son protocolos cuya comunicación se realiza a través de la red eléctrica
MFi	Es un protocolo de comunicaciones propio de Apple diseñado para interactuar con estos dispositivos.
OCF	Este protocolo pretende garantizar la interoperabilidad de millones de dispositivos, gracias a una implementación de referencia (IoTivity)[8] y un programa de certificación.
Thread	Es una tecnología basada en las comunicaciones por red mediante IPv6 que utiliza cifrado AES

Tabla 1 Protocolos de Comunicación

2.2.2 Entorno Industrial:

Podemos definir a IoT industrial como la digitalización completa a través de la integración de tecnologías de procesamiento de datos, software inteligente y sensores, desde los proveedores hasta los clientes. [26]

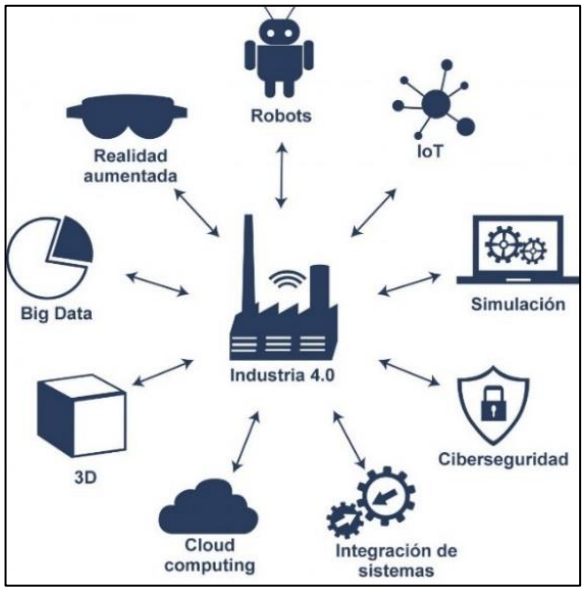


Figura 9. Entorno Industrial[28]

[8] IoTivity es un marco de software de código abierto que permite una conectividad perfecta de dispositivo a dispositivo para abordar las necesidades emergentes de Internet de las cosas.

Los entornos industriales en IoT enfrentan numerosos desafíos de seguridad causados por una gran cantidad de factores y, por lo tanto, necesitan estar preparados para manejar una amplia variedad de amenazas de ciberseguridad. Es probable que las tecnologías de IoT industrial y las empresas de fabricación inteligente se vean afectadas por amenazas, que son típicas en entornos OT y TI. Una buena ilustración de esto es el ataque desarrollado a entornos industriales por el ransomware llamado NotPetya, ya que más del 50% de las empresas afectadas eran entornos industriales [29].

El incremento de dispositivos para proporcionar una mayor inteligencia a los procesos industriales y el uso de técnicas específicas para el tratamiento de datos han supuesto una serie de ventajas con respecto a la industria más tradicional.

Algunas de esas ventajas se comentan a continuación:

- Mejorar la eficiencia energética y mantenimiento predictivo y preventivo de las máquinas, donde podremos obtener, de forma más rápida, datos de los sensores y otros dispositivos II[9]oT para realizar un seguimiento de su funcionamiento de forma constante y, de esta manera, poder prevenirnos ante un posible fallo.
- Mejorar la conectividad respecto a las redes de comunicaciones, esenciales entre el dispositivo y el sistema IIoT dentro del cual opera. En este punto podemos encontrar varias partes:
- Utilizar una segmentación apropiada para el uso de IIoT, como se indica en las buenas prácticas. La seguridad de la red mediante un buen modelo es esencial
- Comunicaciones en tiempo real, lo que implica una necesidad de tener una conectividad continua, además de poder almacenar los datos obtenidos para volver a revisarlos, si fuese necesario. [29]

[9] Internet de las cosas a nivel Industrial

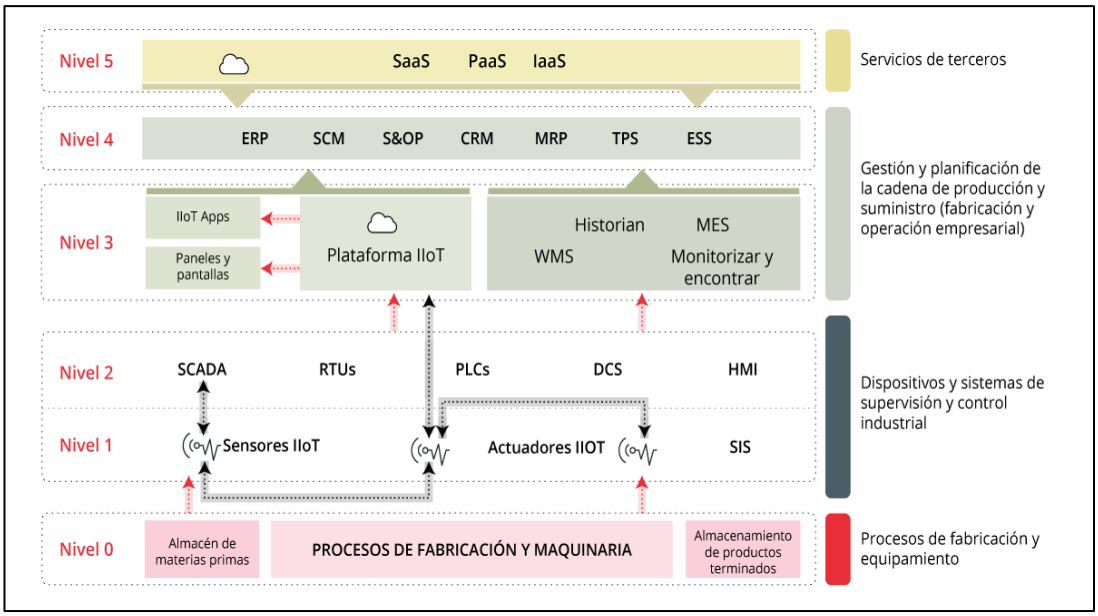


Figura 10. Modelo de referencia de alto nivel de un entorno industrial [29]

2.2.3 Protocolo de enlace de datos de IoT

IEEE 802.15.4: Es el estándar IoT más utilizado para MAC. Define un formato de marco, encabezados que incluyen direcciones de origen y destino, y cómo los nodos pueden comunicarse entre sí. Los formatos de trama utilizados en las redes tradicionales no son adecuados para redes de múltiples saltos de baja potencia en IoT debido a su sobrecarga. En 2008, IEEE802.15.4e se creó para ampliar IEEE802.15.4 y admitir la comunicación de baja potencia. Utiliza la sincronización horaria y el salto de canales para permitir una alta confiabilidad, bajo costo y cumplir con los requisitos de comunicaciones IoT.[30]

IEEE 802.11 AH: Es una versión ligera (de baja energía) del estándar de acceso medio inalámbrico IEEE 802.11 original. Ha sido diseñado con menos gastos generales para cumplir con los requisitos de IoT. Los estándares IEEE 802.11 (también conocidos como Wi-Fi) son los estándares inalámbricos más utilizados. Han sido ampliamente utilizados y adoptados para todos los dispositivos digitales, incluidos computadoras portátiles, móviles, tabletas y televisores digitales. Sin embargo, los estándares WiFi originales no son adecuados para aplicaciones de IoT debido a su sobrecarga de trama y consumo de energía.[30]

WirelessHART: Es un protocolo de enlace de datos que funciona en la parte superior de IEEE 802.15.4 PHY y adopta el acceso múltiple por división de

tiempo (TDMA) en su MAC. Es un protocolo MAC seguro y confiable que utiliza encriptación avanzada para encriptar los mensajes y calcular la integridad para ofrecer confiabilidad. La arquitectura, como se muestra en la Figura 11, consiste en un administrador de red, un administrador de seguridad, una puerta de enlace para conectar la red inalámbrica a las redes cableadas, dispositivos inalámbricos como dispositivos de campo, puntos de acceso, enrutadores y adaptadores. El estándar ofrece mecanismos de seguridad de extremo a extremo, por salto o de igual a igual. [31]

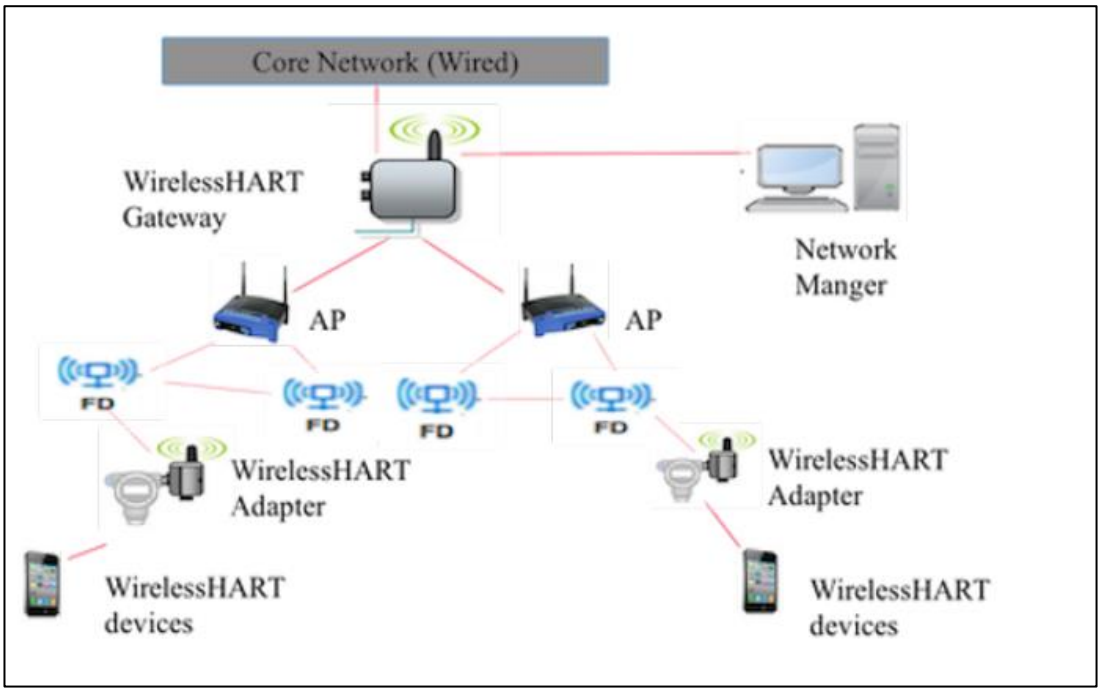


Figura 11 WirelessHart Arquitectura [30]

Z-Wave: Es un protocolo MAC de baja potencia diseñado para la automatización del hogar y se ha utilizado para la comunicación IoT, especialmente para el hogar inteligente y pequeños dominios comerciales. Cubre una comunicación punto a punto de aproximadamente 30 metros y es adecuado para mensajes pequeños en aplicaciones de IoT, como control de luz, control de energía, control de salud portátil y otros. [30]

Bluetooth de baja energía o Bluetooth inteligente: Es un protocolo de comunicación de corto alcance con capa PHY y MAC ampliamente utilizado para redes en el vehículo. Su baja energía puede alcanzar diez veces menos que el Bluetooth clásico, mientras que su latencia puede alcanzar 15 veces más. Su control de acceso utiliza un MAC sin contención con baja latencia y

transmisión rápida. Sigue la arquitectura maestra / esclavo y ofrece dos tipos de marcos: marcos publicitarios y de datos.[30]

La energía inteligente de ZigBee Es un protocolo que está diseñado para una amplia gama de aplicaciones de IoT, incluidos hogares inteligentes, controles remotos y sistemas de atención médica. Admite una amplia gama de topologías de red, incluidas estrella, punto a punto o árbol de clúster. Un coordinador controla la red y es el nodo central en una topología en estrella, la raíz en una topología de árbol o clúster y puede ubicarse en cualquier lugar de punto a punto. [30]

2.2.4 Protocolos en la capa de Red y Encapsulamiento

En este apartado se analizará los protocolos estándar y no estándar que se utilizan para el enrutamiento en aplicaciones IoT y los mecanismos de encapsulación de los mismos.

RPL: El protocolo de enrutamiento para redes de baja potencia y con pérdida, es un protocolo de vector de distancia que puede admitir una variedad de protocolos de enlace de datos, incluidos los discutidos en la sección anterior. Construye un Gráfico Acíclico Dirigido Orientado a Destino (DODAG) que tiene solo una ruta desde cada nodo hoja a la raíz en la que se enrutará todo el tráfico del nodo. Al principio, cada nodo envía un objeto de información DODAG (DIO) publicitándose como la raíz. [30]

CORPL: Es una extensión de RPL es CORPL, o RPL cognitiva, que está diseñada para redes cognitivas y utiliza la generación de topología DODAG pero con dos nuevas modificaciones a RPL. CORPL utiliza el reenvío oportunista para reenviar el paquete eligiendo múltiples reenviadores (conjunto de reenviadores) y coordina entre los nodos para elegir el mejor próximo salto para reenviar el paquete.[30]

6LoWPAN Este protocolo se ejecuta sobre IPv6 en la red de área personal inalámbrica de baja potencia (6LoWPAN) , es el primer estándar más utilizado en esta categoría. Encapsula eficientemente encabezados largos IPv6 en paquetes pequeños IEEE802.15.4, que no pueden exceder los 128 bytes. La especificación admite direcciones de diferentes longitudes, bajo ancho de banda, diferentes topologías que incluyen estrella o malla, consumo de

energía, bajo costo, redes escalables, movilidad, falta de confiabilidad y tiempo de inactividad prolongado. [30]

2.2.5 Protocolos en la capa de Sesión

La mayoría de las aplicaciones IP, incluidas las aplicaciones IoT, utilizan TCP o UDP para el transporte. Sin embargo, hay varias funciones de distribución de mensajes que son comunes entre muchas aplicaciones de IoT. Entre los principales protocolos tenemos los siguientes:

MQTT Message Queue Telemetry Transport Fue introducido por IBM en 1999 y estandarizado por OASIS en 2013 . Está diseñado para proporcionar conectividad integrada entre aplicaciones y middleware en un lado y redes y comunicaciones en el otro lado. Sigue una arquitectura de publicación/ suscripción, como se muestra en la Figura 12, donde el sistema consta de tres componentes principales: editores, suscriptores y un corredor. [30]

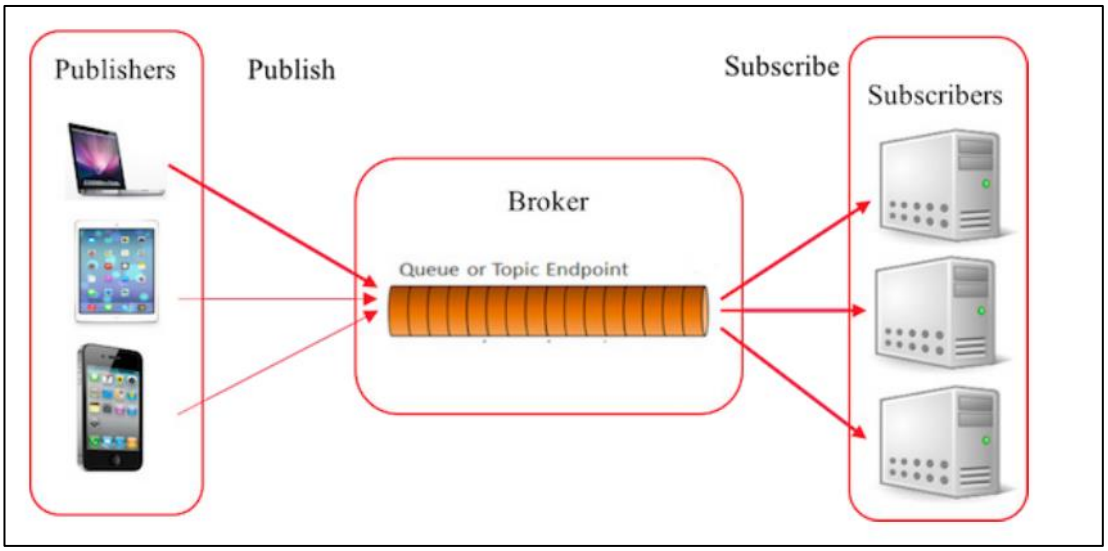


Figura 12 . Arquitectura MQTT [30]

AMQP El Advanced Message Queuing Protocol Es un protocolo de capa de sesión diseñado para la industria financiera. Se ejecuta sobre TCP y proporciona una arquitectura de publicación / suscripción que es similar a la de MQTT. La diferencia es que el corredor está dividido en dos componentes principales: intercambio y colas, como se muestra en la Figura 13.

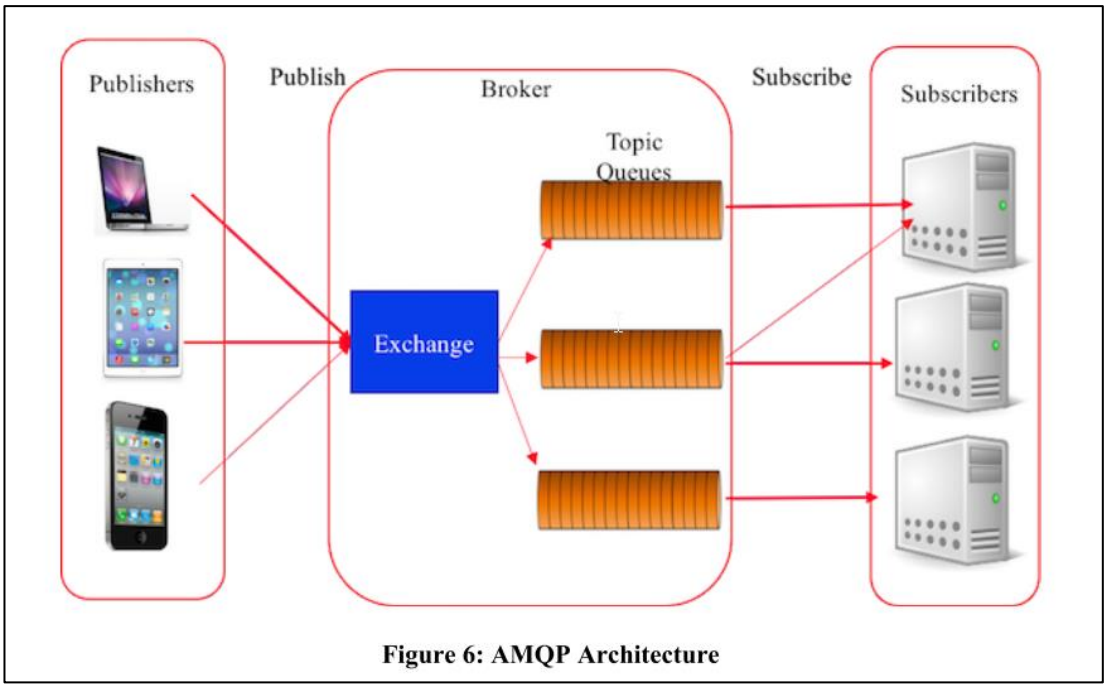


Figura 13 Arquitectura AMQP [30]

2.2.5 Protocolos en la capa de Aplicación

El protocolo de aplicación restringida (CoAP) fue diseñado por IETF para cumplir con ciertas características tales como simplicidad, baja sobrecarga y soporte de multidifusión en entornos con recursos limitados. dispositivos y redes de bajo ancho de banda y bajo consumo de energía, a diferencia de HTTP CoAP es un descubrimiento completamente asíncrono y solicitudes de multidifusión, CoAP es una combinación interesante de hacer que la web sea muy eficiente y agregar características que son importantes para las aplicaciones IOT como suscripciones y descubrimiento. [31]

Características

- Protocolo de transferencia web para dispositivos restringidos
- Enlace UDP con confiabilidad y soporte de multidifusión
- Métodos GET, POST, PUT, DELETE
- Descubrimiento incorporado
- Encabezado simple de 4 bytes
- Transacción asincrónica modelo 7.

CAPITULO 3: CIBERSEGURIDAD

3.1 Definición

La ciberseguridad se define como “el conjunto de tecnologías y procesos construidos para proteger las computadoras, hardware, software, las redes y los datos contra el acceso no autorizado, las vulnerabilidades suministradas a través de Internet por los ciberdelincuentes, los grupos terroristas y los piratas informáticos”.[32]

Otra definición de ciberseguridad es “la actividad o proceso, capacidad, o el estado mediante el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos contra daños, uso o modificaciones no autorizadas” [32]

El diccionario de Oxford define la ciberseguridad de la siguiente manera: "El estado de protección contra el uso criminal o no autorizado de datos electrónicos, o las medidas tomadas para lograrlo". [11] Si bien esta definición puede ser adecuada para los administradores de sistemas y otros profesionales de la tecnología de la información, no tiene en cuenta las consideraciones relevantes de formulación de políticas. Esencialmente, la ciberseguridad es la seguridad del ciberespacio, por lo tanto, es igualmente importante entender el ciberespacio. Cuando los usuarios van en línea, pueden trabajar con su banco, recibir su correo electrónico, realizar negocios u obtener las noticias accediendo a los servicios, pero esos servicios no existen independientemente. Esos servicios se basan en una infraestructura común de servidores y conmutadores, millas de cableado, espectro inalámbrico y enrutadores.[33] La creación de un clima de seguridad y confianza digital que permita reforzar la protección de los organismos públicos y privados y estimule la implicación de los usuarios en el entorno digital, es vital para el pleno desarrollo de la Sociedad y Economía en un contexto en el que los incidentes son cada vez más frecuentes, complejos y de mayor magnitud [28].

3.2 Retos de la Ciberseguridad en IoT

Existen diferentes métodos de protección dependiendo de las amenazas. Para proteger y asegurar las vulnerabilidades de la capa de transporte, la forma de proteger es utilizar protocolos de comunicación seguros como TLS

o SSH. Además, el uso de cifrados sólidos y servicios confiables asegura la ruta de transporte entre dispositivos. También se recomienda el uso de herramientas de prueba preparadas para la verificación de una capa de transporte segura. [11] .

Existe un concepto que se denomina “Security by Default”, que no es más que el establecimiento de una configuración por defecto que sea segura en el momento de la fabricación y distribución de un dispositivo. Con este concepto se pretende solucionar el problema que tienen estos dispositivos, que no vienen dados por las capacidades o calidad de los mismos, sino por la ausencia de interfaces amigables que permitan administrarlos como en el caso de los PC o smartphones[9].

Las organizaciones enfrentan muchas amenazas con una variedad de vectores de ataques para llevar a cabo ataques. Los actores de amenazas pueden apuntar a los elementos del ciberespacio (por ejemplo, redes, datos, servicios y usuarios). Sin embargo, también pueden usar estos elementos para atacar a la industria a través del ciberespacio. Por ejemplo, un pirata informático que opera de forma independiente o bajo las instrucciones de un estado nacional puede apuntar a un hospital. El hacker puede enviar ransomware a un hospital para extorsionar el pago antes de que el hospital pueda recuperar el acceso a sus archivos y dispositivos. Pero durante ese ataque, el pirata informático también puede instalar una puerta trasera en la red del hospital, proporcionando acceso persistente que usarán para robar datos, incluida la información del paciente y sus transacciones.

La ciberseguridad en cifras: los datos muestran incremento en la preocupación empresarial

Según un estudio realizado por cámara valencia, las empresas con soluciones IoT esperan conseguir un “24%” de beneficios gracias a su estrategia de seguridad y el 76% de las empresas que trabajan con soluciones cloud consideran la ciberseguridad como fuente de nuevas oportunidades de negocio. En la figura 14 se puede observar en un gráfico estas estadísticas.

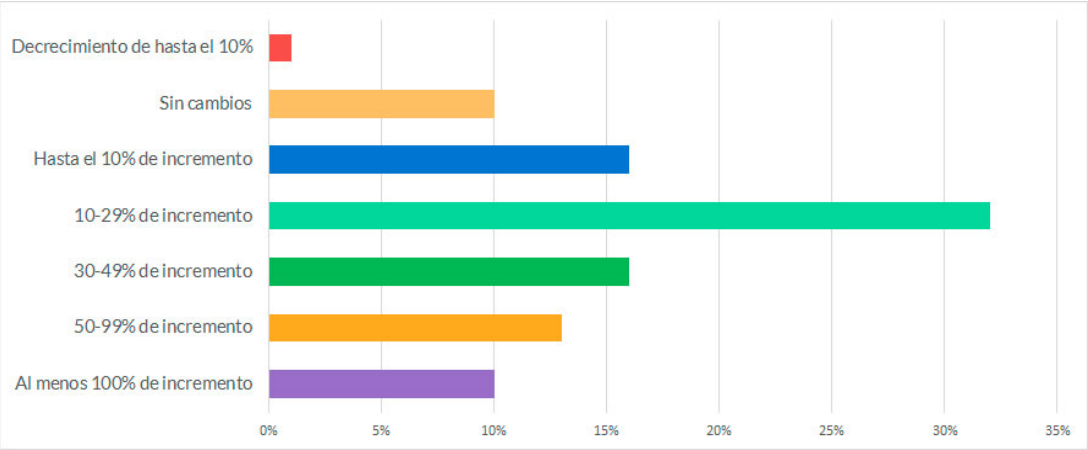


Figura 14. Empresas que piensan que es necesario variar el presupuesto de Ciberseguridad para los próximos tres años [34]

Como vemos en el gráfico, el 87% de las empresas encuestadas va a invertir. Un tercio incrementará el presupuesto de ciberseguridad entre un 10 y 29 por ciento. El 10% doblará la inversión. [34].

Por lo antes mencionado, se han desarrollado varias medidas de seguridad que ayudaran a las organizaciones a mitigar estas amenazas.

3.2.1 Fin de la autenticación de doble factor.

La autenticación de doble factor ha sido desde siempre una de las herramientas que aumentan exponencialmente la seguridad de cualquier cuenta al vincularla a un dispositivo o detección biométrica. Durante el 2018 se desarrollaron ataques tan sofisticados como el uso de modelos de cera para saltar un escáner biométrico o el pirateo de tarjetas SIM para saltar el control de autenticación de doble factor por lo cual para el 2020 es hora de desarrollar nuevas herramientas que sean capaces de blindar nuestra privacidad y el acceso a nuestros datos más confidenciales. [35]

Figura 15. Esquema de Doble Factor de Autentificación. [36]

3.2.2 Ransomware y minado de monedas a través de Cryptohacking

El Ransomware (secuestro de información) es el término genérico para referirse a todo tipo de software malicioso que le exige al usuario del equipo el pago de un rescate. La forma de infección más usual es a través de la apertura de archivos adjuntos de correos electrónicos no solicitados o al hacer clic en vínculos que aseguran provenir de entidades bancarias o de empresas de mensajería. También se encontraron versiones de Cryptolocker que se distribuyeron a través de redes peer- to-peer (P2P) para compartir archivos, haciéndose pasar por claves de activación para programas populares de software como Adobe Photoshop y Microsoft Office. [37].

ESET (empresa eslovaca de seguridad informática) advierte que el ransomware ha sido una de las fuentes de negocio de los cibercriminales en 2018, dada la tendencia anunciada anteriormente, y sitúa la elección de las empresa hacia pagar grandes sumas de dinero por recuperar sus sistemas comprometidos en lugar de contar con políticas de ciberseguridad que las mantengan protegidas ante cualquier amenaza. [38]

Figura 16. Ejemplo de un Ransomware [37]

Cryptohacking

Esta modalidad pretende explotar las capacidades de proceso de los sistemas de otros, para el lucro personal de hackers que utilizan las máquinas en minería de criptomonedas. El auge del mercado de las criptomonedas y el crecimiento explosivo que ha experimentado, pone a estas plataformas en el punto de mira de los cibercriminales. Son comunes las infecciones de equipos con software de minería de criptomonedas o el robo de wallets de usuarios.

Figura 17. Estadística del robo de Criptomonedas [37].

Según los datos del último 'Índice Global de Ciberamenazas' de Check Point, en julio se produjo un aumento significativo en exploits que afectan a las tres principales vulnerabilidades del IoT, creciendo más del doble respecto al mes de mayo. La compañía indica que estos ataques están relacionados con la propagación de malware contra objetos conectados como Mirai, IoTroop/Reaper y VPNFilter. El informe especifica que el 45% de las organizaciones de todo el mundo se vieron afectadas por los ataques dirigidos contra ellas, frente al 35% registrado en junio y el 21% en mayo. Dichos ataques permiten que los cibercriminales ejecuten código malicioso y obtengan control remoto de los dispositivos objetivo. "Las vulnerabilidades del IoT son a menudo el camino que ofrece menos resistencia. Una vez que se alcanza un dispositivo puede ser fácil infiltrarse en otros objetos conectados.

Por tanto, es vital que las organizaciones apliquen parches a las vulnerabilidades conocidas a medida que estén disponibles para garantizar que las redes permanezcan seguras", afirma Maya Horowitz, directora del equipo de Inteligencia de Amenazas de Check Point.[3]

3.2.3 Internet de las Cosas, en la mira de los ciberdelincuentes.

Figura 18. IoT y Ciberseguridad [39]

El Internet de las Cosas va a cambiar el mundo, pero para conseguirlo es necesario una postura de ciberseguridad mucho más estricta que la actual. El

uso de contraseñas por defecto, falta de hardening[10], abandono del proyecto y aparición de vulnerabilidades que no son parchadas, interfaces poco cuidadas, falta de cifrados o un diseño inadecuado son algunos de los retos a los que el IoT se ha enfrentado y deberá seguir haciendo frente [35]

Desafortunadamente, la falta de seguridad de la tecnología IoT no sólo es culpa de los profesionales que dejan agujeros y brechas de seguridad en el hardware o en el software de los dispositivos, sino también de los consumidores, que son causa importante de que los ataques de piratas informáticos sigan siendo tan numeroso, debido a que no son proactivos en mantenerse seguros.

A corto plazo, según los datos de la firma de análisis de mercado Gartner, este 2016 se sobrepasarán los 6.400 millones de dispositivos. A cinco años, las previsiones apuntan a que habrá más de 50.000 millones dispositivos conectados a internet. Además, se estima que esta tendencia generará 12.000 millones de euros solo en Europa hasta el 2020. [28]

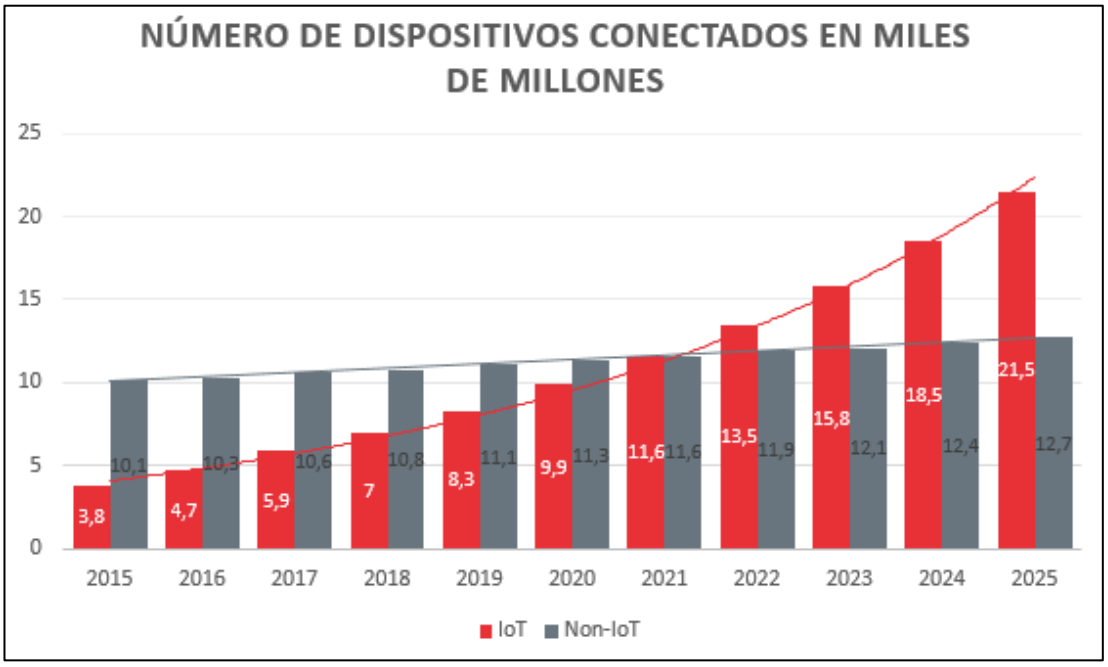


Figura 19. Estadística de dispositivos conectados hasta el 2025 [39]

Los ataques a las redes centrales se encuentran entre los riesgos de seguridad más importante para los billones de dispositivo IoT. Ya que un solo hacker puede llevar un ataque informático de denegación al servicio

[10] Es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad

distribuido o (DDoS), que inunda los dispositivos interconectados en la red con demasiada solicitud, por ende, el servidor no puede procesar el gran número de solicitudes “legitimas” y el servidor colapsa y se apaga, dejando a los dispositivos desamparados.

3.2.4 Machine Learning y Big Data

Según Gartner, se estima que el gasto TIC en Big Data a nivel mundial alcanzaró los 55.000 millones de dólares (42.652 millones de euros) en 2016. El Big Data comienza a cobrar cada vez más importancia gracias a la proliferación de páginas web, aplicaciones de imagen y vídeo, redes sociales, dispositivos móviles, apps, sensores, internet de las cosas, etc. capaces de generar más de 2.5 quintillones de bytes al día. Las vastas cantidades sin precedentes de nueva información que se crean y se comparten cada segundo, así como el análisis de dichos datos, se convierten en un activo transformador de gigabytes de información en conocimiento tanto para ciudadanos, empresas o gobierno [28] , esto permitirá detectar nuevas amenazas que generalmente escapan de los métodos de detección tradicionales, aprendiendo del comportamiento y actuando sin la intervención humana [38] .

La inteligencia artificial (IA) y el aprendizaje automático (ML) han sido ampliamente promocionados en los últimos años como el futuro de la tecnología , ya que tienen una gran cantidad de aplicaciones, incluida la identificación de actividad de red anómala, la actualización de sistemas basados en reglas y la reducción de falsos positivos. [40]

Según el artículo publicado por Anna L. Buczak llamado “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection” su artículo presenta los resultados de una encuesta bibliográfica de métodos de aprendizaje automático “machine Learning “(ML) y minería de datos (DM) para aplicaciones de ciberseguridad. Los métodos ML / DM son descritos, así como la aplicación de cada método para problemas de detección de intrusiones cibernéticas, el problema con el manejo de algoritmos de machine Learning es que estas técnicas basadas en el aprendizaje no pueden detectar nuevos ataques (día cero).

3.2.5 Casas Inteligentes

Una Smart Home o casa inteligente ha de ser entendida como aquella casa que hace uso de las nuevas tecnologías (TIC) para conseguir que sus activos, servicios e infraestructuras sean más accesibles e interactivos desde cualquier parte del mundo. Aquí, los sistemas de telemedida y su securización adquieren un papel determinante.

El desarrollo de una ciudad inteligente, así como la manera de protegerla no resulta una tarea sencilla, ya que, como se ha dicho, existen muchos desafíos derivados de la propia tecnología y de la complejidad resultante de la integración de los diferentes sistemas y escenarios que la conforman. Entre los principales retos de ciberseguridad en una ciudad inteligente tenemos: [41]

- Ciberseguridad pobre o inexistente, en términos generales
- Proveedores de tecnología que dificultan o imposibilitan la investigación en ciberseguridad
- Existencia de superficies de ataque grandes y complejas.
- Falta de evaluaciones de seguridad (auditorías y consultorías) sobre el software que se aplica en las ciudades inteligente.
- Existencia de sistemas heredados inseguros, con códigos mal escritos y varios problemas de seguridad.
- Existencia de problemas con las actualizaciones de software.
- Existencia de problemas de cifrado.

Al existir una gran variedad de vectores de ataque, una vez que prácticamente han irrumpido en una casa inteligente, los atacantes pueden controlar todos los dispositivos y dispositivos inteligentes conectados a la red doméstica. En este caso, eso significa que podrían controlar la temperatura en la casa, encender la sauna, reproducir música a todo volumen desde el estéreo (algo que realmente hicieron, cambiaron el sonido de la alarma a una pista de batería y bajo), imprimir cualquier cosa en una red impresora y así sucesivamente. Más importante aún, podrían abrir remotamente la puerta principal y desactivar las cámaras de seguridad y los sensores de movimiento, una forma fácil de robar la casa. Y como sabían las coordenadas del teléfono del propietario, podían planificar la operación para cuando él estuviera lejos de casa.

¿Cómo asegurar una casa inteligente más segura?

Estos son algunos consejos pasos para proteger la red doméstica y los dispositivos conectados:

Configuraciones de Seguridad en la red inalámbrica. El antiguo protocolo de privacidad equivalente por cable (WEP) sigue siendo ampliamente utilizado, pero es débil y se puede comprometer fácilmente. Para mantener una red segura hay que asegurar que la red inalámbrica doméstica esté protegida por el protocolo Wi-Fi Protected Access II (WPA2) y una contraseña fuerte y compleja. Otra medida a tener en cuenta es deshabilitar las funciones WPS[11] (configuración protegida de Wifi) y UPNP (Universal Plug and Play). WPS facilita la adición de nuevos dispositivos a la red simplemente presionando el botón WPS en el enrutador y luego presionando el botón WPS en el dispositivo. Sin embargo, esto puede ser utilizado por personas no autorizadas para obtener acceso a su enrutador, por lo tanto, la necesidad de desactivarlo. [42]

SSID o nombre de la red. El nombre de la red inalámbrica no debería contener información que pueda ser usada por los atacantes, por ejemplo, no llamar a la red “[Tu nombre] Casa". En cambio, se lo debería llamar con un nombre al azar, esto dificulta que los piratas informáticos identifiquen el tipo de enrutador, evitando así que exploten vulnerabilidades conocidas. El nombre de la red no debe revelar ninguna información personal, ya que incluso un poco puede usarse en el robo de identidad.

Cree dos redes Wi-Fi diferentes. Si el enrutador lo permite se debe crear dos redes diferentes, una para el manejo de cuentas que se realicen pagos con tarjetas de crédito y otra para la navegación normal de la Web.

Gestión de contraseñas.

- Ni los equipos de red (como enrutadores y conmutadores) ni los dispositivos nuevos (como los televisores inteligentes) se deben usar contraseñas de administrador predeterminadas de fábrica. Cambiar cada contraseña de administrador a algo adecuadamente fuerte y complejo, se las debe cambiar regularmente en el futuro, ya que si un

[11] Wps significa Configuración protegida de Wi-Fi. Es un estándar de seguridad de red inalámbrica que intenta establecer conexiones entre un enrutador y una red inalámbrica.

atacante determina qué enrutador tiene, puede buscar sus credenciales predeterminadas yendo a sitios como RouterPasswords y DefaultPassword.

- Usar contraseñas seguras que sean largas (16–20 caracteres) y complicadas. Siempre puede realizar un reinicio maestro si alguna vez olvida su contraseña.
- Una vez que la red es segura, examine cada dispositivo IoT que posea y lo que está haciendo. Deshabilite el acceso de administración remota y otras potentes herramientas de red si no se van a utilizar. [43]

3.2.6 Botnets

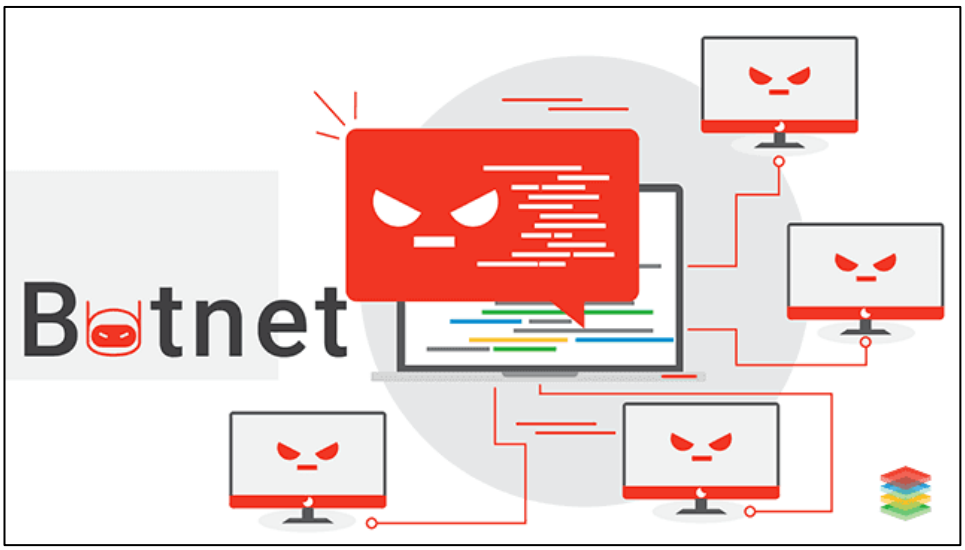


Figura 20. Botnets [44]

El término Bot, derivado de "ro-bot" en su forma genérica, se usa para describir un script o un conjunto de scripts o un programa diseñado para realizar funciones predefinidas repetida y automáticamente después de activarse intencionalmente o mediante una infección del sistema. Aunque los bots se originaron como una característica útil para llevar a cabo operaciones repetitivas y que requieren mucho tiempo, están siendo explotados con fines maliciosos. [45] .

En IoT la botnet está controlada por lo que se denomina “botmaster” que ejecuta actividades coordinadas con la ayuda de los bots zombie. Se pueden desarrollar ataques como DDOS, spam, campaña de phishing, fraude de clics y spyware. Una de las principales maneras que los dispositivos IoT se

convierten en zombies es debido a la falta de seguridad primitiva, infección de virus o la apertura de un archivo adjunto de correo electrónico malicioso.

Una vez que las computadoras están infectadas, las Botnets se comunican a través de Internet, y luego las Botnets tienen acceso libre para modificar información personal, atacar otras computadoras y cometer otros delitos. [44]

Creación de Botnets

Para la creación de una botnet depende en gran medida de las habilidades y requisitos del atacante ya que elige entre escribir su propio código o simplemente extiende o personaliza un botnet existente. En la Web también se puede comprar Botnets ya desarrolladas, en las cuales los bots (máquinas zombie) están listos para usar y son altamente configurables con instrucciones paso a paso sobre cómo comprometer los sistemas. Las instrucciones incluyen instrucciones para obtener exploits de empaque, caracteres simples e interfaces gráficas de usuario, y varias otras herramientas para obtener la entrada de puerta trasera en las redes. [46]

El código de una botnet generalmente contiene componentes configurables que incluyen información del canal y el servidor IRC, el puerto de servicio TCP IRC remoto, la ubicación y el nombre del archivo de código bot en la máquina infectada y otros componentes que permiten al creador cambiar dinámicamente el comportamiento de ataque de la misma.

Propagación de Botnets

Para la propagación de las Botnets y la búsqueda de máquinas zombies se ubican sistemas y herramientas vulnerables para explotarlos que luego se utilizan como puerta trasera a estos sistemas que facilitan la instalación de malware de la botnet cargando u ordenando a la máquina víctima que descargue una copia del malware. El malware de bot también se propaga a través de redes de igual a igual, el intercambio de archivos abiertos y el intercambio directo de archivos de cliente a cliente.

Ciclo de vida de Botnets

En general, las Botnets tienen un comportamiento similar independientemente de su variante o la familia de malware a la que pertenecen, las Botnets regulares comparten ciclos de vida cuando comprometen nuevos dispositivos y terminan dejandolos.

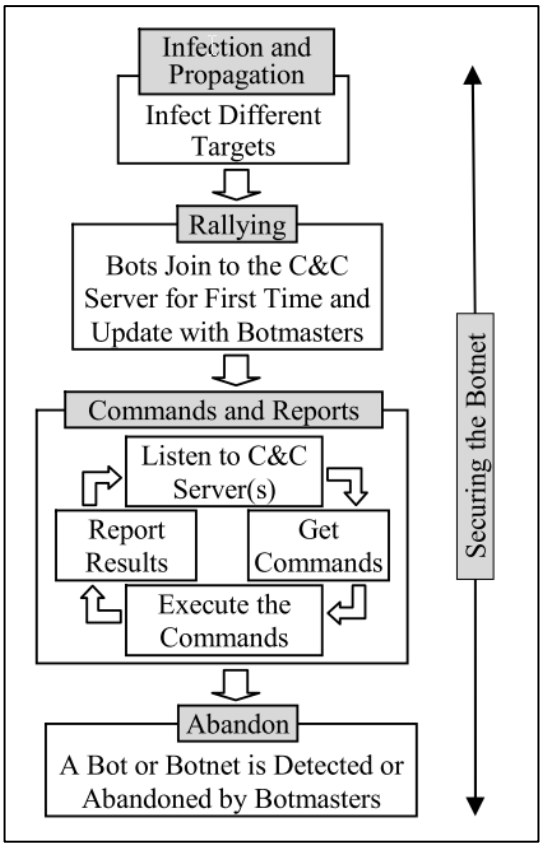


Figura 21. Ciclo de vida de una botnet [45]

El ciclo de vida de una botnet IoT típica se visualiza en la Figura 21 la cual se detalla a continuación:

Infección y Propagación: Escanear la red en busca de puertos abiertos en los dispositivos conectados. Realiza fuerza bruta los puertos descubiertos para obtener acceso a las víctimas.

Reunión: Desauntetica a competidores potenciales en los hosts infectados y avisa al botmaster si ya se encuentra conectado a la máquina zombie. Adicionalmente la botnet recibe información de la máquina zombie como la IP del servidor.

Comandos Y Reportes: Ejecuta y, a veces, eliminar scripts maliciosos (se ejecuta en la memoria). De la misma manera el botmaster ejecuta comandos en la máquina zombie los cuales se ejecutan en un orden lógico.

Abandono: Cuando una botnet no va a ser usada nunca más por razones de banda ancha o algunas otras circunstancias , el botmaster elimina la botnet y todas las máquinas zombies son liberadas .[45]

Este ciclo de vida se observó en la Botnet Mirai[12] y en algunas de sus variantes como Satori o Persirai. Aunque la operación general sigue siendo la misma, algunos pasos pueden diferir. Por ejemplo, la Botnet Satori en lugar de escanear la red en busca de puertos abiertos en los dispositivos intenta conectarse en los puertos 37.215 o 52 869 utilizando un exploit, mientras que la botnet Persirai explota una vulnerabilidad reportada de día cero que proporciona acceso directamente a los datos de la contraseña. Sin embargo, una vez que los dispositivos IoT están infectados, todos pueden usarse para ejecutar ataques DDoS a gran escala. [45] .

[12] Mirai es un malware que convierte los dispositivos en red que ejecutan Linux en bots controlados de forma remota que pueden usarse como parte de una botnet en ataques de red a gran escala

CAPITULO 4: Casos de Estudio: Vectores de Ataque a dispositivos IoT

En e siguiente capítulo se exponen cuatro casos de estudio , en los cuales se desarrollan pruebas de concepto técnicas que permiten determinar los diferentes vectores de ataques a los que son vulnerables los dispositivos que forman parte de IoT, como se puede obtener información confidencial de una organización al lograr explotar las vulnerabilidades de los mismos y también se realiza recomendaciones de mitigación y prevención hacía los ataques desarrollados según la metodología Owasp 2017 , también se realiza un análisis de cómo funcionan las Botnets y cómo usar los dispositivos infectados para el criptmoniado de divisas .

4.1 Shodan como vector de ataque

En la actualidad cualquier dispositivo que se conecta a Internet, independientemente de la información que contenga, pagos al seguro social, historial médico, o tarjetas de crédito supone un riesgo a la confidencialidad de los datos. En base a esta premisa se desarrolló Shodan que es un proyecto creado por el experto en seguridad John Matherly, que lo ha definido como “el buscador más aterrador del mundo”. Su nombre procede del tipo de inteligencia artificial malvada del mítico videojuego System Shock.

Shodan tiene la capacidad de descubrir e indexar prácticamente cualquier dispositivo**,** entre una amplia gama que abarca webcams, de señalización para vías, routers, firewalls, sistemas de circuito cerrado de televisión, sistemas de control industriales para plantas de energía nuclear, redes eléctricas, electrodomésticos domésticos y mucho más. La parte más peligrosa y negativa de esta detección es que todos estos dispositivos se encuentran conectados a Internet, sin que sus dueños sean conscientes de los peligros y riesgos a nivel de seguridad informática que ello conlleva. [47]

Filtros de búsqueda Shodan

Los filtros de búsqueda de Shodan, permiten tener un control mayor de lo que se busca y así obtener resultados específicos, entre los más importantes tenemos los que se muestran en la tabla 3. [48]

Búsqueda por país. Por ejemplo, Argentina
country:ar
Búsqueda por ciudad. Por ejemplo, Buenos Aires
city:BuenosAires
Búsqueda por sistema operativo. Por ejemplo, Windows
os: Windows
Búsqueda por número de puerto. Por ejemplo, 25
port:25
Búsqueda por Proveedor de internet "ISP"
En caso de querer filtrar las búsquedas por ISP (Internet Service Provider) podemos utilizar este filtro. Ejemplo: isp:telefonica
Búsqueda por fecha
before:01/09/2028.

Tabla 2. Filtros de Shodan[48]

A través de la búsqueda de dispositivos con Shodan y los filtros mencionados en la tabla 4, los atacantes infectaron a miles de dispositivos con código malicioso para formar una botnet[13]. Aunque no es un medio sofisticado de ataque, su fuerza radica en la cantidad de dispositivos infectados, ya que pueden utilizarse para desbordar servidores lo que provoca perdida de disponibilidad.

4.2 Consideraciones de Seguridad en dispositivos Iot

Existen varias consideraciones para una organización en lo que respecta a medidas de seguridad para sus dispositivos, y así poder llegar a un nivel de madurez adecuada en lo que corresponde a Seguridad Informática.

La figura 22 tomada de la página web de Open Web Application Security, OWASP (2017) [3] muestra claramente la relación de los vectores de ataque, las debilidades de seguridad, los controles de seguridad, los impactos técnicos y su influencia en el negocio.

[13] Una botnet es un número de dispositivos conectados a Internet, cada uno de los cuales ejecuta uno o más bots

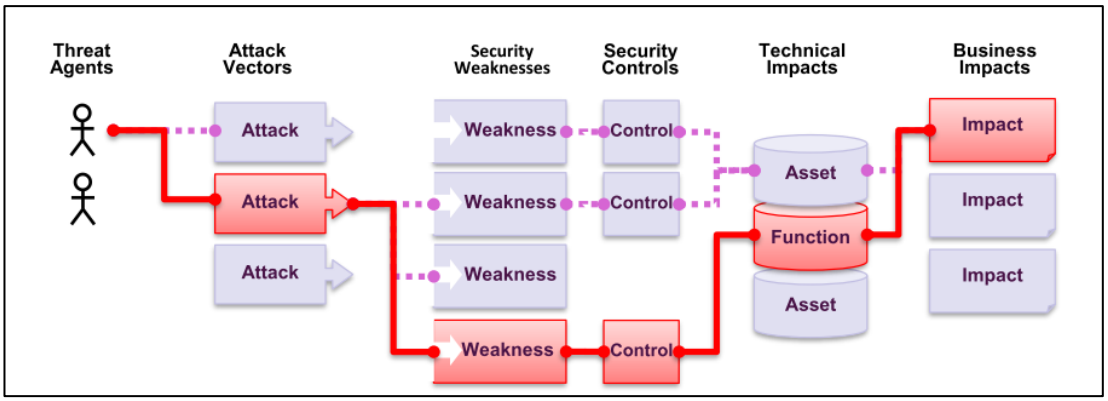


Figura 22. Riesgos de Seguridad , Owasp 2017 [3]

En el caso de estudio 4.2.1, 4.2.2, los vectores de ataque se basan en Open Web Application Security Project (OWASP 2017). La razón por la cual se decidió usar OWASP es porque esta metodología cubre los vectores de ataque más típicos contra dispositivos IoT. Cabe recalcar que en estas pruebas de concepto se excluye los dispositivos comerciales de IoT para casas inteligente, cámaras de vigilancia, dispositivos de red y televisores inteligentes.

En la tabla 5 se consideran los posibles vectores de ataque contra dispositivos IoT según Owasp 2017 [3]

VECTORES DE ATAQUE	
A1:2017- Injection	Los defectos de inyección, como la inyección de SQL, NoSQL, OS y LDAP, se producen cuando se envían datos no confiables a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a los datos sin la autorización adecuada.
A2:2017-Broken Authentication	Las funciones de la aplicación relacionadas con la autenticación y la administración de sesiones a menudo se implementan de manera incorrecta, lo que permite a los atacantes

	comprometer contraseñas, tokens de sesión, o explotar otros defectos de implementación para asumir las identidades de otros usuarios de manera temporal o permanente.
A3:2017- Sensitive Data Exposure	Muchas aplicaciones web y API no protegen adecuadamente los datos confidenciales como por ejemplo los financieros, la atención médica , etc. Los atacantes pueden robar o modificar dichos datos débilmente protegidos para realizar fraudes con tarjetas de crédito, robo de identidad u otros delitos.
A4:2017-XML External Entities (XXE)	Muchos procesadores XML antiguos o mal configurados evalúan referencias de entidades externas dentro de documentos XML. Las entidades externas se pueden usar para revelar archivos internos utilizando el controlador de URI de archivo, recursos compartidos de archivos internos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio.
A5:2017-Broken Access Control	Las restricciones sobre lo que los usuarios autenticados pueden hacer a menudo no se aplican de manera adecuada. Los atacantes pueden explotar estas fallas para acceder a funciones y / o datos no autorizados, como acceder a las cuentas de otros usuarios, ver archivos confidenciales, modificar los datos de otros usuarios, cambiar los derechos de acceso, etc.
	La configuración incorrecta de seguridad es el problema más comúnmente visto. Esto suele ser el resultado de configuraciones

A6:2017-Security Misconfiguration	predeterminadas inseguras, configuraciones incompletas, almacenamiento en la nube abierta, encabezados HTTP mal configurados y mensajes de error detallados que contienen información confidencial.
A7:2017- Cross-Site Scripting (XSS)	Los defectos de XSS ocurren cada vez que una aplicación incluye datos no confiables en una nueva página web sin una validación o escape adecuados, o actualiza una página web existente con datos proporcionados por el usuario utilizando una API de navegador que puede crear HTML o JavaScript.
A8:2017- Insecure Deserialization	La deserialización insegura a menudo conduce a la ejecución remota de código. Incluso si las fallas de deserialización no resultan en la ejecución remota de código, pueden usarse para realizar ataques, incluidos ataques de repetición, ataques de inyección y ataques de escalada de privilegios.
A9:2017-Using Components with Known Vulnerabilities	Los componentes, como bibliotecas, marcos y otros módulos de software, se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, dicho ataque puede facilitar la pérdida grave de datos o la adquisición del servidor.
A10:2017- Insufficient Logging & Monitoring	El registro y monitoreo insuficientes, junto con la integración faltante o ineficaz con la respuesta a incidentes, permite a los atacantes atacar más los sistemas, mantener la persistencia, girar a más sistemas y manipular, extraer o destruir datos.

Tabla 3. Vectores de ataque Según Owasp 2017 [3]

4.2.1 Caso de estudio #1: Ataque a Routers

Un router es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red, tiene como función principal establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

Es decir, si se coloca de manera online un router, una cámara, una TV o incluso una heladera inteligente que se encuentre conectada al router sin antes cambiar la contraseña predeterminada está permitiendo que se lleven a cabo varios tipos de ataques. Las investigaciones recientes de la compañía ESET sugieren que al menos el 15% de los routers domésticos no están protegidos, es decir que hay potencialmente 105 millones de routers vulnerables.

4.2.1.1 Ataques de fuerza bruta

En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

En la siguiente prueba de concepto vamos a observar cómo a través de un ataque de fuerza bruta se puede obtener acceso al router, los archivos propios del mismo y posteriormente a los dispositivos conectados, creando así un problema de confidencialidad, disponibilidad, y no repudio de los datos que se manejan dentro de la red Wlan. Para esta prueba de concepto usaremos el buscador Shodan que como se mencionó en el apartado 4.1 ya que es el primer motor de búsqueda del mundo para dispositivos conectados a Internet.

Especificaciones de los componentes:

- **Motor de Búsqueda:** Shodan
- **Router**: Marca: NuCom, Modelo NC-WR744G.
- **Sistema Operativo para ejecución de ataques**: ParrotOs

Para el desarrollo de esta prueba de concepto, aplicaremos la metodología CEH la cual consta de 7 fases como observamos en la siguiente ilustración.

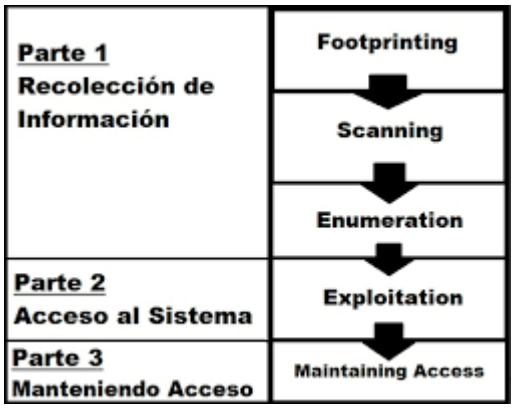


Figura 23. Metodología CEH [49]

Siguiendo la metodología anteriormente mencionada, el primer paso es la recolección de información para lo cual usaremos el buscador Shodan, en el cual buscaremos el modelo del router obteniendo los siguientes resultados.

Figura 24. Resultado de la búsqueda del modelo del router en Shodan

Como se observa en la figura 24 se obtuvo un total de 824 resultados. Uno de los mayores defectos de los routers domésticos es que si sale a Internet con su IP privada y aparece en la lista de Shodan, es vulnerable a varios tipos de ataque, de tal manera que si alguien conoce el usuario y la contraseña del router podría acceder desde cualquier parte del mundo, y desde cualquier dispositivo que tenga acceso a Internet (Portátil, Smartphone, Tablet, Smart TV, etc.).

Continuando con la metodología CEH, luego de hacer la fase de obtención de información procederemos a la parte de explotación, para lo cual se observa

en la figura 25, que se intentó acceder al router con las credenciales por defecto admin/1234 , admin/admin , admin/ pero no hubo éxito.

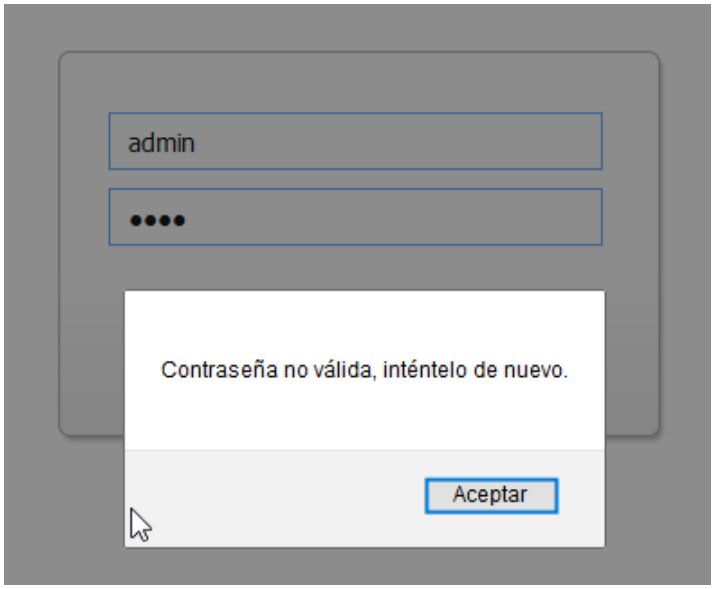


Figura 25. Panel de Login del Router

Para lo cual como primer vector de ataque consiste en hacer fuerza bruta a través del programa hydra[14]. Luego de la etapa de reconocimiento y detectar que existe un vector de ataque que es el login del panel de administración, se procederá a usar la herramienta hydra que es usada para obtener acceso a servidores, páginas web a través de fuerza bruta.

Hydra es una herramienta desarrollada para llevar ataques del tipo fuerza bruta de manera paralela y modular, se destaca en su uso por la rapidez en que realiza dichos ataques, el aplicativo permite llevar a cabo múltiples ataques a diferentes sistemas con diferentes usuarios.

Para ejecutar la herramienta Hydra, se necesita conocer varios parámetros entre los cuales tenemos. La IP del router al cual queremos atacar, un diccionario con nombres de usuario, un diccionario con una lista de contraseñas y el protocolo que se usará para conectarse.

En esta prueba de concepto, supondremos que el usuario es el que viene por defecto por lo cual omitiremos el diccionario de usuarios en la ejecución del comando.

[14] Hydra es un cracker de inicio de sesión de red en paralelo. Hydra funciona mediante el uso de un conjunto de métodos para descifrar contraseñas utilizando diferentes enfoques

El comando que usaremos es el siguiente:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt IPROUTER -s 8081 http-post-form
"/info/Login.html:admin_Username=^USER^&admin_Password=^PASS^:submit=logIn_
btn" -V -t 1
```

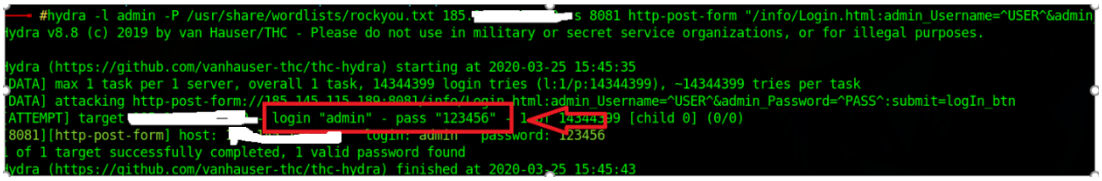


Figura 26. Descubriendo Usuario y Password del router

En la figura 26, se observa que, al primer intento, el ataque es exitoso encontrando el usuario/password correcto para acceder al router, mostrándonos que las credenciales correctas son usuario=admin y clave=123456. Luego de obtener las credenciales, se procede a verificar si estas son correctas, para lo cual se accede al panel de administración web ingresando el usuario y clave que acaba de crackear a través de fuerza bruta el programa medusa.

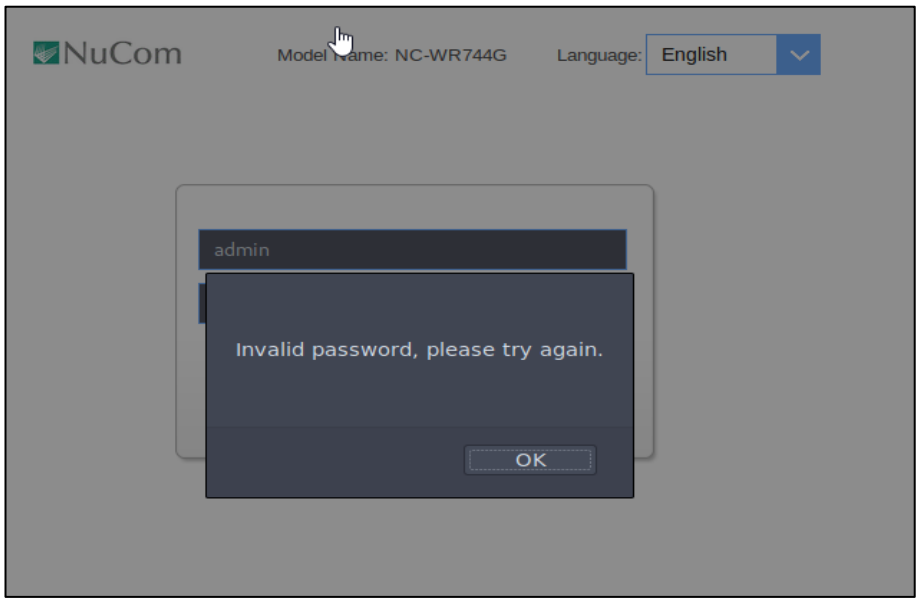


Figura 27. Credenciales Obtenidas Inválidas

Como se puede observar en la figura 27 al tratar de ingresar con las credenciales que nos daba validas el programa hydra nos muestra un error por lo cual, se ejecutará una segunda prueba con un diccionario diferente para comprobar que existe algún tipo de honeypot en el router.

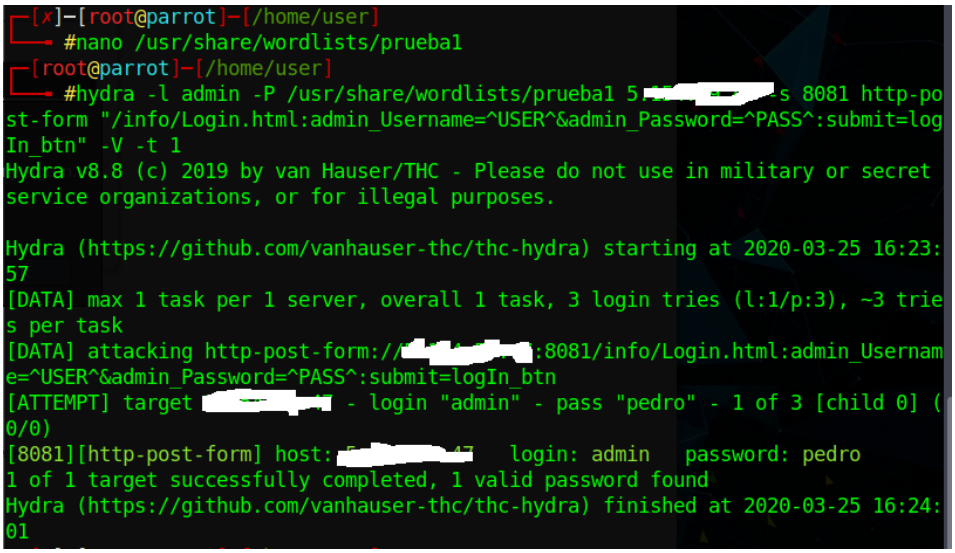


Figura 28. Ataque de fuerza bruta con un diccionario diferente

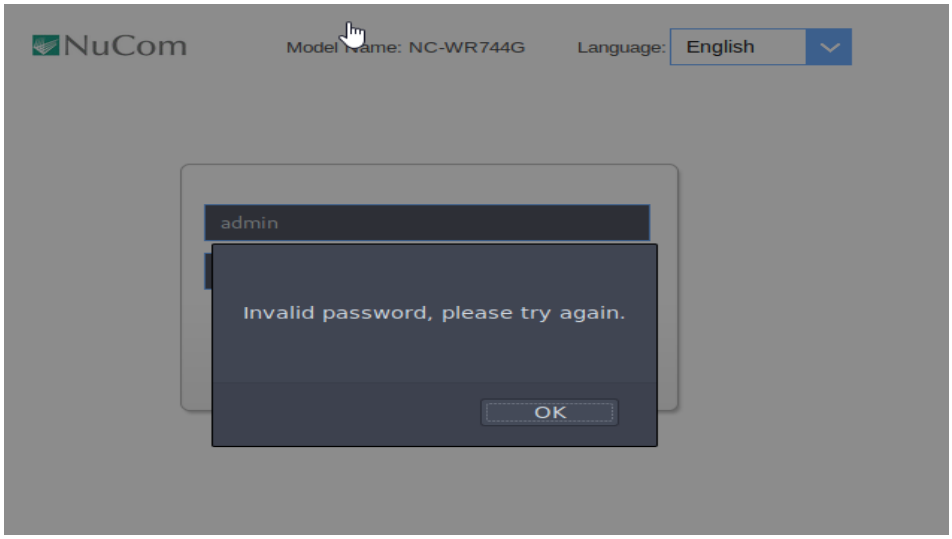


Figura 29. Credenciales Obtenidas Inválidas

Como se puede observar en la figura 28 y 29 respectivamente, el router tiene un mecanismo de protección de tipo Honeypot[15] ante este tipo de ataques ya que, al colocar un diccionario diferente, con la única palabra “pedro”, da por ataque correcto con credenciales admin/pedro lo cual es un error, es por lo cual se buscará otro vector de ataque.

Volviendo a la primera fase de la metodología CEH, buscaremos más información del router a través del software nmap que viene instalado por defecto en el sistema operativo ParrotOs, para lo cual ejecutaremos el

[15] En terminología informática, un honeypot es un mecanismo de seguridad informática configurado para detectar, desviar o, de alguna manera, contrarrestar los intentos de uso no autorizado de los sistemas de información.

siguiente comando el cual nos permitirá ver los servicios que se encuentran ejecutando en el router.

```
nmap -sV IPROUTER
```

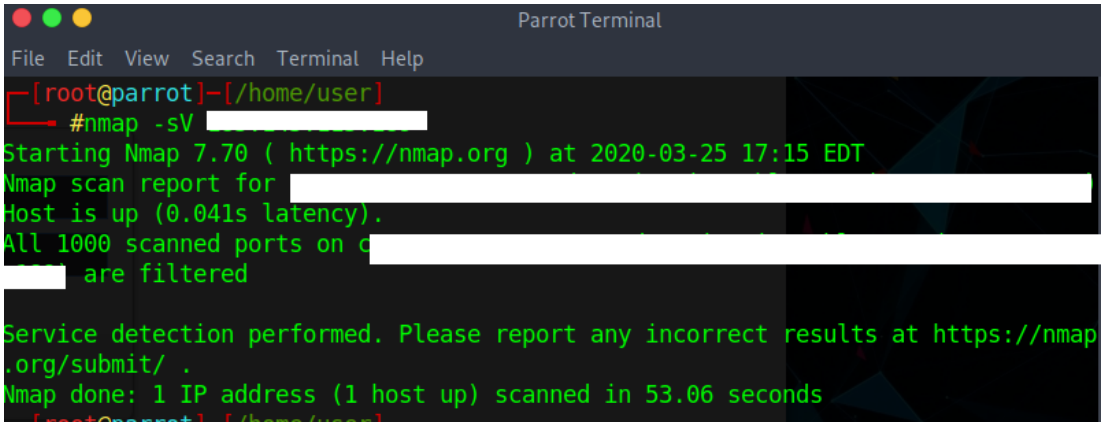


Figura 30. Resultado de la ejecución del comando

Como se puede observar en la figura 30 todos los puertos se encuentran filtrados, lo cual sucede cuando existe algún cortafuegos en el router lo cual no permite verificar los servicios corriendo en el mismo. Para lo cual se tratará de evadir el mismo con el siguiente comando.

```
nmap -Pn IPROUTER
```

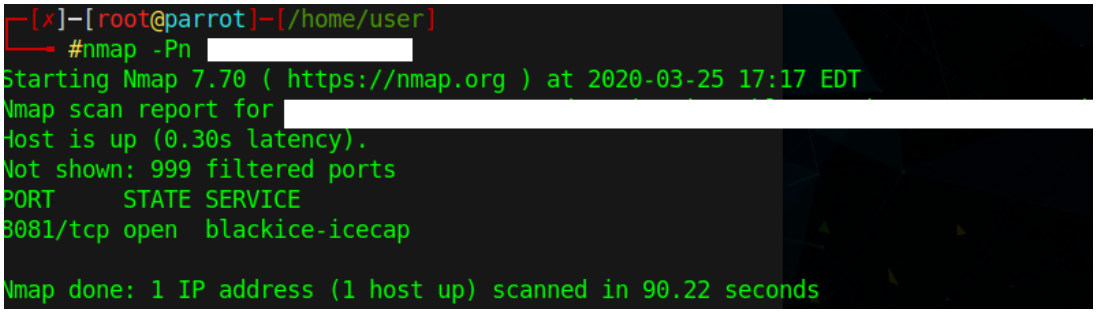


Figura 31. Resultado de la ejecución del comando

Nos muestra que existe el puerto 8081 abierto, este puerto por lo general se usa para correr WebServices, lo que nos hace suponer que se podrían conectar al mismo a través del servicio de telnet, por lo cual verificaremos si el servicio encuentra ejecutando en el puerto 23

```
telnet IPROUTER
```

Figura 32. Servicio de Telnet Ejecutándose

Al observar que el servicio se encuentra ejecutando, realizaremos el ataque por fuerza bruta a través del programa medusa. De igual manera que el escenario anterior, intentaremos con el usuario por defecto (root) por lo cual omitiremos el diccionario de usuarios.

```
medusa -u root -P /usr/share/wordlists/rockyou.txt -h IP ROUTER -M telnet
```

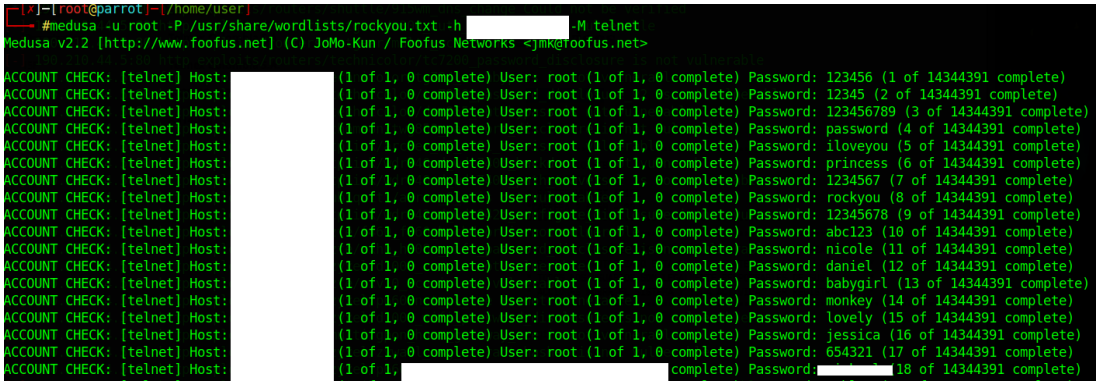


Figura 33. Credenciales obtenidas a través de fuerza bruta

Luego de obtener la clave a través de fuerza bruta, probamos las credenciales y observamos que podemos acceder a los archivos del router como se observa en la figura 34.

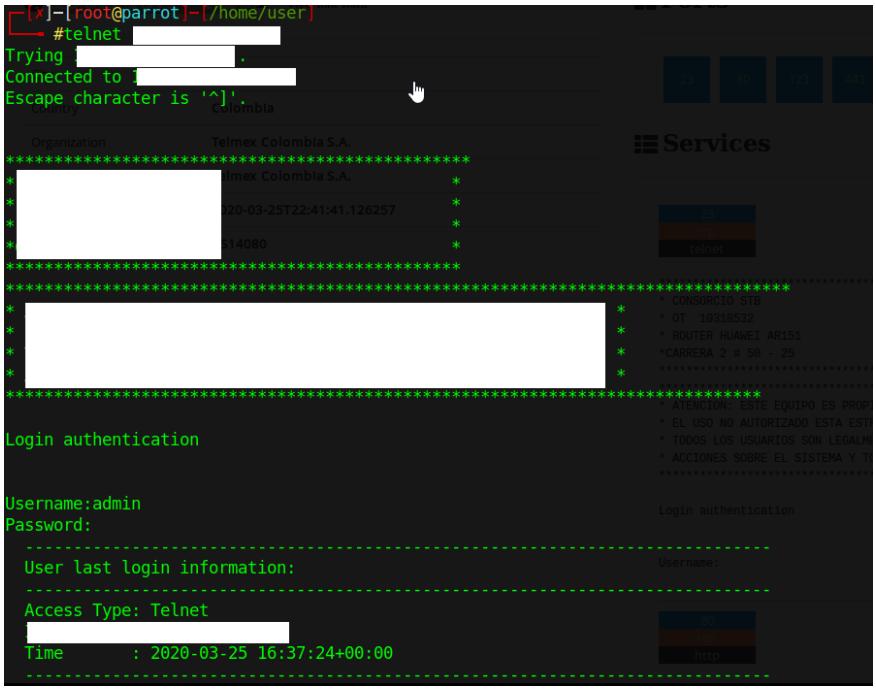


Figura 34. Acceso correcto al router a través de telnet

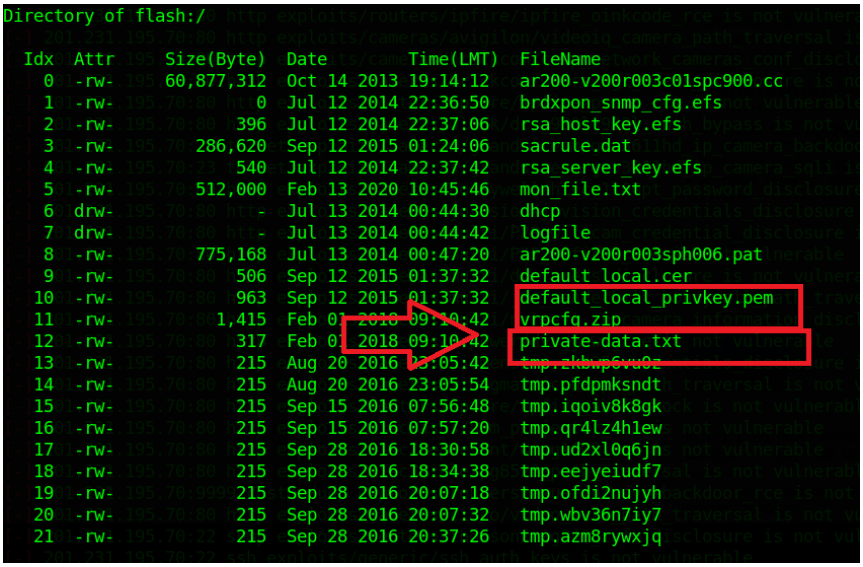


Figura 35. Archivos del router

Como podemos observar en la figura 35, existen varios archivos importantes dentro del router, entre los cuales uno llamado “datos privados” y una llave RSA para poder acceder al servidor a través de SSH lo cual nos daría acceso total a la red interna de la organización ya que se podría hacer pivoting[16] desde el router hacia otro equipo. Ya con persistencia en el dispositivo, el siguiente paso de un “ciberdelincuente” es poder expandirse por el sistema, buscar

[16] Pivoting es una técnica que Metasploit usa para enrutar el tráfico desde una computadora pirateada hacia otras redes a las que no puede acceder una máquina hacker. Otra red con el rango 10.10. 10.0 / 24.

dispositivos conectados a él con el fin de encontrar vulnerabilidades para poder hacerse con el control como por ejemplo un Active Directory, un servidor, una máquina industrial, el portátil del CEO para poder extorsionarle, o dispositivos de IoT como cámaras, sensores de luz, etc.

Medidas de prevención y Mitigación de ataques de fuerza bruta según metodología Owasp 2017

Como se mencionó en el apartado 4.2, los escenarios se realizaron usando la metodología OWASP 2017, por lo tanto, el vector de ataque de la primera prueba de concepto se encuentra explicado en el vector de ataque “A2:2017 Broken Authenticacion” el cual se especifica en la tabla 6. [3]

Vectores de ataque	La fuerza bruta es una manera de ingreso a los sistemas, ya que los atacantes tienen acceso a cientos de millones de combinaciones válidas de nombre de usuario y contraseña para poder adivinar las contraseñas, listas de cuentas administrativas predeterminadas, fuerza bruta automatizada
Debilidad de seguridad	La prevalencia de la autenticación interrumpida está muy extendida debido al diseño y la implementación de la mayoría de los controles de identidad y acceso.
Impactos en el negocio	Los atacantes pueden obtener acceso a unas pocas cuentas, o solo a una cuenta de administrador para comprometer el sistema. Como se explica en el caso práctico se obtuvo acceso a la cuenta de administrador, teniendo de esta manera todos los privilegios sobre el router y los dispositivos conectados en el mismo. Dependiendo del dominio de la aplicación, esto puede permitir el lavado de dinero, el fraude de la seguridad social y el robo de identidad, o revelar información altamente confidencial legalmente protegida
	• Implementar la autenticación de múltiples factores para evitar el relleno automatizado de

Prevención	credenciales, la fuerza bruta y los ataques de reutilización de credenciales robadas. • No usar credenciales predeterminadas, especialmente para usuarios administradores o servicios que se encuentren expuestos a internet. • Implementar comprobaciones de contraseñas débiles, como probar contraseñas nuevas o modificadas en una lista de las 10000 peores contraseñas principales. • Alinear las políticas de longitud, complejidad y rotación de las contraseñas con las pautas del NIST 800-63 B en la sección 5.1.1 para Secretos memorizados u otras políticas modernas de contraseñas basadas en evidencia. • Limitar o demorar cada vez más los intentos fallidos de inicio de sesión. [3]

Tabla 4. Vector de Ataque A2:2017 Broken Authenticacion [3]

4.2.1.2 Explotando vulnerabilidades en routers remotos

Según el portal bleepingcomputer, investigadores descubrieron sólo en Shodan unos 32.000 dispositivos vulnerables a estos fallos de seguridad y que prácticamente cualquier atacante puede aprovechar para incluir esos dispositivos en una botnet. Los modelos de los routers afectados son el ZYXEL P660HN-T1A y el Huawei HG532**,** TP-LINK además del chipset Realtek RTL81XX**.** [50]

En este caso de estudio, se usará una nueva técnica de hackeo a los routers remotos que es la explotación de vulnerabilidades conocidas no parcheadas, para lo cual se usará el Framework RouterSploit que es un marco de explotación de código abierto dedicado a dispositivos integrados , se compone de varios módulos que ayudan a las operaciones de prueba de penetración los cuales son los siguientes: [51]

- exploits: Son módulos que aprovechan las vulnerabilidades identificadas y obtienen acceso al sistema
- creds: El módulo está diseñados para probar las credenciales contra los servicios de red
- escáneres: El módulo comprueban si un objetivo es vulnerable a algún exploit[17]

Para el desarrollo de esta prueba de concepto se usará los siguientes componentes

- Router: TP-Link
- Sistema Operativo de Ataque: ParrotOs
- Framework de Explotación: RouterSploit

Luego de la instalación del framework vamos a ejecutar los siguientes comandos para ejecutar el scanner sobre el router para encontrar vulnerabilidades.

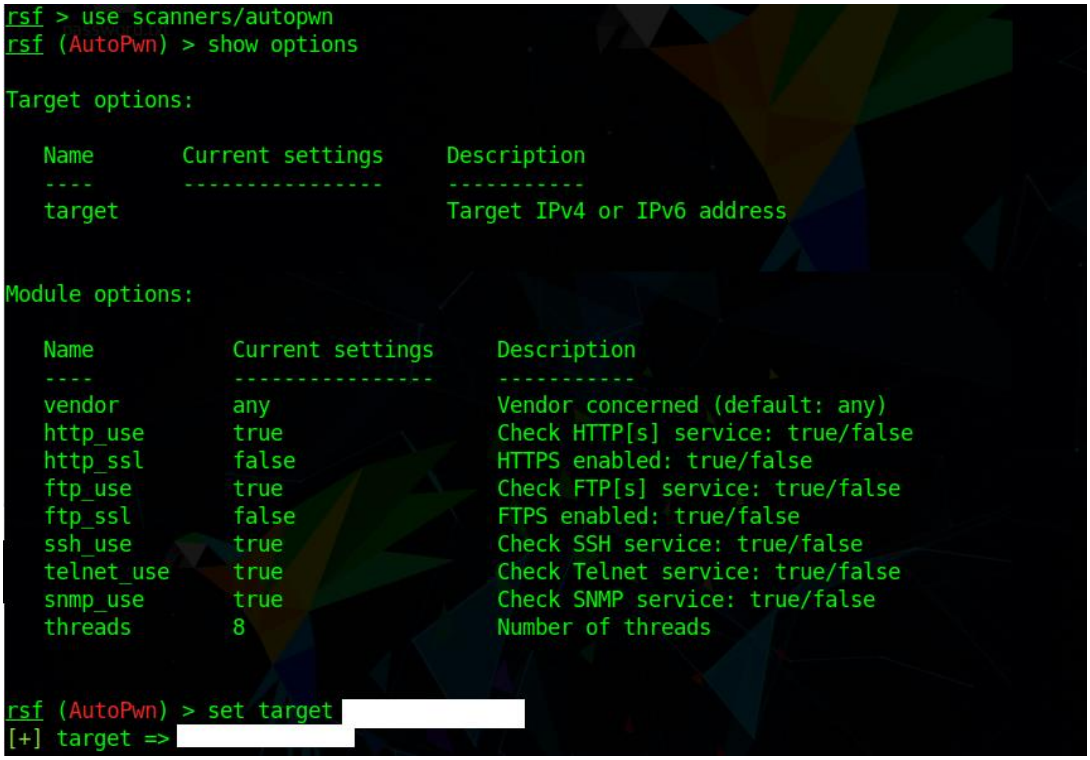


Figura 36. Ejecución del framework RouterSploit

[17] Código compilado que explota una vulnerabilidad en un sistema.

Explicación de los parámetros para la ejecución

```
use scanners/autopwn  // Usa el escáner del framework para buscar vulnerabilidades
show options  // muestra los parámetros necesarios para la ejecución
set target IP // Se agrega la IP del router remoto que va a ser analizado
run / Se ejecuta el escáner
```

En la figura 36 se muestra la ejecución del framework RouterSploit con los parámetros configurados y la IP del router agregada, en la figura 3 se puede observar que se encuentra encerrado en un recuadro rojo las vulnerabilidades posiblemente explotables .

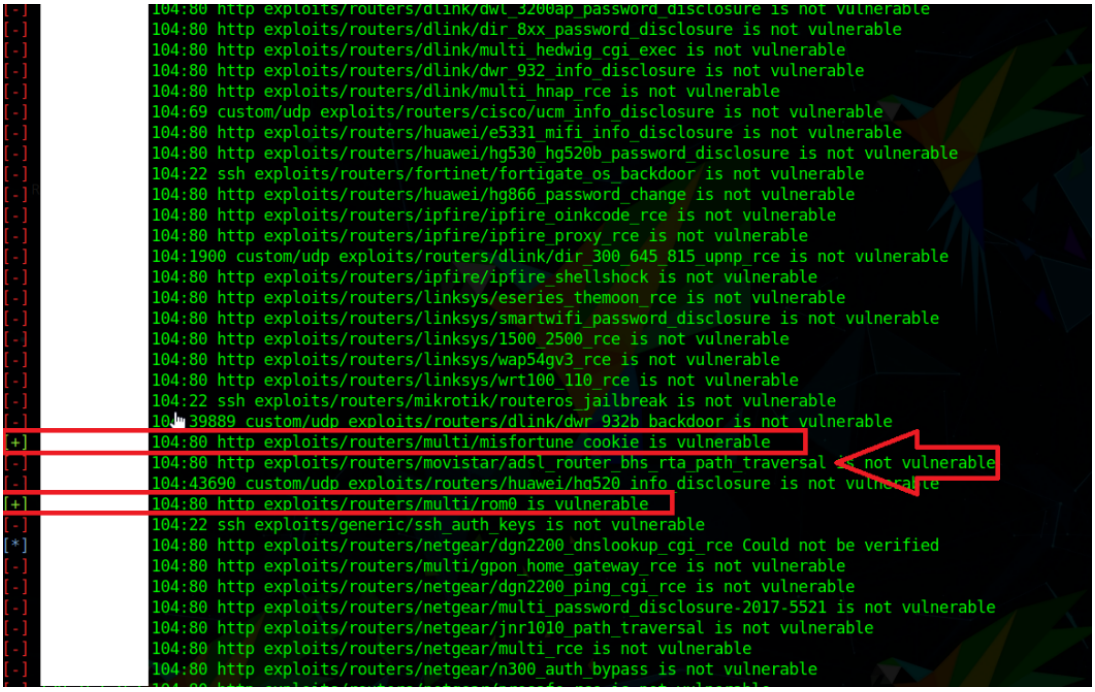


Figura 37. Vulnerabilidades encontradas en el router

Vulnerabilidad de rom0

Esta vulnerabilidad permite a un atacante remoto obtener fácilmente el control de su enrutador y conexión a Internet. El atacante puede utilizar de forma remota una solicitud HTTP GET al URI "/ rom-0 para descargar el archivo de copia de seguridad ROM-0 de su enrutador sin ser autenticado, y acceder a todos los datos importantes y privados almacenados en el router, su usuario/contraseña de inicio de sesión, su contraseña de Wi-Fi , y sus datos de configuración. Esta vulnerabilidad está presente en muchos dispositivos de red que usan RomPager Embedded Web Server. [52] [53]

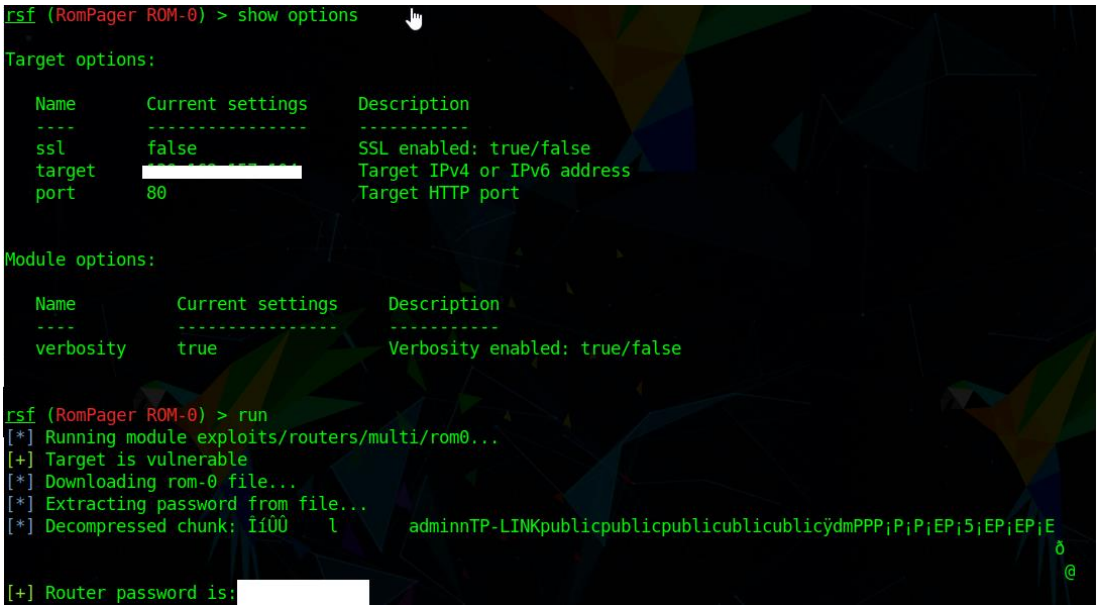


Figura 38. Ejecución exitosa del xploit y obtención de la contraseña

Como se observa en la figura 38, se ejecutó de manera exitosa el xploit “/exploits/routers/multi/rom0” obteniendo el password del router luego de hacer una petición HTTP a la URI “iprouter/ rom-0” obteniendo el archivo con todos los datos sensibles , entre ellos la clave del router.

Para probar que la contraseña obtenida sea correcta, se procede a acceder a la consola de administración web con las credenciales obtenidas, en la figura 39 se observa cómo se pudo entrar a través de la interfaz web al router, pudiendo observar todos los dispositivos conectados y a toda la configuración del router.

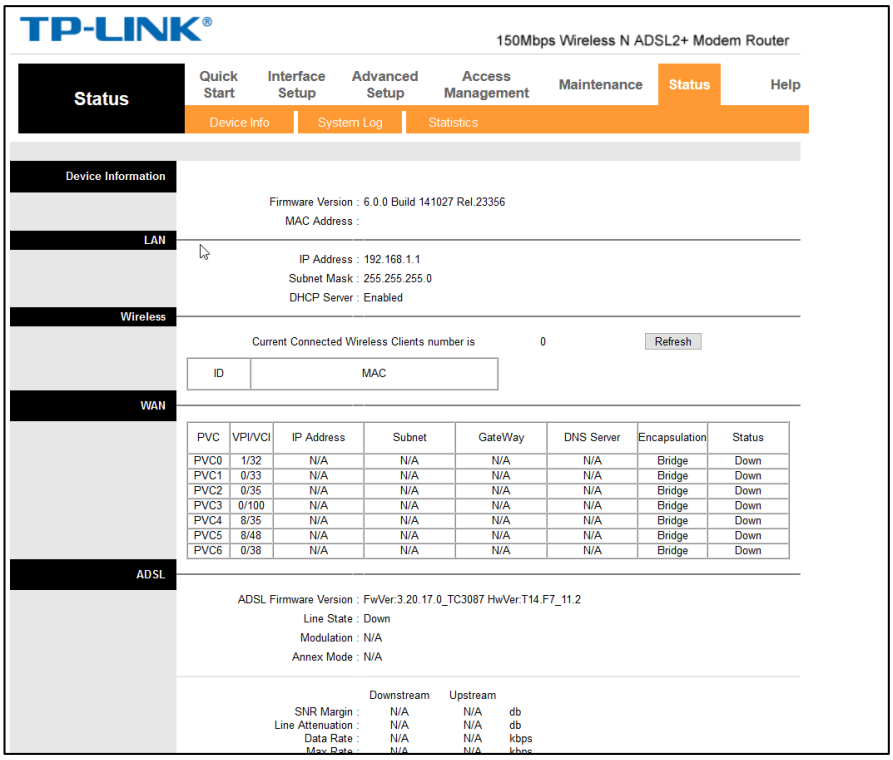


Figura 39. Consola de Administración del router

Al explotar esta vulnerabilidad y poder conocer la contraseña del router, el atacante puede ejecutar una ataque de DNS Spoofing[18], el cual consiste en cambiar el DNS del router por unas falsas para redirigir sus usuarios conectados a páginas fraudulentas y así robar credenciales de otras plataformas web o incluso, realizar una estafa bancaria. El atacante también puede exponer la LAN[19] a Internet, acceder a sus servicios internos o computadoras conectadas al abusar de las funciones de reenvío de puertos

Medidas de prevención y mitigación de ataques de explotación de vulnerabilidades según OWASP 2017.

Como se analizó en el escenario anterior, el router no poseía las actualizaciones necesarias para parchar las vulnerabilidades, ni la configuración correcta de seguridad, este tipo de ataques se encuentran explicados en el vector de ataque “A6:2017 Security Misconfiguration” el cual se especifica en la tabla 6. [3]

[18] La falsificación de DNS, también conocida como envenenamiento de la caché de DNS, es una forma de piratería informática de seguridad en la que los datos corruptos del Sistema de nombres de dominio se introducen en la caché del resolutor DNS, lo que hace que el servidor de nombres devuelva un registro de resultados incorrecto.

[19] Red de Área Local

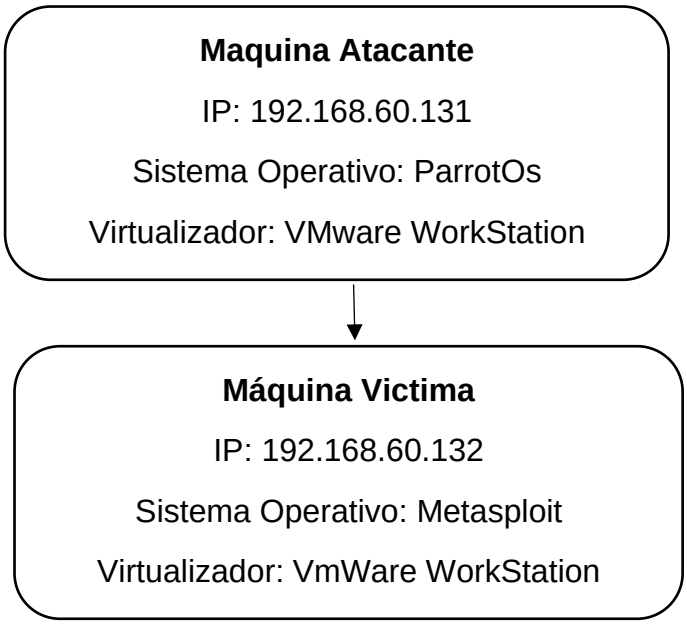
Vectores de ataque	Los atacantes a menudo intentan explotar fallas no parcheadas o acceder a cuentas predeterminadas, páginas no utilizadas, archivos y directorios desprotegidos, para obtener acceso no autorizado o al sistema.
Debilidad de seguridad	La configuración incorrecta de seguridad puede ocurrir en cualquier nivel de una pila de aplicaciones, incluidos los servicios de red, plataforma, servidor web, servidor de aplicaciones, base de datos, marcos, código personalizado y máquinas virtuales, contenedores o almacenamiento preinstalados. Los escáneres automáticos son útiles para detectar configuraciones incorrectas, el uso de cuentas o configuraciones predeterminadas, servicios innecesarios, opciones heredadas, etc.
Impactos en el negocio	Tales fallas frecuentemente dan a los atacantes acceso no autorizado a algunos datos del sistema o funcionalidad. Ocasionalmente, tales fallas resultan en un compromiso completo del sistema. El impacto empresarial depende de las necesidades de protección de la aplicación y la sensibilidad de los datos.
Prevención	• Actualización del firmware que solucione las vulnerabilidades, para los dispositivos que lo tengan disponible. • Configurar las Listas de Control de Acceso (ACL) para que el equipo pueda ser accedido sólo desde las direcciones electrónicas que correspondan. • No utilizar el Servicio de DNS incluido en los enrutadores vulnerables.

Tabla 5 Medidas de Prevención y Mitigación[3]

4.2.2 Caso de estudio #2: Atacando equipos de la red interna de una organización

4..2.2.1 Explotando versiones vulnerables de servicios en ejecución

En el siguiente caso de estudio, se plantea el escenario que luego de obtener acceso al router por lo tanto a la clave del Wifi como se observó en el caso de estudio #1, se podría realizar un ataque a la red interna de una Casa Inteligente, para lo cual se plantea la siguiente prueba de concepto con los siguientes componentes.



Siguiendo la metodología de CEH, el primer paso es obtener información de los dispositivos que se encuentran en la red interna, sensores, cámaras, impresoras a través de los cuales se podría obtener información valiosa. Para lo cual usaremos la herramienta nmap en un escaneo pasivo con el siguiente comando el cual no permite escanear toda la subnet de la red y obtener los servicios que se están ejecutando en cada uno de los dispositivos

```
Nmap -sV 192.168.60.1/24
```

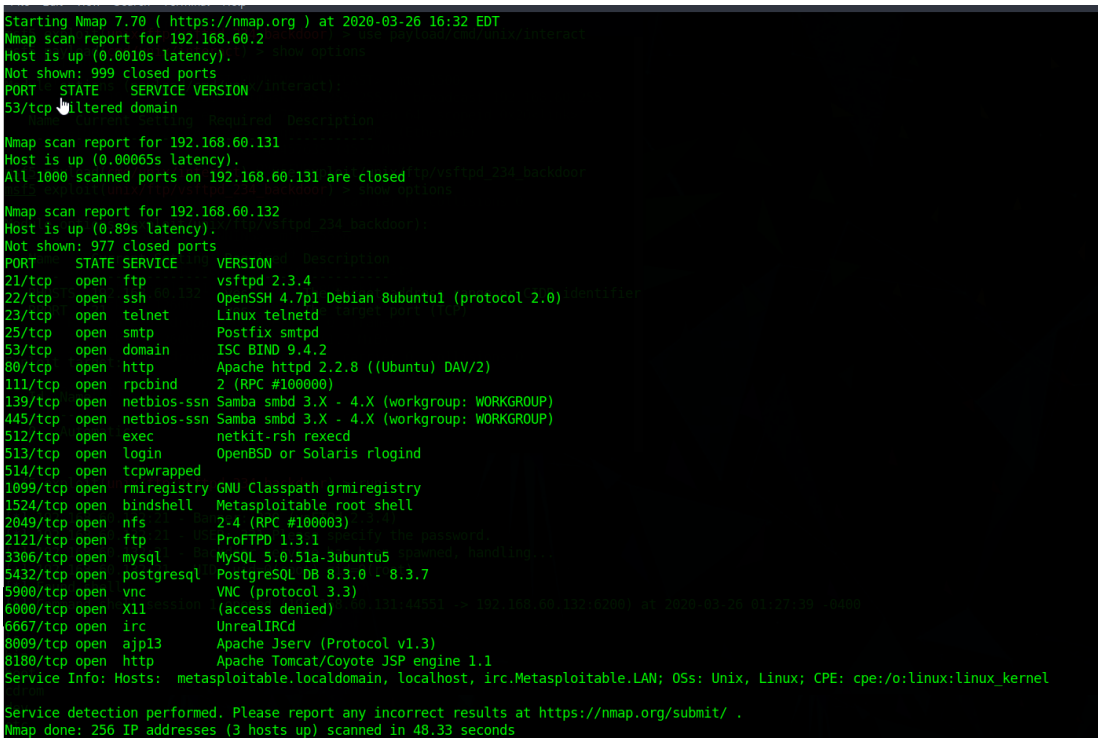


Figura 40. Dispositivos encontrados en la red y los servicios que están ejecutando

Como se puede observar en la figura 40 se detectó un equipo activo en la red interna con la IP “192.168.60.132” el cual tiene ejecutando varios servicios, los mismos que son un potencial vector de ataque, ya que si el atacante los puede vulnerar alguno, podría acceder a información confidencial dentro de esa máquina. Luego de verificar los servicios en ejecución, para la siguiente prueba de concepto se aprovechará la vulnerabilidad de la versión del servicio ftp[20] para poder acceder al sistema, para lo cual usaremos el framework Metasploit[21].

Detalles de la Vulnerabilidad de puerta trasera “Vsftpd”

El Protocolo de transferencia de archivos (FTP) es un protocolo de red estándar utilizado para la transferencia de archivos de computadora entre un cliente y un servidor en una red de computadoras. FTP se basa en una arquitectura modelo cliente-servidor que utiliza conexiones de control y datos separadas entre el cliente y el servidor. Los usuarios de FTP pueden

[20] Protocolo para la transferencia de archivos

[21] El Proyecto Metasploit es un proyecto de seguridad informática que proporciona información sobre vulnerabilidades de seguridad y ayuda en pruebas de penetración y desarrollo de firmas IDS.

autenticarse con un protocolo de inicio de sesión de texto sin cifrar, normalmente en forma de nombre de usuario y contraseña, pero pueden conectarse de forma anónima si el servidor está configurado para permitirlo.[54]

El término “vsftpd”, significa "Daemon FTP muy seguro", es un servidor FTP para sistemas basados en UNIX, incluido Linux. Está licenciado bajo la Licencia Pública General de GNU y es compatible con IPv6 y SSL [55]. Para la explotación de la esta vulnerabilidad usaremos el framework Metasploit, para lo cual ejecutaremos los siguientes comandos como se observa en la figura 41 y 42 respectivamente:

Detalle de los comandos ejecutados en Metasploit.

Msfconsole // se ejecuta el framework.

Use exploit/unix/ftp/vsftpd_234_backdoor // Se hace un llamado el exploit que explota esta vulnerabilidad.

set rhosts 192.168.62.132 // Se agrega la IP de la máquina vulnerable que descubrimos en primera instancia.

use payload/cmd/unix/interact // se pone en escucha un listener, ya que si el exploit se ejecuta correctamente obtendrá una shell reversa.

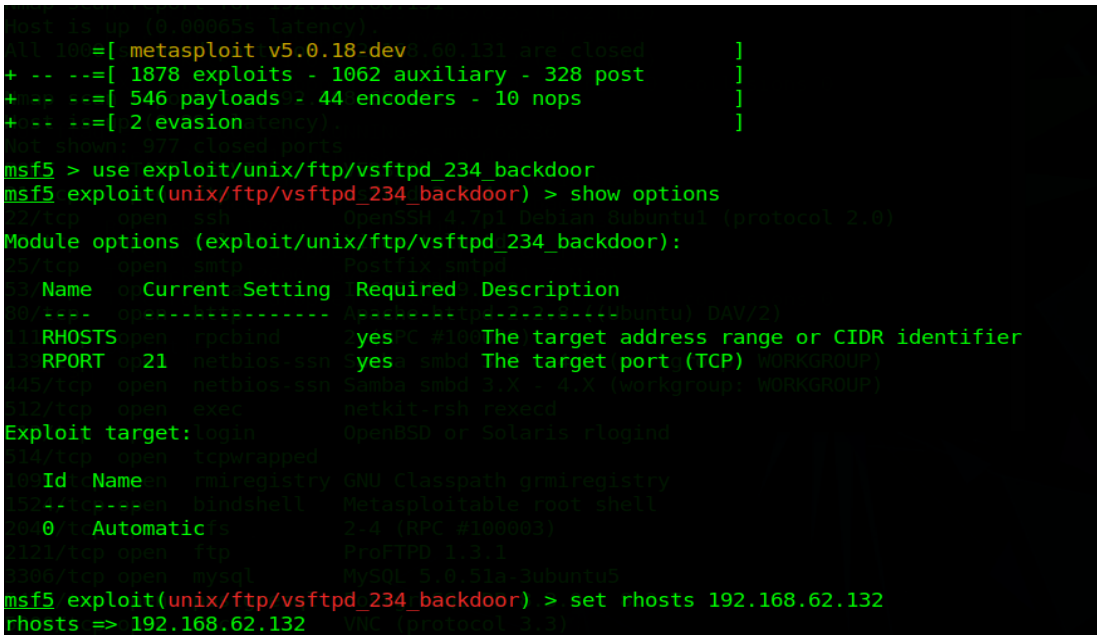


Figura 41. Configuración de parámetros necesarios para la ejecución del exploit

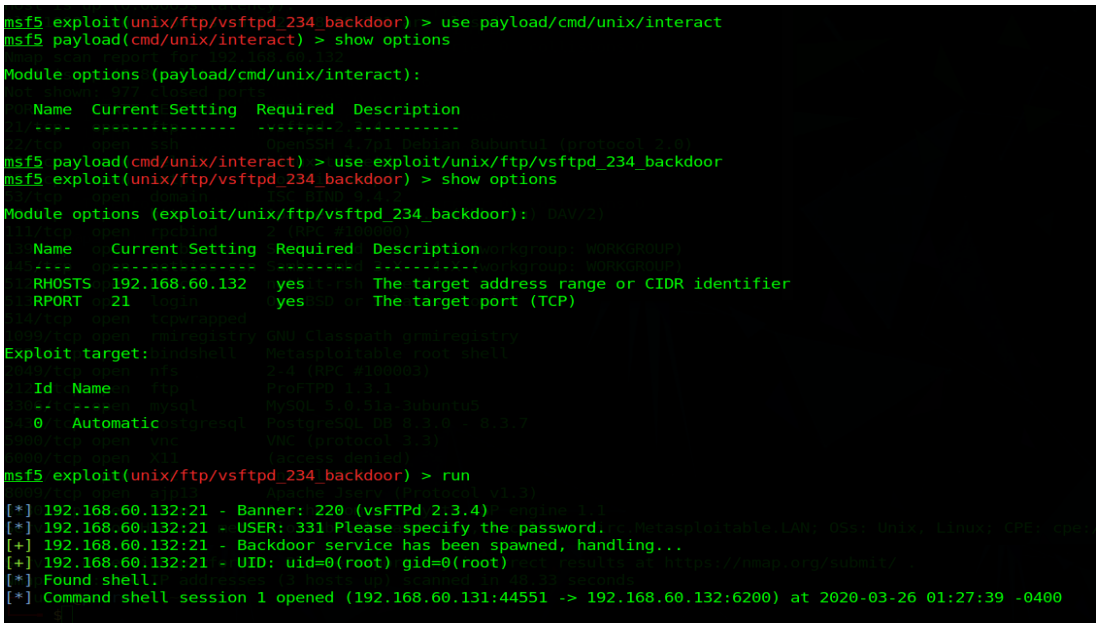


Figura 42. Ejecución del listener para la creación de la shell interactiva

Como se observar en la figura 42, la ejecución del exploit fue exitosa y se obtuvo una sesión con privilegios de Super Usuario en la máquina víctima y de esta manera se tiene acceso a toda la información del sistema como se observa en la figura 43.

Figura 43. Verificación de privilegios en la shell obtenida.

Figura 44. Sistema de Archivos de la máquina comprometida

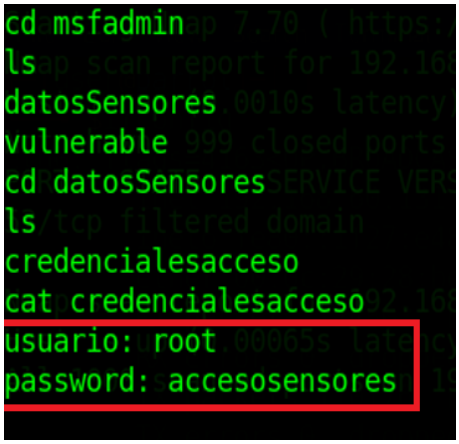


Figura 45. Descubriendo información confidencial

Como se puede observar en la figura 44 y 45 respectivamente, a través de la explotación de la vulnerabilidad “Vsftpf 2.3.4” en la computadora víctima se logró obtener información confidencial, en este caso dentro de la carpeta de msfadmin , se encontró una carpeta llamada “datosSensores” , en la misma había un archivo llamado “credencialesacceso” el mismo que contenía los datos de acceso a un panel de sensores que se encontraban hosteados en la nube en el servidor WeatherLink como se observa en la figura 46 .

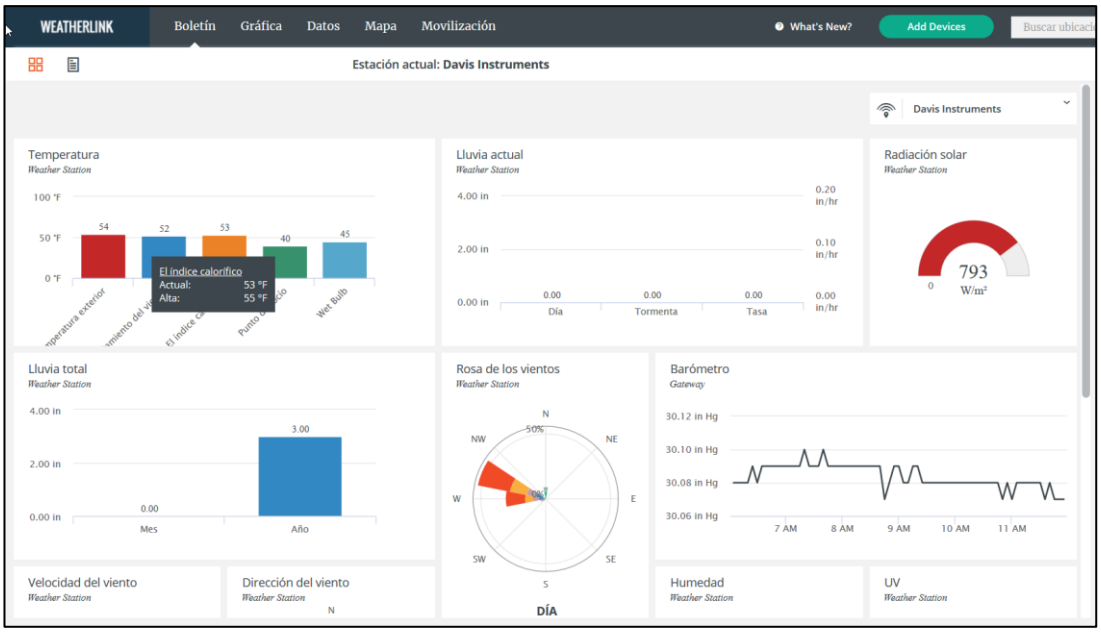


Figura 46. Ingreso al panel de sensores, a través de las credenciales obtenidas

Medidas de prevención y Mitigación

Los ataques que se desarrollan a infraestructuras que no cuentan con la actualización de parches de seguridad o actualización de servicios expuestos a internet, se encuentran explicados en el vector de ataque “A9:2017 Using Componentes with Known Vulnerabilities” el cual se detalla en la tabla 7. [3]

Vectores de ataque	Los servicios que están expuestos a internet y no poseen las medidas mínimas de seguridad, son blancos fáciles a diferentes tipos de ataques , ya que es fácil encontrar exploits ya escritos para muchas vulnerabilidades conocidas.
Debilidad de seguridad	La prevalencia de este problema está muy extendida. Los patrones de desarrollo con muchos componentes pueden hacer que los equipos de desarrollo ni siquiera comprendan qué componentes usan en su aplicación o API, y mucho menos mantenerlos actualizados
Impactos en el negocio	Si bien algunas vulnerabilidades conocidas provocan solo impactos menores, algunas de las violaciones más grandes hasta la fecha se han basado en la

	explotación de este tipo de vulnerabilidades conocidas. Dependiendo de los activos que esté protegiendo la organización, tal vez este riesgo debería estar en la parte superior de la lista.
Prevención	• Elimine dependencias no utilizadas, características innecesarias, componentes, archivos y documentación. • Hacer un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor (por ejemplo, marcos, bibliotecas) y sus dependencias. • Suscribirse a las alertas por correo electrónico para conocer las vulnerabilidades y actualizaciones de seguridad relacionadas con los componentes que utiliza. • Supervisar las bibliotecas y los componentes que no están mantenidos o que no crean parches de seguridad para versiones anteriores. Si no es posible aplicar parches, considere implementar un parche virtual para monitorear, detectar o proteger contra el problema descubierto.

Tabla 6 Vector de Ataque A9:2017 Using Componentes with Known Vulnerabilities[3]

El vector de ataque A9:2017 Using Componentes with Known Vulnerabilities es uno de los vectores de ataque más críticos contra los que protegerse en un entorno de IoT. Si el administrador no conoce las versiones utilizadas de los componentes, genera un riesgo considerable en la infraestructura , es decir cualquier componente desactualizado genera una posible ruta de ataque para intrusos.

4.2.3 Caso de estudio #3: Atacando controladores de acceso VertX

HID es uno de los fabricantes de sistemas de control de acceso más grandes del mundo y se ha convertido en una parte omnipresente de la postura de seguridad física de muchas grandes empresas, los controladores HID se encuentran en los aeropuertos, campus universitarios, hospitales, complejos gubernamentales o edificio de oficinas. Estos controladores poseen lectores de tarjetas está conectado a un controlador de puerta detrás de escena, que es un dispositivo que controla todas las funciones de la puerta, incluidos el bloqueo y desbloqueo, horarios, alarmas, etc.

En los últimos años, estos controladores de puerta han recibido interfaces de red para que puedan administrarse de forma remota, lo cual es muy útil para enviar actualizaciones y cronogramas de la base de datos de tarjetas, pero como con todo lo demás en la red, existe el riesgo de vulnerabilidades explotables de forma remota.

Las dos líneas principales de controladores de puertas de HID son sus plataformas VertX y Edge, para que estos controladores se integren fácilmente en las configuraciones de control de acceso existentes, tienen un servicio de descubrimiento que responde a un paquete UDP en particular. Un sistema de administración remota puede transmitir una sonda de descubrimiento al puerto 4070, y todos los controladores de puerta en la red responderán con información como su dirección MAC, tipo de dispositivo, versión de firmware e incluso un nombre común.

Aunque parezca una función inofensiva, al momento de intentar vulnerar estos dispositivos, los atacantes obtienen mucha información de los mismos, para lo cual en el caso de estudio #3, vamos a usar una herramienta llamada Shodan Eye.

Esta herramienta recopila toda la información sobre todos los dispositivos que están directamente conectados a Internet con las palabras clave especificadas, los tipos de dispositivos indexados pueden variar enormemente: desde computadoras de escritorio pequeñas, refrigeradores hasta plantas de energía nuclear y todo lo demás.

Es necesario hacer énfasis que se debe ingresar el ApiKey Shodan para poder ejecutar esta herramienta, en la figura 47 se observa la ejecución de la

herramienta con la palabra de identificación “HID VertX” que buscará en Shodan e Internet los dispositivos que respondan a esta búsqueda y los guardará en un archivo de texto.

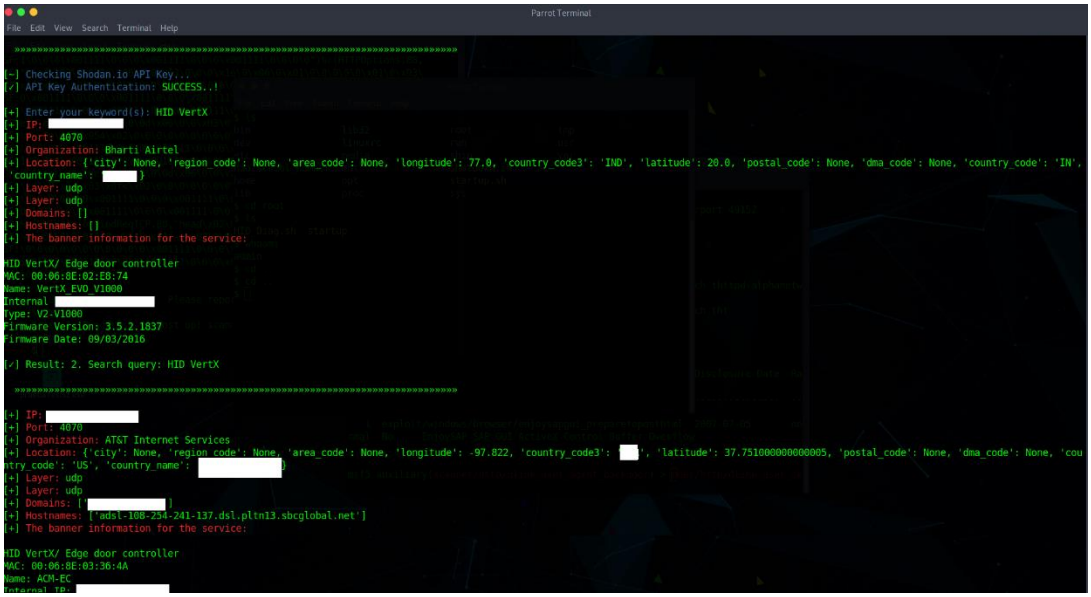


Figura 47. Resultados de la ejecución de EyeShodan

La ejecución del comando nos mostró un total de 101 resultados de dispositivos que coinciden con la palabra clave “HID VertX”, este descubrimiento se realiza mandando un mensaje udp al puerto 4070 haciendo que estos dispositivos respondan con datos tales como: Organización Localización, Dominios , Nombres de Host , Dirección Mac , Nombre , Ip Interna , Firmware como se observa en la figura 47.

Luego de obtener estos datos, para el caso de estudio, se intentará ingresar en la consola de administración para lo cual primero se probará con las claves por defecto admin/admin, admin/1234, admin/123456. Como se puede observar en la figura 48, el login al panel de administración se encontraba por defecto con las claves admin / empty, permitiendo acceder a la configuración del controlador. Desde la consola de administración se puede realizar acciones como abrir, cerrar modificar la configuración completa del controlador como se ve en la figura 48 ,49 respectivamente.

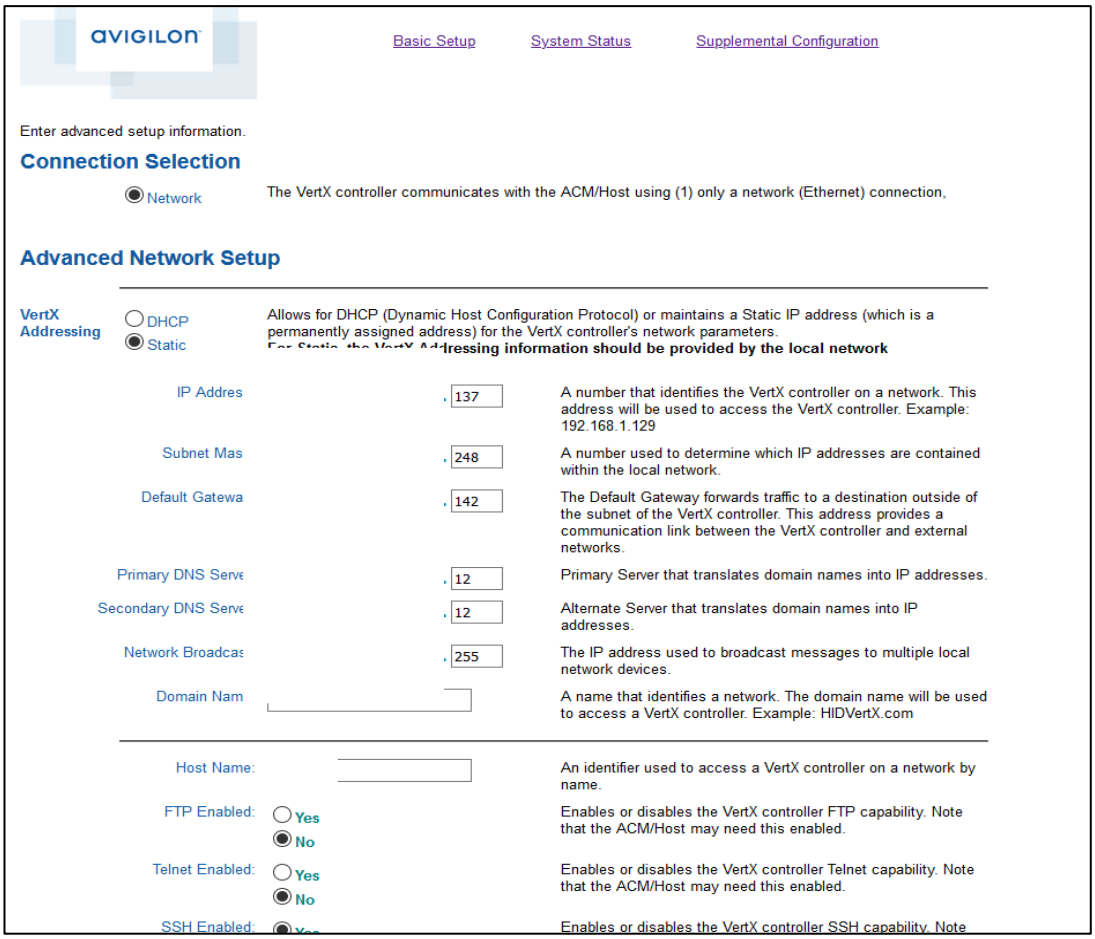


Figura 48. Configuraciones de Red del Controlador

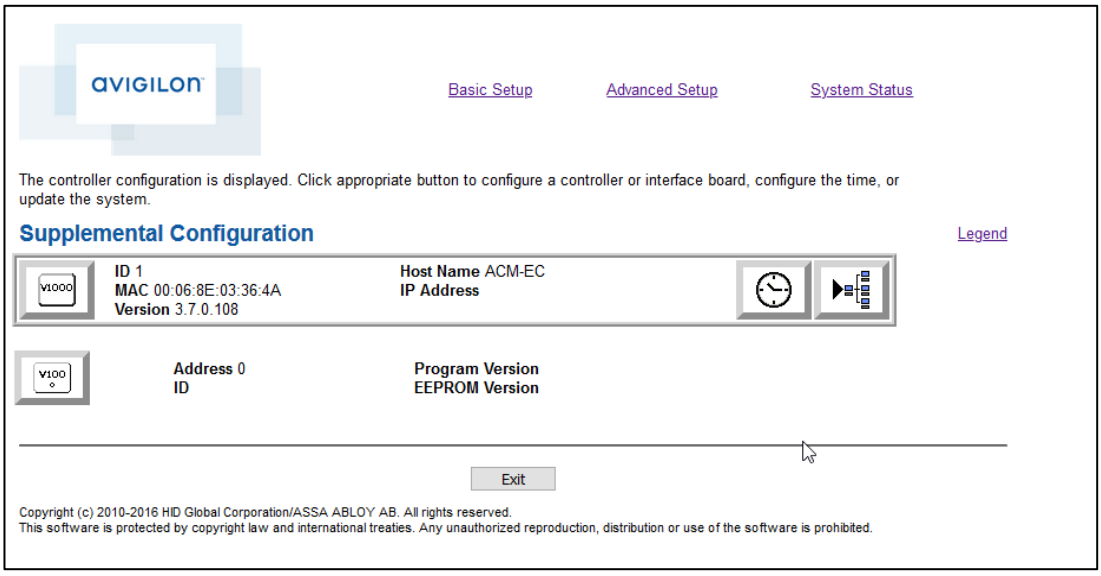


Figura 49 , Panel de Servicios

Como se puede observar en la figura 48 , se encuentra habilitado el servicio de SSH para el dispositivo , para lo cual se hará un escaneo con la herramienta nmap para confirmar que el servicio está en ejecución.

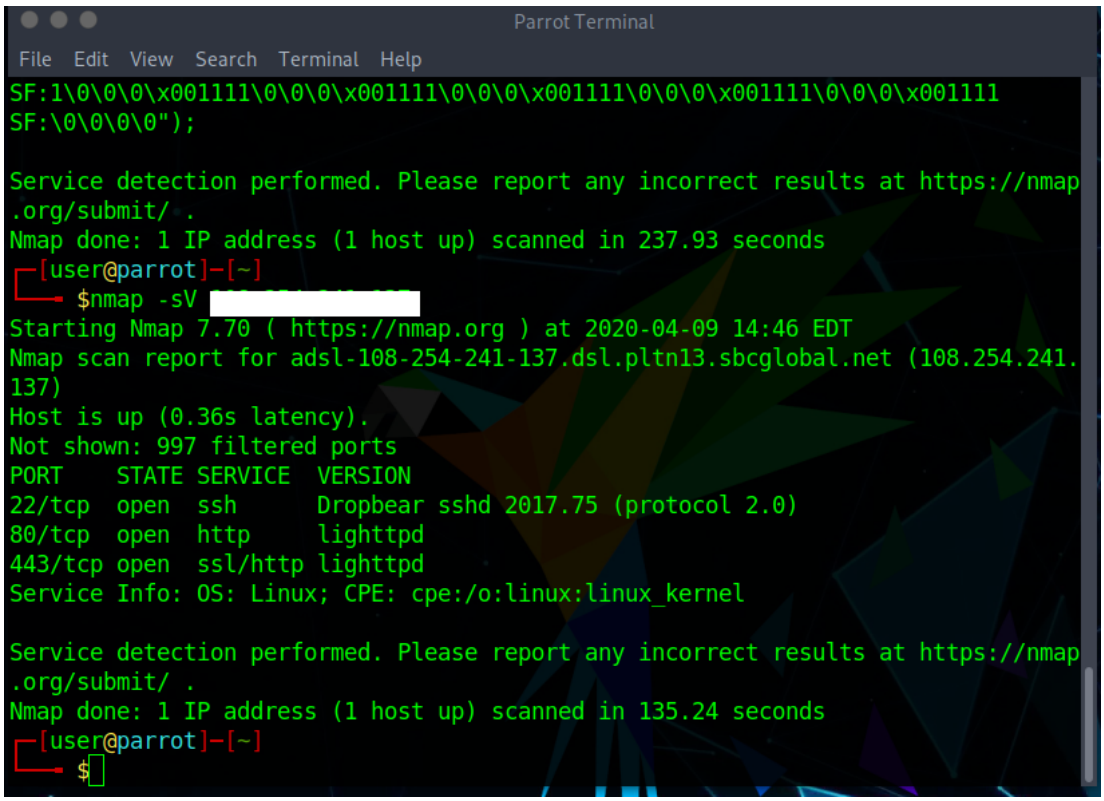


Figura 50. Descurbiendo Servicios activos en el dispositivo

Como se puede observar en la figura 50, efectivamente en el dispositivo HIV está ejecutando el servicio SSH, al cual nos conectaremos con las credenciales por defecto como se puede observar en la figura 51.

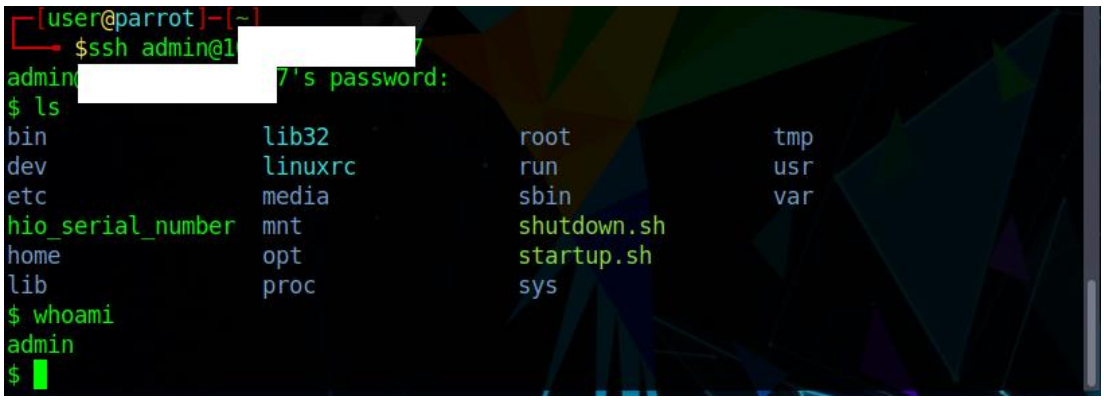


Figura 51 Conexión por SSH a el controlado HID

Como se puede observar en la figura 51, la conexión fue exitosa con el controlador a través del protocolo ssh con privilegios de administrador. La conexión mediante ssh permite al atacante la ejecución de archivos .sh, lo

cual posibilita al atacante ejecutar algún tipo de Malware para infectar a este dispositivo y hacerlo parte de una botnet como se analizará en el caso de estudio #4 de este trabajo.

Las medidas de prevención y mitigación de este tipo de ataques son las mismas que se contempla en el caso de estudio #1 en el apartado 4.2.1.1 por lo que no se creyó conveniente agregarlas nuevamente .

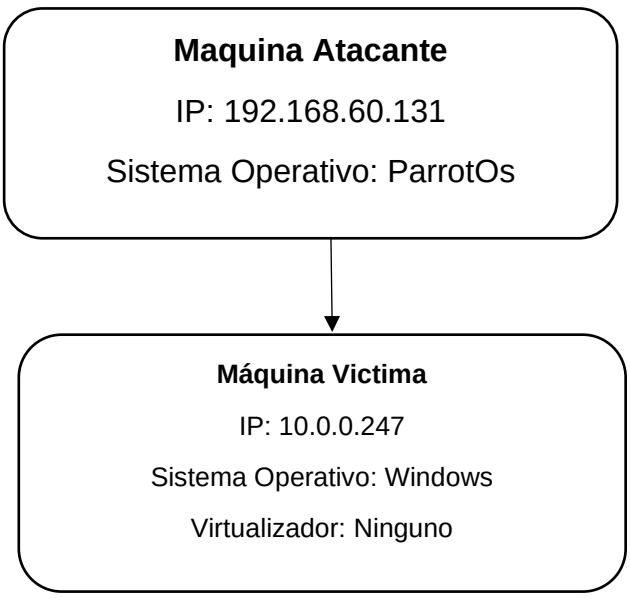
4.2.4 Caso de estudio #4: Criptomining con Botnets.

Antecedentes:

La minería de criptomonedas con Botnets está haciendo millones para sus creadores al infectar secretamente varios dispositivos en todo el mundo. A principios de febrero del año 2019, más de medio millón de dispositivos informáticos fueron secuestrados por una botnet minera de criptomonedas llamada Smominru, lo que obligó a los diversos dispositivos a extraer casi 9,000 criptomonedas Monero sin el conocimiento de los propietarios de los dispositivos, según el portal de tecnología ZDNet.

Escenario

Para el escenario #3 se realizará la instalación y configuración de una botnet en un sistema operativo Linux, posteriormente se procederá a infectar un sistema operativo Windows y se realizará un análisis de todos los tipos de ataque que se pueden desarrollar al equipo infectado, haciendo principal énfasis en el minado de criptomonedas a través de la botnet.



La botnet que se usará para esta prueba de concepto se denomina BYOB que es un proyecto que fue implementado para investigadores y desarrolladores de seguridad. Esta herramienta está diseñada para implementar algunas características de otras Botnets según el requisito que se necesite; la demostración de la instalación y ejecución de esta herramienta está hecha en ParrotOs.

Pasos para la instalación y ejecución de la botnet BYOB

1. Primero se procede a clonar el repositorio de la botnet a nuestro servidor Linux

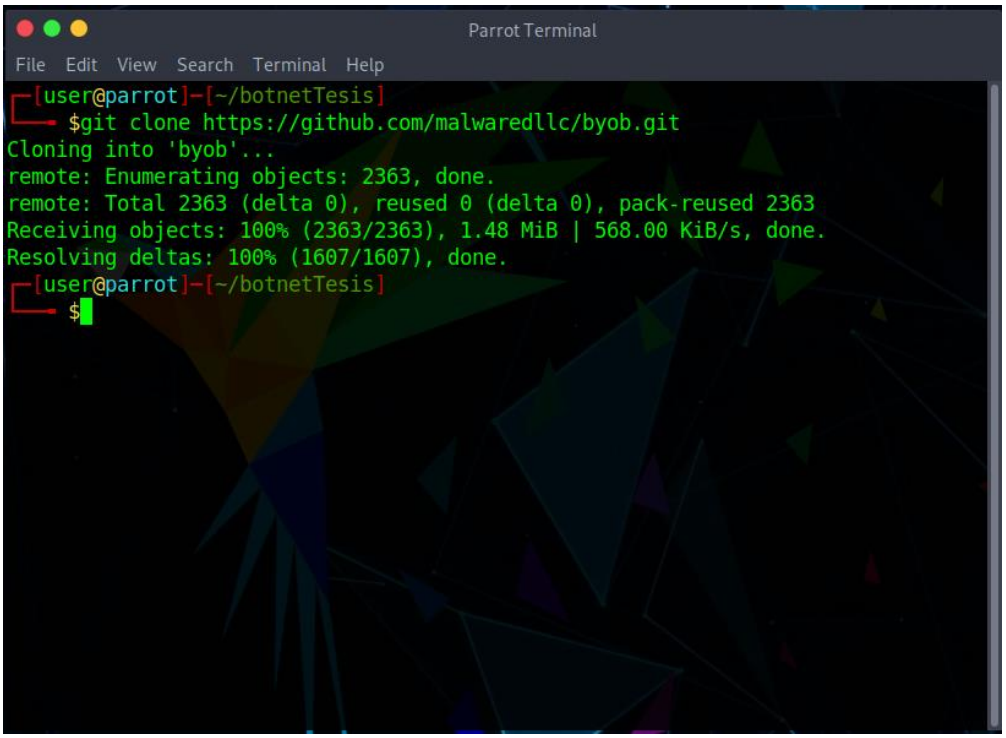


Figura 52 . Clonado del repositorio de la botnet en el servidor Linux

2. Una vez clonado el repositorio se procederá a instalar los requerimientos para el funcionamiento de la botnet

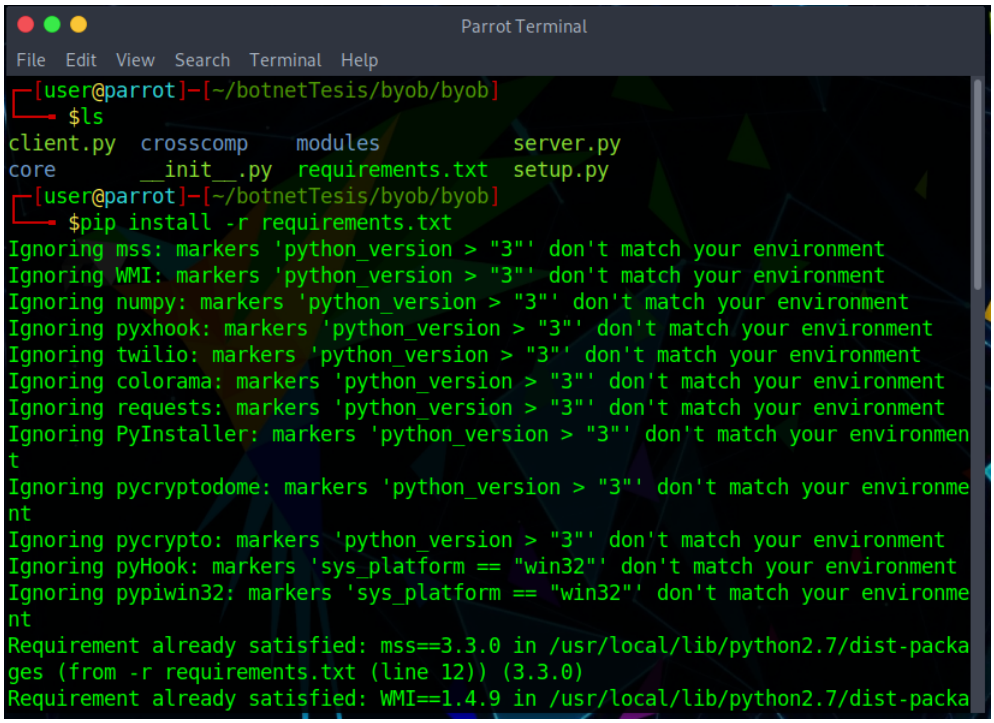


Figura 53 Instalación de los requerimientos para la botnet

3. Luego de realizar la instalación de las dependencias y librerías, se procede a ejecutar la botnet, para lo cual se usarán dos terminales, el primer terminal será el Servidor Bot donde se manejarán las sesiones y el segundo terminal el Cliente Bot donde se creará el payload para infectar a los usuarios. Para lo cual primero iniciaremos el servidor

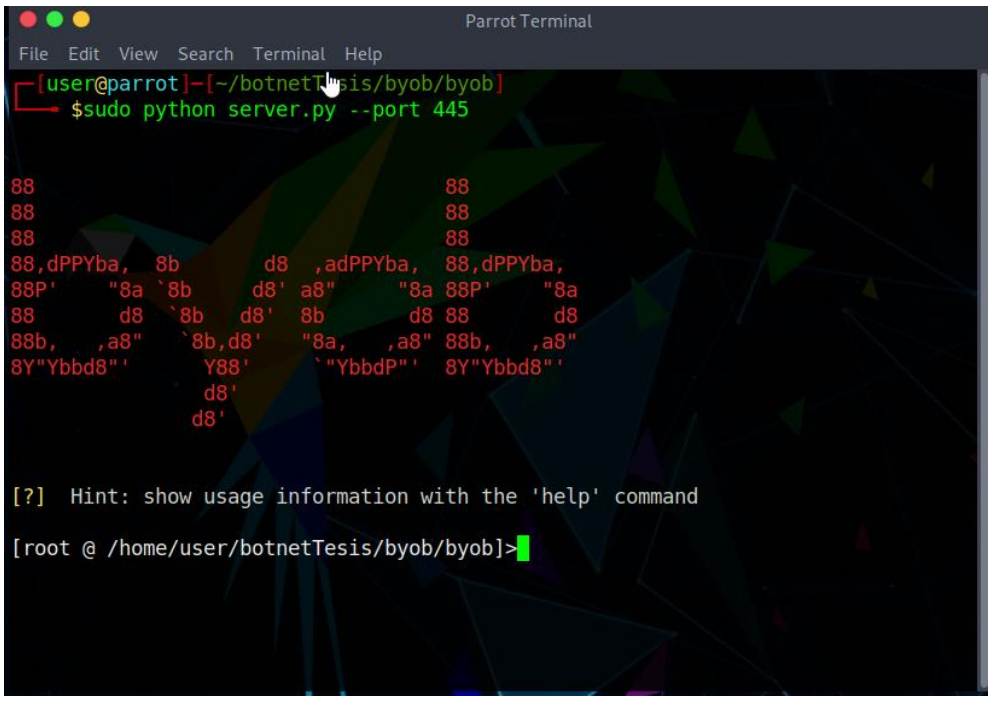


Figura 54. Arrancando el servidor de la botnet

Como se puede observar en la figura 55 existen varios comandos que se pueden ejecutar en las máquinas infectadas, desde capturar imagen/video del dispositivo infectado, ejecutar un Ransomware para encriptar todos los archivos como se mencionó en apartado 3.2.2, y obtener una shell reversa con el cliente para tener un control completo.

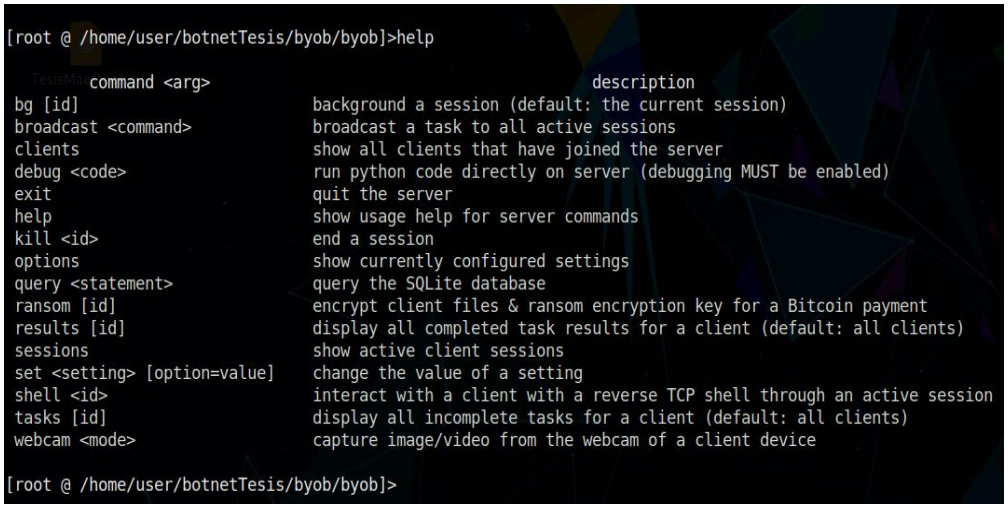


Figura 55. Opciones de la botnet con los dispositivos infectados

4. Una vez que el servidor está en escucha, se procede a crear el payload que va a ser enviado a los dispositivos para ser infectados

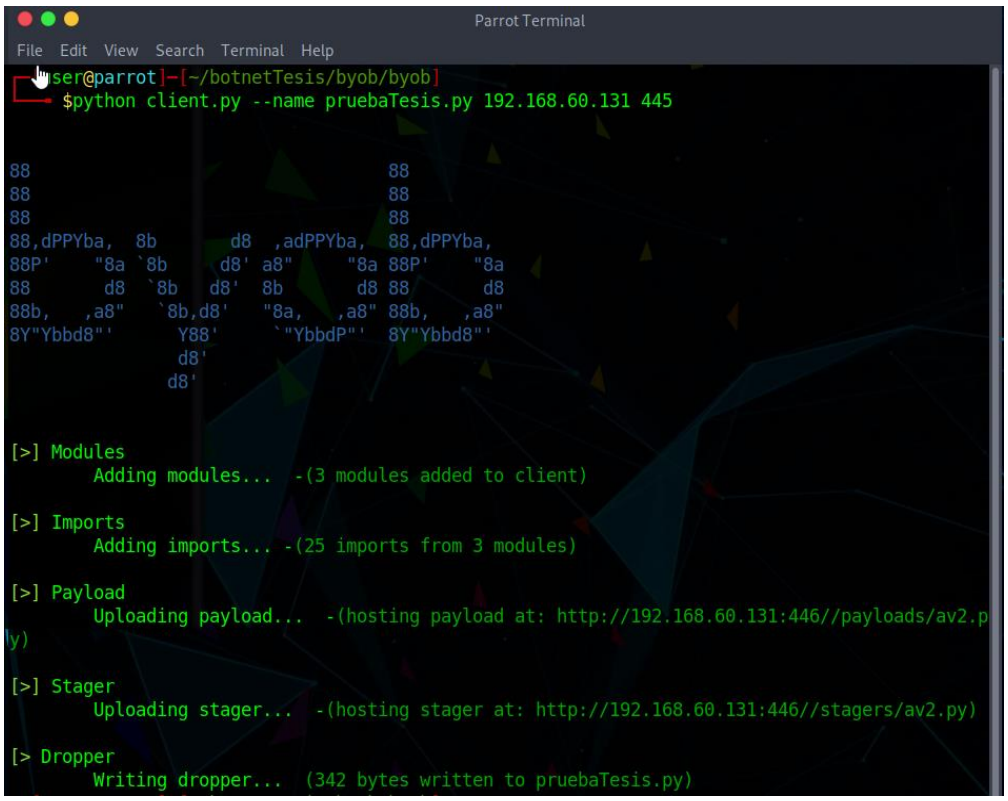


Figura 56 Ejecución del cliente y creación del Payload pruebaTesis.py

5. Como se puede observar en la figura 57, creo un archivo llamado pruebaTesis.py, el cual contiene el payload en el cual la dirección IP de la botnet se encuentra encodeada en formato base 64 que al ejecutarse en los dispositivos, los infectará y creará una conexión reversa hacia nuestra botnet.

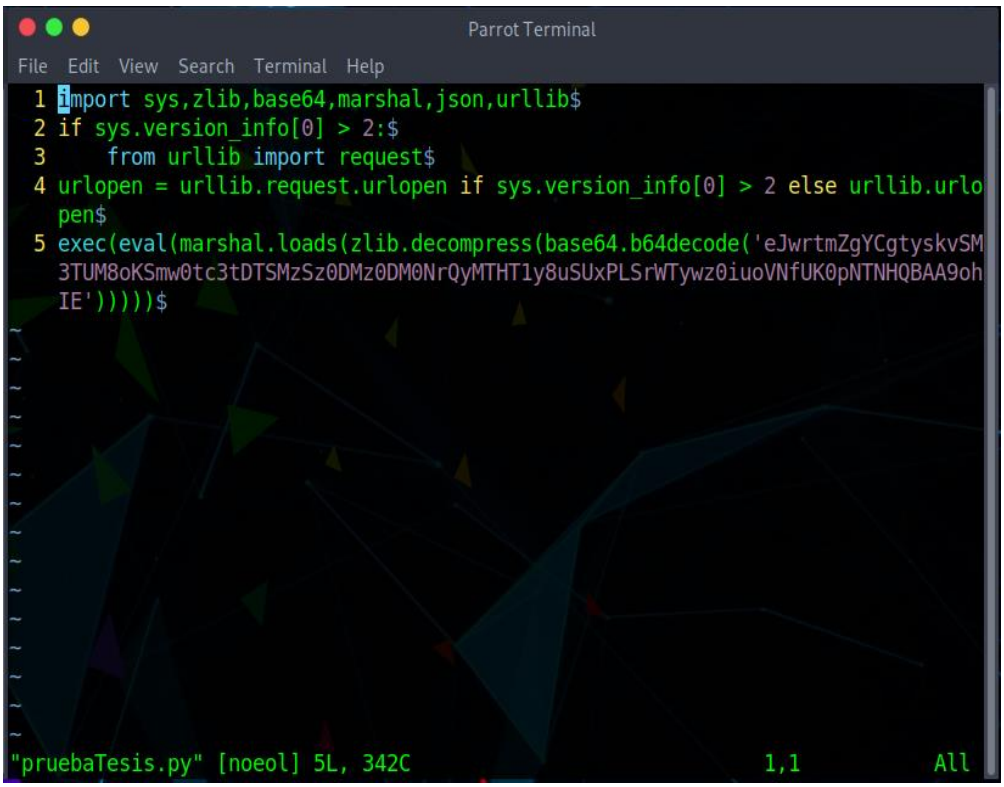


Figura 57 Archivo pruebaTesis.py

Para el desarrollo de esta prueba de concepto se infectará una máquina Windows.

4.2.3.2 Infectando equipos Windows

Como se mencionó en el apartado anterior , para infectar a los dispositivos es necesario que la víctima ejecute el archivo , para lo cual se puede emplear varias técnicas de ingeniera social, entre las más comunes tenemos el phishing , que un método que los ciberdelincuentes utilizan para engañar y conseguir que se revele información personal, como contraseñas o datos de tarjetas de crédito, y descarguen archivos que parecen legítimos , pero en realidad tienen malware integrado logrando infectar sus equipos.

1. Para infectar un dispositivo con sistema operativo Windows, se creará un archivo llamado pruebaTesis1, luego se procede a enviar el archivo a la víctima por correo electrónico o cualquier otro medio, y cuando la

víctima lo ejecute, se obtendrá una conexión reversa. Como se puede observar en el recuadro rojo de la figura 58, se está haciendo un llamado a la IP de la máquina atacante y luego procede a descargar todos los módulos en la máquina víctima y se obtiene una sesión como se observa en la figura 59.

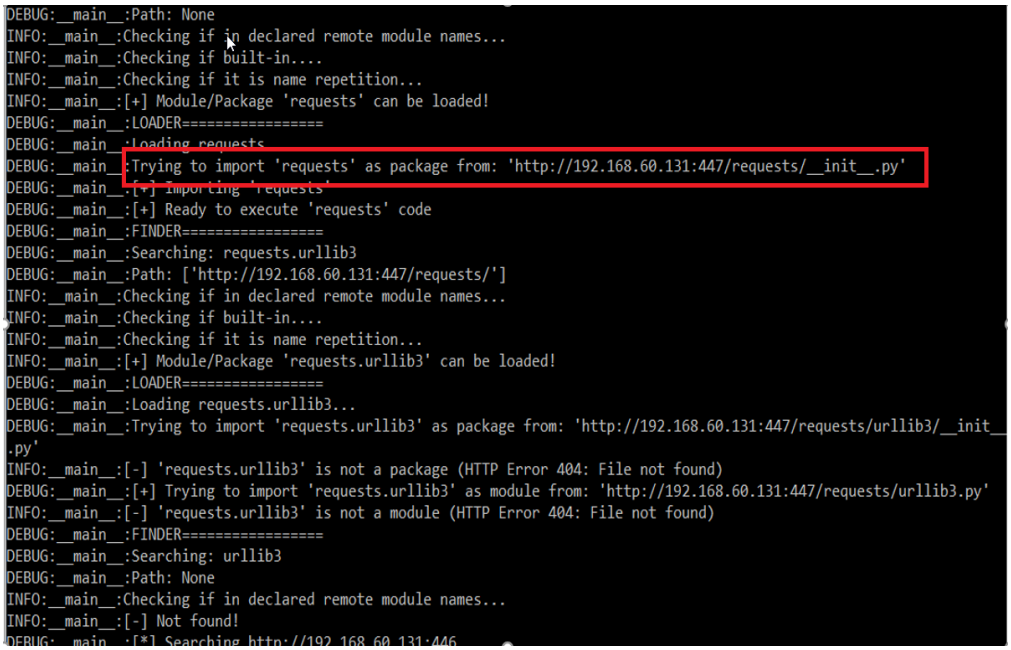


Figura. 58 Ejecución del archivo pruebaTesis.py en la máquina Windows

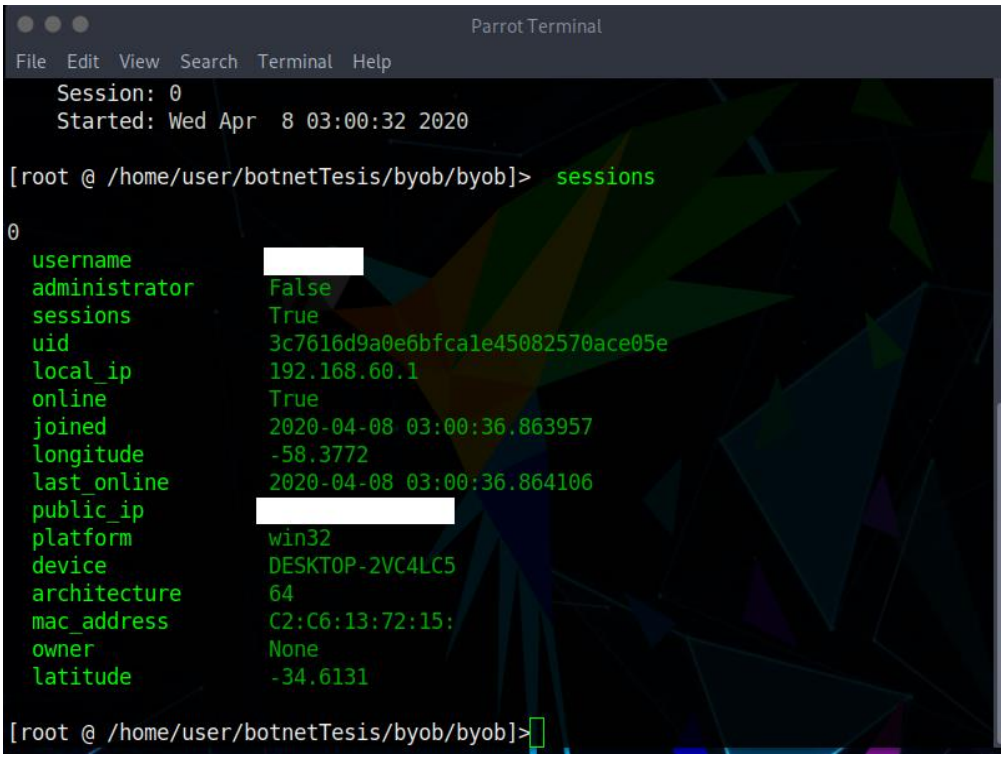


Figura 59 Sesión Obtenida en la botnet

2. Una vez obtenida la sesión, se procede a obtener una shell reversa TCP a través del comando “shell” como se muestra en la figura 60 , con el comando help se observa también todos los comandos que podemos ejecutar en la máquina zombie.

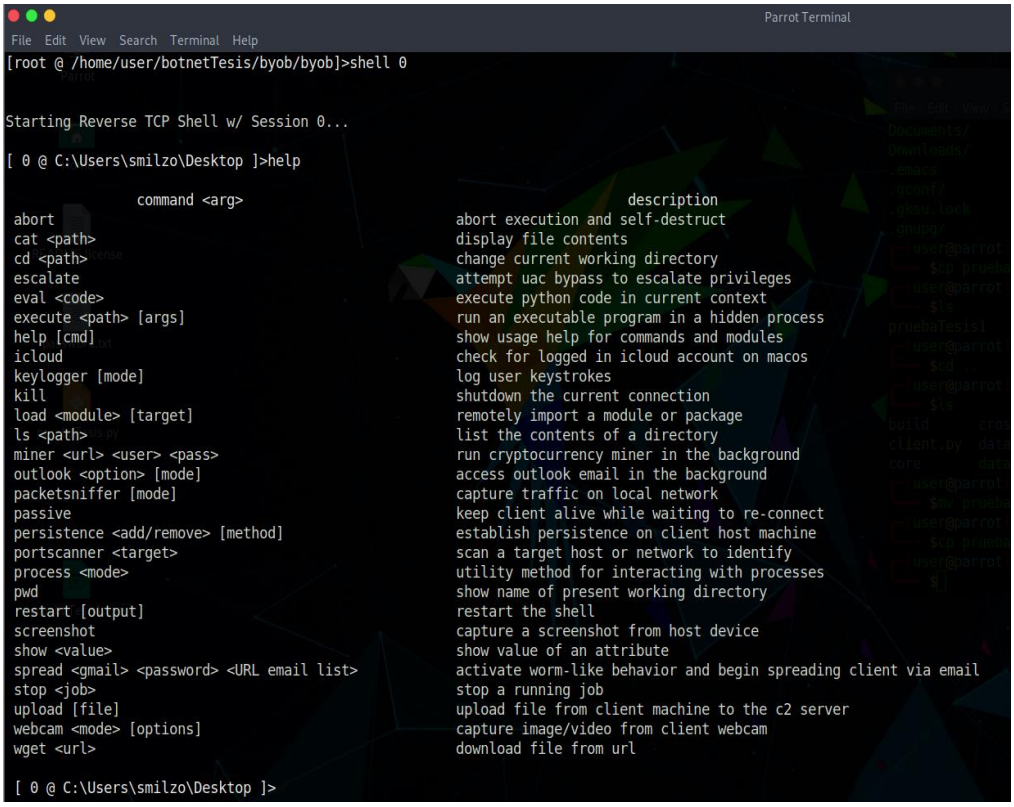


Figura 60 . Shell reversa de la máquina infectada en la botnet

3. En este trabajo se hará un análisis del minado de criptomonedas a través de Botnets , para lo cual usaremos el comando miner que recibe los siguientes parámetros:
    - url: del servidor donde de minado
    - usuario: de la cuenta:
    - password: de la cuenta

    Para la siguiente prueba de concepto se creo una cuenta en la página https://minergate.com/internal con los siguientes datos

    Usuario: pruebatesismaestria@gmail.com

    Password: PruebaTesisMaestria123@

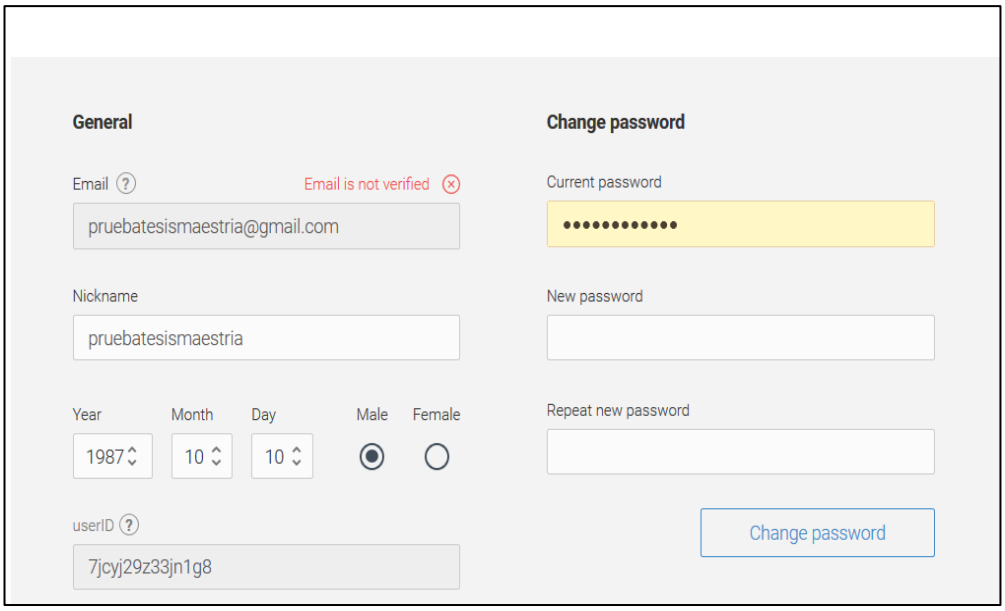


Figura 61 Datos de conexión de minergate

4. Luego de crear un usuario en página minergate, vamos a poner a minar al dispositivo infectado por nuestra botnet, para lo cual vamos a ejecutar el siguiente comando, que hará que el dispositivo comienzo a minar en segundo plano sin el conocimiento del usuario.

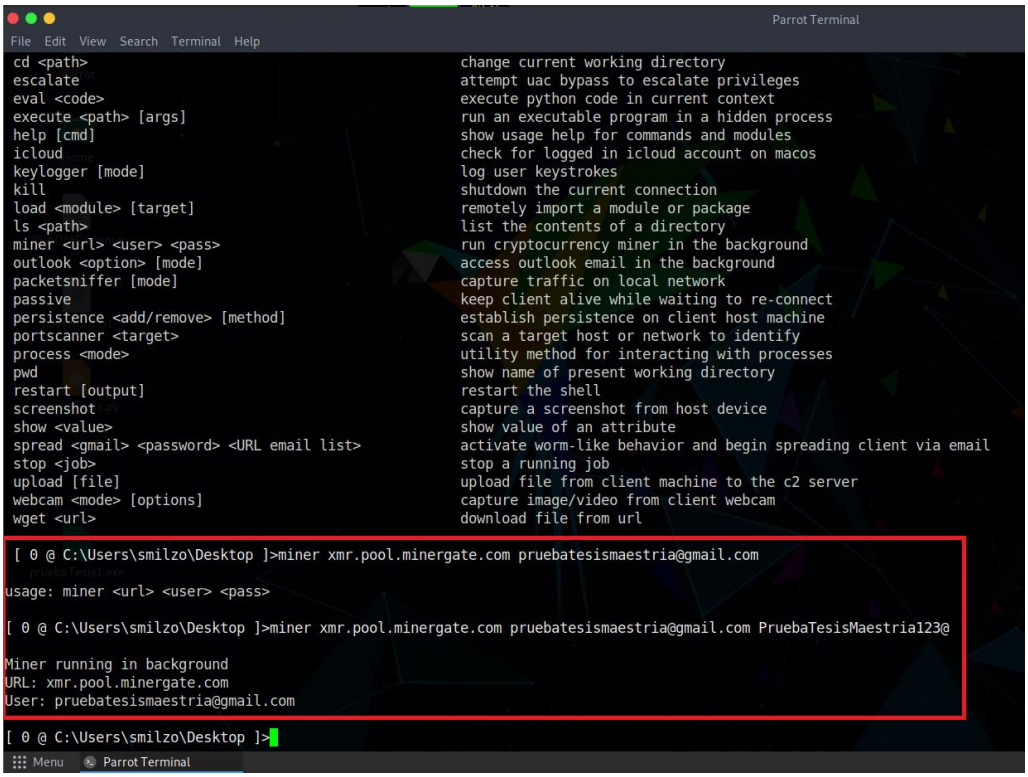


Figura 62. Máquina infectada minando en segundo plano

Si antes las redes de dispositivos infectados se utilizaban sobre todo para lanzar poderosos ataques DDoS, poco a poco su utilización ha sido

centrándose cada vez más en el minado de criptodivisas. Según informan desde ProofPoint, un grupo de cibercrminales puso en marcha en mayo 2017 utilizando el exploit EternalBlue una botnet llamada **Smominru**, la cual infectó a 526.000 servidores Windows y consiguió minar 8.900 Moneros, que al cambio serían entre 2,8 millones y 3,6 millones de dólares estadounidenses.

Monero es una moneda muy prometedora para los mineros, ya que se basa en algoritmo CryptoNight (Proof-of-Work) y podría ser minada en CPUs, en lugar de GPUs costosos, esto significa que cualquier persona que tiene una computadora o computadora portátil puede exitosamente minar Monero u obtener beneficio de eso. Es así que la obtención de varios dispositivos de IoT infectados en la botnet, permite a los ciber atacantes poner a minar estos dispositivos y así obtener un beneficio económico, como se observa en la figura 63.

Figura 63 Rentabilidad de Monero

Conclusiones

En el siguiente trabajo, se ha querido dar a conocer el estado del arte de “el Internet de las cosas” desde una perspectiva de ciberseguridad, mostrando principal énfasis en la evolución de los controles de seguridad, la protección de los dispositivos de IoT, y la privacidad de los datos que manejan estos dispositivos.

Por consiguiente, la realización del presente trabajo requirió el desarrollo de varios casos de estudios con el objetivo de:

- Conocer cuales son los principales vectores de ataque a los dispositivos Iot en una empresa y los riesgos que presentan a la confidencialidad, disponibilidad e integridad de los datos que manejan.
- Analizar la metodología OWASP, en la cual se resaltaron las vulnerabilidades y contramedidas contra los diferentes tipos de ataques que se desarrollaron en este trabajo.
- Conocer cual es le estado de madurez con respecto a la estandarización y los protocolos de IoT, para así lograr formar una arquitectura homogénea que permita la comunicación de diferentes tecnologías. De este modo, se puede hacer una distinción entre las tecnologías establecidas que ya estaban en el mercado antes de que IoT y las tecnologías que se han desarrollado recientemente específicamente para el propósito de IoT
- Establecer medias mínimas de seguridad para los diferentes tipos de dispositivos IoT a través de la metodología OWASP, de esta manera cuando una organización comience a considerar y diseñar diferentes controles de seguridad en los dispositivos de IoT o en la arquitectura perimetral, los procesos y las tareas estarán alineadas con el valor de los activos de IoT y la valoración de los datos.
- Otro elemento clave a mencionar, es la seguridad en el acceso a la configuración del os dispositivos de IoT. Como se muestra en el capítulo 4, existen diferentes maneras de acceder estos

dispositivos, a través de una consola de ssh , o directamente a través de una interfaz web para lo cual , según la metodología OWASP “A2:2017 Broken Authenticacion” se especifica cuáles son los controles que se deben tener en cuenta para poder hacer más robusta la seguridad y disminuir los vectores de ataque. Una parte básica de la implementación de los controles técnicos de seguridad es desactivar y cerrar todos los puertos y servicios innecesarios y no utilizados. La regla podría ser que solo un número mínimo de puertos y servicios deben estar abiertos y activos, y estos son los relacionados con las aplicaciones en ejecución. Todos los demás puertos y servicios deben estar cerrados.

Como resumen, el resultado de este trabajo es conocer el nivel de seguridad de los dispositivos IoT que se encuentran expuestos a internet, y cuáles son los diferentes tipos de amenazas a los que están expuestos y las recomendaciones para la mitigación de la mismas.

Por otra parte, como hemos visto a lo largo de todo este trabajo, IoT es una realidad, pero que avanza poco a poco, y no parece que vayan a ponerle freno las preocupaciones por la seguridad, limitaciones tecnológicas o costes, por lo cual lo mejore es estar preparados con la mejores medidas de seguridad y así tener seguro el activo más importante de una organización, los datos

Bibliografía

[1] ErnestoB, “¿Cuál es el estado actual de la seguridad en la IoT?,” 2018. [Online]. Available: https://bitcoin.es/actualidad/cual-es-el-estado-actual-de-la-seguridad-en-la-iot/. [Accessed: 14-Oct-2018].

[2] H. Russo, “El estado actual del Internet de las Cosas en Latinoamérica,” p. 1, 2018.

[3] V. Dehalwar, A. Kalam, M. L. Kolhe, and A. Zayegh, “Review of web-based information security threats in smart grid,” *2017 7th Int. Conf. Power Syst. ICPS 2017*, pp. 849–853, 2018.

[4] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[5] M. Thapa, “Mitigating Threats in IoT Network using Device Isolation,” 2018.

[6] ErnestoB, “¿Cuál es el estado actual de la seguridad en la IoT?,” *2018*. [Online]. Available: https://bitcoin.es/actualidad/cual-es-el-estado-actual-de-la-seguridad-en-la-iot/. [Accessed: 14-Oct-2018].

[7] B. Cendón, “No Title,” 2017. [Online]. Available: http://www.bcendon.com/el-origen-del-iot/. [Accessed: 12-Feb-2020].

[8] D. Fernandez Sanches, “Diseño Logico de una aplicacion para determinar el nivel de seguridad de un dispositivo IoT,” 2017.

[9] M. C. Losa, “Escuela Politécnica Superior de Jaén,” no. April, p. 260, 2016.

[10] L. Fedele and L. Fedele, “From Basic Maintenance to Advanced Maintenance,” *Methodol. Tech. Adv. Maint.*, pp. 63–112, 2011.

[11] V. Sulkamo, “IoT from cyber security perspective Case study JYVSECTEC School of Technology, Communication and Transport Information Technology Master’s Degree Programme in Cyber Security,” no. June, 2018.

[12] L. Miller, “IoT Security for Dummies,” *Insid. Secur.*, vol. 91, pp. 399–404, 2016.

[13] M. Tijssen and E. Poll, “Creating secure IoT systems,” 2017.

[14] S. Tabbane, “IoT Standards Part I: IoT Technology and Architecture,”

no. September, 2018.

[15] A. Cobos, “Diseño e implementación de una arquitectura IoT basada en tecnologías Open Source.,” p. 133, 2016.

[16] “Internet de las cosas Estas son las capas del Internet de las Cosas,” 2018. [Online]. Available: https://www.t-systemsblog.es/estas-son-las-capas-del-internet-de-las-cosas/.

[17] Luis del Valle Hernández, “Arquitectura IoT, prototipando los dispositivos del futuro.” [Online]. Available: https://programarfacil.com/podcast/arduino-wifi-proyectos-iot/.

[18] S. Raman, “Security Risk Management for the IoT systems,” 2018.

[19] F. Hu, *Security and Privacy in Internet of Things (IoTs)*. 2016.

[20] Ahmed Banafa, “https://www.bbvaopenmind.com/tecnologia/mundo-digital/estandarizacion-y-retos-de-implantacion-de-internet-de-las-cosas/,” 2016. [Online]. Available: https://www.bbvaopenmind.com/tecnologia/mundo-digital/estandarizacion-y-retos-de-implantacion-de-internet-de-las-cosas/. [Accessed: 03-Feb-2020].

[21] V. Bhuvaneswari and R. Porkodi, “The internet of things (IOT) applications and communication enabling technology standards: An overview,” *Proc. - 2014 Int. Conf. Intell. Comput. Appl. ICICA 2014*, no. March, pp. 324–329, 2014.

[22] Ahmed Banafa, “Estandarización y retos de implantación de Internet de las Cosas,” 2016. [Online]. Available: https://cambiodigital-ol.com/2018/12/iot-que-necesitan-saber-los-profesionales-de-la-red/.

[23] IERC, “IERC-European Research Cluster on the Internet of Things,” *Ierc*, p. 1, 2015.

[24] S. Raman *et al.*, “Análisis de botnets y ataques de denegación de servicio,” vol. 3, no. August, pp. 329–343, 2018.

[25] P. Guillemin *et al.*, “Internet of Things Standardisation - Status, Requirements, Initiatives and Organisations,” *Internet Things - Convert. Technol. Smart Environ. Integr. Ecosyst.*, no. February, pp. 259–276, 2013.

[26] Ignacio Porro Sáez, “IoT: protocolos de comunicación, ataques y recomendaciones,” 2019. [Online]. Available: https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones.

[27] Ignacio Porro Sáez, “IoT: protocolos de comunicación, ataques y recomendaciones,” 2019. [Online]. Available: https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones. [Accessed: 04-Feb-2020].

[28] INCIBE, “Tendencias en el mercado de la Ciberseguridad,” 2016.

[29] European Union Agency for Network and Information Security, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, no. November. 2018.

[30] T. Salman and R. Jain, “Networking protocols and standards for internet of things,” *Internet Things Data Anal. Handb.*, pp. 215–238, 2017.

[31] A. Mohammed, I. Alkuhlani, and S. B. Thorat, “Internet of Things (IOT) Standards , Protocols and Security Issues,” *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 11, pp. 491–495, 2015.

[32] R. KumarGoutam, “Importance of Cyber Security,” *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 14–17, 2015.

[33] C. Jaikaran, “Cybersecurity : An Introduction,” 2018.

[34] CamaraValencia, “La ciberseguridad en cifras: los datos muestran incremento en la preocupación empresarial,” 2019. [Online]. Available: https://ticnegocios.camaravalencia.com/servicios/tendencias/la-ciberseguridad-en-cifras-los-datos-muestran-incremento-en-la-preocupacion-empresarial/. [Accessed: 04-Mar-2020].

[35] L. O. S. P. Retos and D. E. L. A. Ciberseguridad, “CIBERSEGURIDAD EN 2019,” pp. 1–16, 2019.

[36] “Doble autenticación.”

[37] ESET, “TODO SOBRE EL RANSOMWARE: Guía básica y preguntas frecuentes,” p. 8, 2016.

[38] G. Empresas, “Mañana es hoy.”

[39] INCIBE, “La importancia de la seguridad en IoT. Principales amenazas,” 2019. [Online]. Available: https://www.incibe-cert.es/blog/importancia-

seguridad-iot-principales-amenazas. [Accessed: 04-Mar-2020].

[40] Kudelski Secury Team, “2019 Cybersecurity Trends to Watch: IoT, AI, and Machine Learning,” 2019. [Online]. Available: https://modernciso.com/2019/01/30/2019-cybersecurity-trends-to-watch-iot-ai-and-machine-learning/. [Accessed: 22-Dec-2019].

[41] C. de C. I. (CCI), M. García-Menéndez, C. Cerrudo, M. Palao, and K. El-Yattoumi, “Smart Cities ante el desafío de la seguridad,” no. 2, 2016.

[42] David Balaban, “How to Set up a Secure Home Network,” 2019. [Online]. Available: https://hackernoon.com/how-to-set-up-a-secure-home-network-a3d0f829fd6c. [Accessed: 13-Jan-2020].

[43] F. Y. Rashid, “How to Secure Your (Easily Hackable) Smart Home.” [Online]. Available: https://www.tomsguide.com/us/secure-smart-home-how-to,news-19380.html. [Accessed: 16-Oct-2017].

[44] Insights, “What is Botnet, Prevention and Detection Techniques,” 2018. [Online]. Available: https://www.xenonstack.com/insights/what-are-botnets/. [Accessed: 16-Mar-2020].

[45] M. Eslahi, R. Salleh, and N. B. Anuar, “Bots and botnets: An overview of characteristics, detection and challenges,” *Proc. - 2012 IEEE Int. Conf. Control Syst. Comput. Eng. ICCSCE 2012*, no. November, pp. 349–354, 2012.

[46] M. T. Banday, J. A. Qadri, and N. A. Shah, “Study of Botnets and their threats to Internet Security,” *Work. Pap. Inf. Syst.*, no. January 2009, 2009.

[47] A. N.-T. Stock, “Shodan, la alternativa a Google más peligrosa,” 2019. [Online]. Available: https://www.ticbeat.com/tecnologias/shodan-alternativa-peligrosa-google/. [Accessed: 23-Jan-2020].

[48] L. Fernández, “¿Conocías Shodan? Todo sobre este motor de búsqueda orientado al hacking,” 2020. [Online]. Available: https://www.redeszone.net/noticias/seguridad/navegadores-bloquean-cookies-terceros/. [Accessed: 03-Jan-2020].

[49] “ETHICAL HACKING.” [Online]. Available: http://reader.digitalbooks.pro/book/preview/42132/x630-fanjul-v2-8. [Accessed: 04-Apr-2020].

[50] Ionut Ilascu, “New Gafgyt Variant Recruits Routers to DDoS Servers for Valve Games,” 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-gafgyt-variant-recruits-routers-to-ddos-servers-for-valve-games/. [Accessed: 10-Mar-2020].

[51] Lucyoa, “Exploitation Framework for Embedded Devices.” [Online]. Available: https://github.com/threat9/routersploit. [Accessed: 05-Apr-2020].

[52] AVAST, “Your router is vulnerable to network attacks!” [Online]. Available: https://help.avast.com/en/av_free/17/hns/cve-2014-4019.html#details.

[53] “Insecurity breeds at home Small Office Home Office (SOHO).”

[54] T. File, T. Protocol, S. S. H. File, T. Protocol, T. M. Project, and M. Framework, “Vsftpd 2.3.4 backdoor vulnerability,” pp. 6–8, 2011.

[55] OWASP, “Penetration testing methodologies,” pp. 1–5, 2016.