Análisis de las vulnerabilidades de seguridad en un hogar inteligente: Simulación en ambiente controlado con el asistente de Amazon Echo.

Autor: Luis Bernardo Estrada Bolívar.

Correo: bernardo.estrada@udea.edu.co

Título de la tesis: Confiabilidad de los sistemas de seguridad del hogar inteligente basado en IoT.

Ingeniería de telecomunicaciones.

Décimo semestre.

Universidad de Antioquia.

1. Exámenes de posibles fallas de seguridad de la información ante ataques comunes a los hogares inteligentes

Para el desarrollo del presente análisis se usó el nuevo asistente Amazon Echo de 4ª generación, el cual es un parlante inteligente con Alexa (ver figura 1) que se puede controlar por medio de comandos de voz. Este asistente puede controlar otros dispositivos inteligentes usados en el hogar, lo que lo convierte en un blanco de ataques informáticos según los directivos de Fortinet [1].

Descripción de los ataques efectuados

Se realizaron dos ataques ante la seguridad del dispositivo, el primer ataque fue un sabotaje el cual está clasificado en el anexo 1 de seguridad de los dispositivos IoT en la categoría de ataques o abusos con la amenaza de ingeniería social, el cual se completó con un ataque físico a la aplicación que controla este dispositivo; el segundo ataque se realizó mediante el envío de un virus informático de denegación de servicios (DoS) mediante el símbolo del sistema de Windows y los canales de comunicación que posee Alexa (Wifi y

bluetooth), estos ataques se realizaron para con el objetivo de evidenciar las fallas de seguridad de un hogar inteligente.

Figura 1. *Parlante inteligente con Alexa.*
Fuente: *(Amazon, 2019)*

1.1.Configuración de Alexa

El asistente Amazon Echo debe ser configurado por medio de una aplicación que está disponible tanto para sistemas Android como para sistemas IOS, en ambos sistemas las configuraciones son similares y requieren que el asistente tenga una conexión a internet estable para que su instalación y funcionamiento sean correctos. Se le conceden permisos a la aplicación de Amazon (ver figuras **2**, **3** y **4**) para que pueda acceder a los datos personales del usuario, conocer la ubicación exacta del dispositivo dentro del hogar, la dirección del inmueble donde se encuentra instalado, el correo electrónico, el acceso a otras cuentas de plataformas como Netflix, Amazon, entre otras. Adicionalmente para completar una configuración segura se conecta el dispositivo a la red wifi bajo el modo configuración del dispositivo. Luego de aplicar todos los cambios correctamente, Alexa le habla al usuario para que éste le haga una serie de preguntas, allí puede identificar su voz y guardarla como el administrador del sistema.

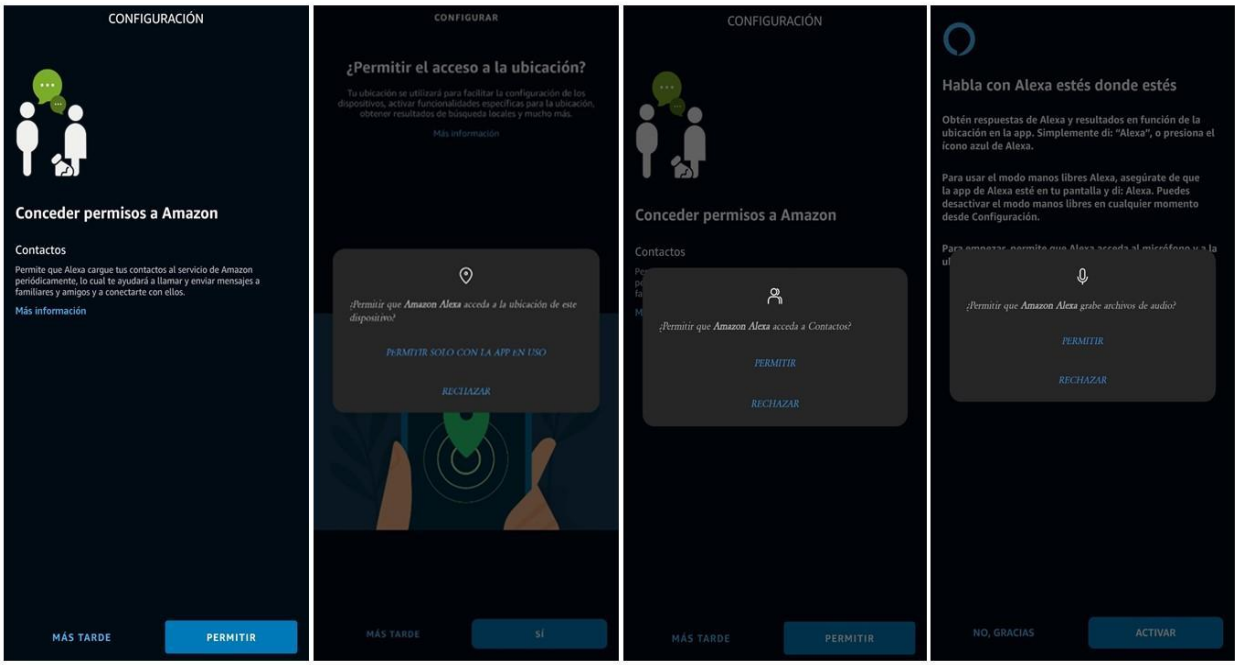

Figura 2. *Configuración en la app de Amazon parte I.*

Fuente: Autor del proyecto.

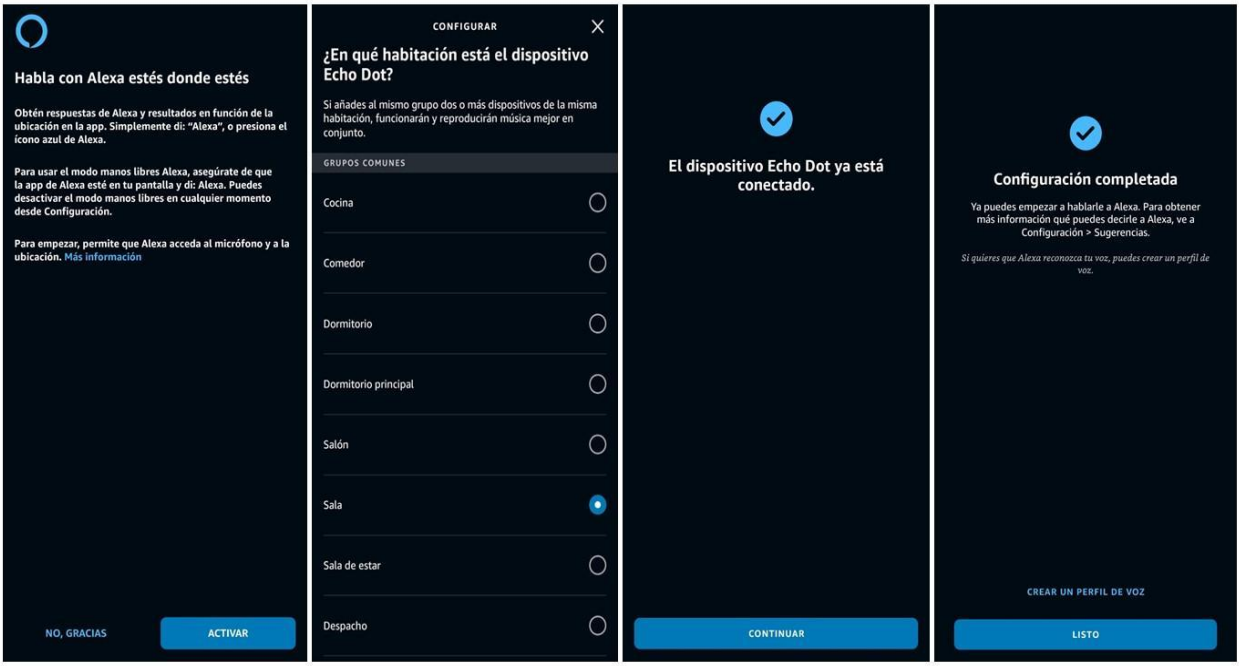

Figura 3. *Configuración en la app de Amazon parte II.*

Fuente: Autor del proyecto.

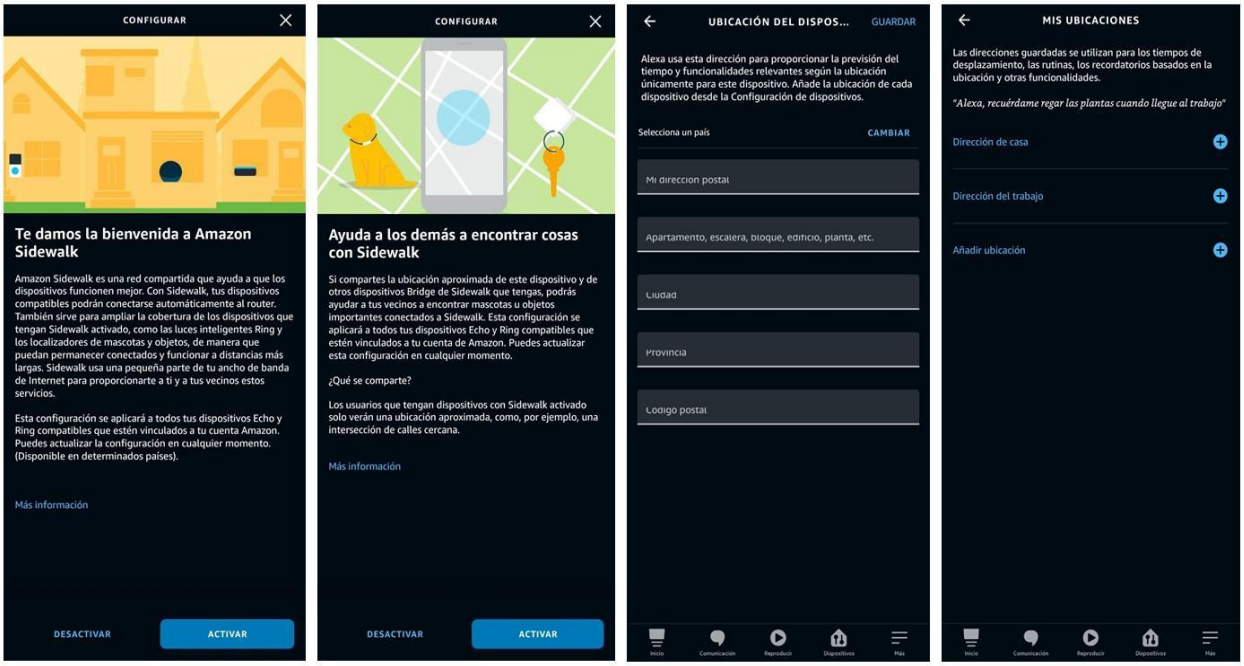

Figura 4. *Configuración en la app de Amazon parte III.*

Fuente: Autor del proyecto.

El asistente cuenta con una configuración de seguridad adicional, la cual puede ser ejecutada al ingresar a la cuenta principal y realizar la identificación del tono de voz del usuario, en donde Alexa graba la voz del usuario y puede identificarla en usos futuros. Esta configuración crea un perfil del usuario en donde guarda sus datos y va generando un historial con base a las preguntas que se le formule, con el fin de poder "predecir" el comportamiento del usuario. Para ver la operatividad de esta función, se hacen dos rondas de preguntas las cuales se presentan a continuación:

Preguntas generales:

- ¿Alexa, dime cuál es el clima hoy de la ciudad?
- ¿Alexa, cuál es el valor del dólar hoy?
- ¿Alexa, qué es la Internet de las cosas?
- ¿Alexa, qué es el Internet?
- ¿Alexa, qué es una smart home?

Las respuestas obtenidas fueron verificadas en diferentes páginas web para comprobar la veracidad de los datos.

Preguntas relacionadas con dispositivos IoT.

¿Alexa, puedes subir la cortina?
¿Alexa, puedes encender la luz de la sala?
¿Alexa, puedes apagar luces?
¿Alexa, puedes encender el termostato?
¿Alexa, activa el sonido?

Las respuestas de estas preguntas generan acciones de control en los demás dispositivos IoT, tales como subir o bajar la cortina, encender o apagar la luz, cambiar la temperatura del lugar, entre otras.

1.2.Características de un ataque de ingeniería social hacia un dispositivo IoT

El objetivo de la ingeniería social es manipular psicológicamente a la víctima para generar confianza y que ésta proporcione información para tener acceso a las cuentas electrónicas que maneja. [2] Otra característica de este ataque es que el ciberdelincuente tenga acceso físico tanto a la red en donde se encuentra conectada el dispositivo asistente Amazon echo como al mismo dispositivo, una vez con este acceso garantizado puede tomar dos caminos, el primero es por medio aplicaciones como: Quien roba mi WiFi: Analizador WiFi, Escaner WiFi, y Fing, las cuales pueden encontrar en la play store (ver figura **5**), para que estas puedan identificar datos necesarios para hacer ataques con más fuerza de entrada y encontrar información personal del usuario, los datos importantes para generar ataques son la dirección IP a la que está conectada el dispositivo, la dirección IP del dispositivo dentro de la red, la puerta de enlace, la dirección MAC, y los DNS de la red.

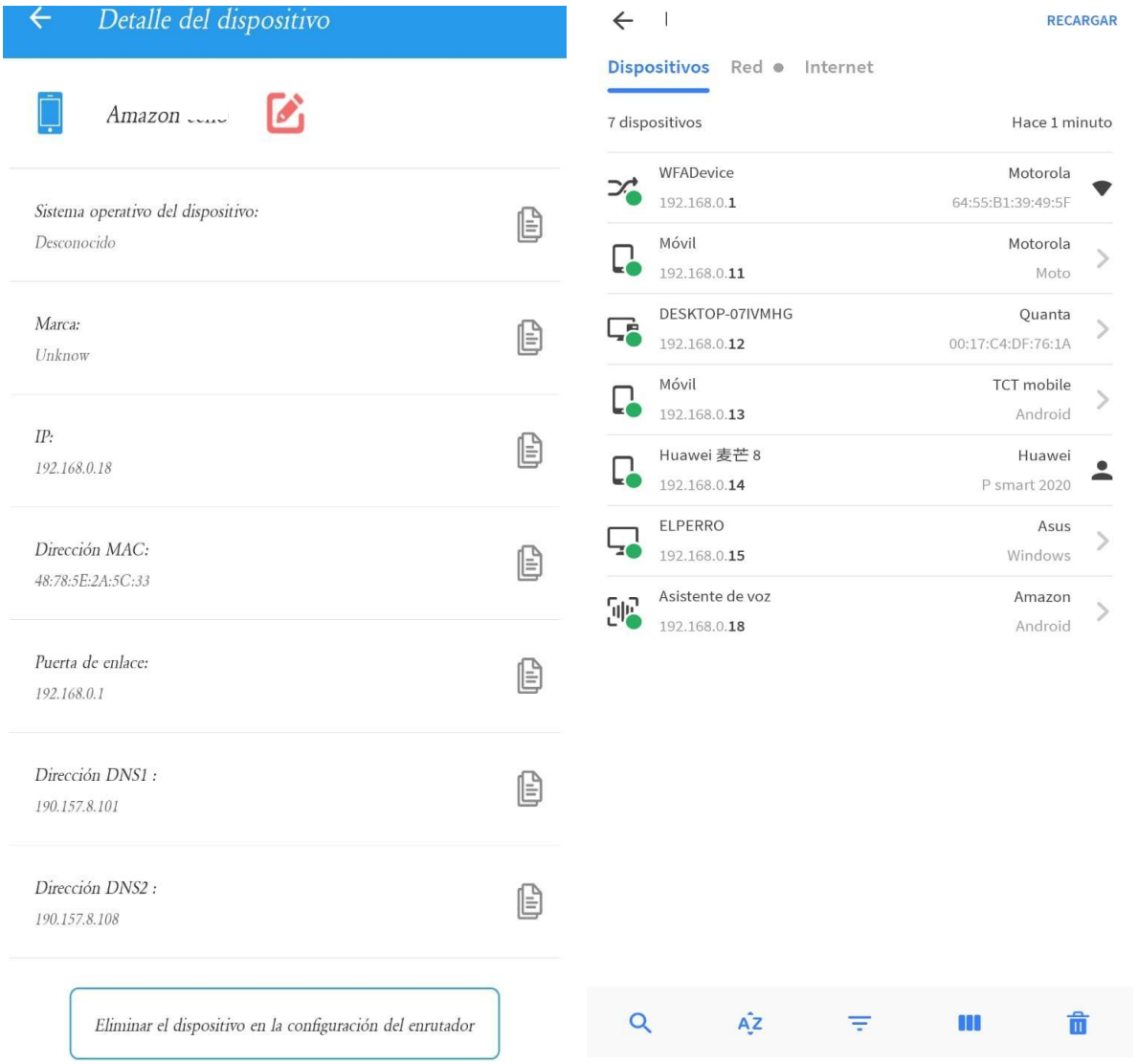

Figura 5. *Datos importantes del dispositivo inteligente.*

Fuente: Autor del proyecto.

Un segundo método de entrada basado en la ingeniería social es encontrar al asistente y comenzar a hacer preguntas, como las siguientes:

- ¿Alexa, puedes darme información del perfil de este usuario?
- ¿Alexa, cuántos dispositivos están conectados a esta red?
- ¿Alexa, puedo cambiar la contraseña de mi red?
- ¿Alexa, cuál es mi agenda hoy?
- ¿Alexa, cuáles son mis recordatorios de hoy?

Las anteriores preguntas también fueron hechas por dos personas ajenas al perfil del usuario principal y el dispositivo inteligente respondió cada una de estas entregando la información correspondiente.

Con estas preguntas se puede encontrar la información necesaria para poder controlar toda la red y tener acceso a información del usuario y de sus datos privados. Este método es la puerta de entrada para poner en jaque a cualquier dispositivo y poder generar ataques para lograr interceptar y secuestrar datos, caídas del sistema, pérdida o daño de los dispositivos y también averías o fallos en toda la red. Por tal motivo es necesario que el usuario ubique el asistente Amazon Echo en un lugar privado de la casa, con el fin de evitar que intrusos puedan utilizar la ingeniería social para conseguir información confidencial.

1.3. Características de un ataque de denegación de servicios DoS hacia un dispositivo IoT

Este ataque requiere una serie de pasos para su correcto funcionamiento, si se tiene como base un ataque de ingeniería social en donde se conoce la dirección IP del router y del dispositivo es más fácil llevar a cabo este ataque a la seguridad y no será necesario hacer ataques de fuerza bruta para saturar el router y que la red caiga, también se debe tener identificado si existe un servidor que esté basado en un sistema operativo de Windows o cualquier otra plataforma.

Para realizar este ataque se tiene en cuenta que el servidor está basado en un sistema operativo de Windows.

1.3.1. Pasos para realizar un ataque DoS

- Conocer la dirección IP del router y del dispositivo.
- Ejecutar como administrador el símbolo de Windows en cualquiera de sus versiones.
- Con la dirección IP del router y del dispositivo se puede realizar un ping con un tamaño de bytes cercano al máximo permitido y así lograr saturar el dispositivo, lo que se conoce también como ping de la muerte. Se realiza un primer intento de hacer un ping hacia el dispositivo Amazon Echo, sin

embargo este se encuentra protegido para no responder la solicitud de ping, sin embargo el router sí responde la solicitud.

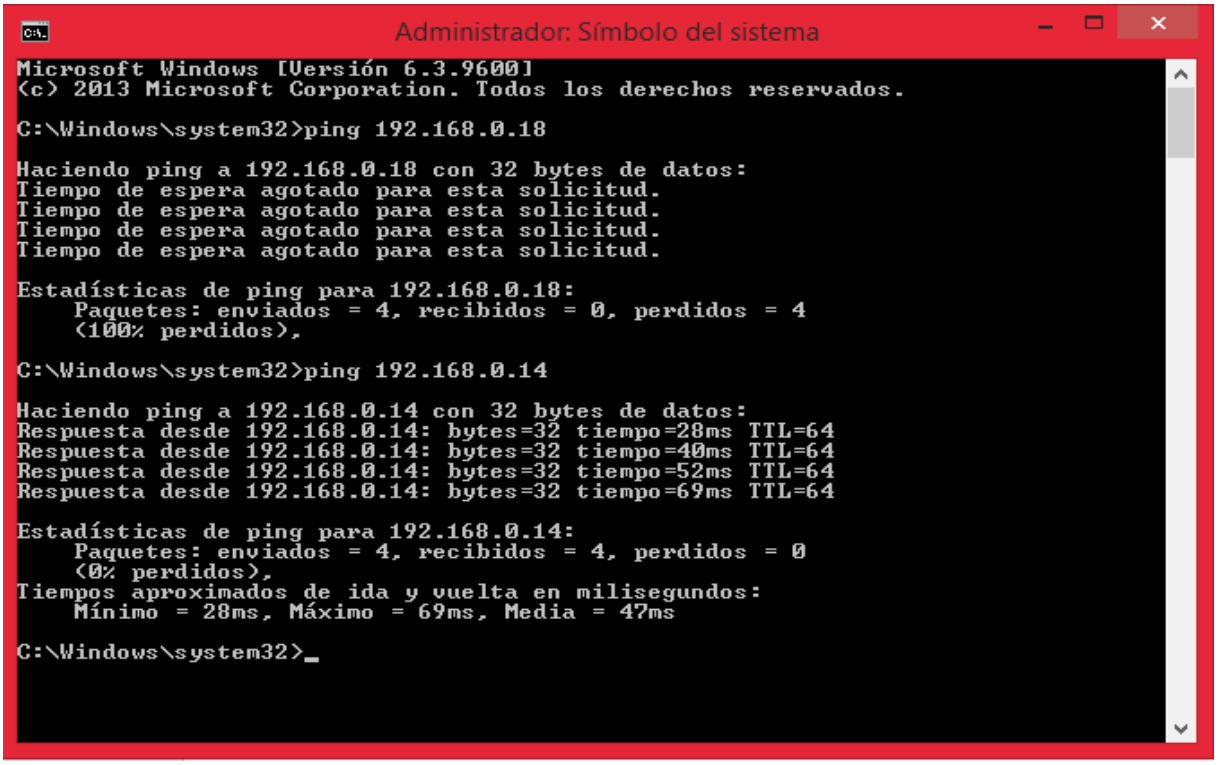

Figura 6. *Ping para dispositivos de la red.*

Fuente: Autor del proyecto.

- A continuación se puede generar un ping sostenido adicionando al final de la línea –t para generar un bucle infinito.

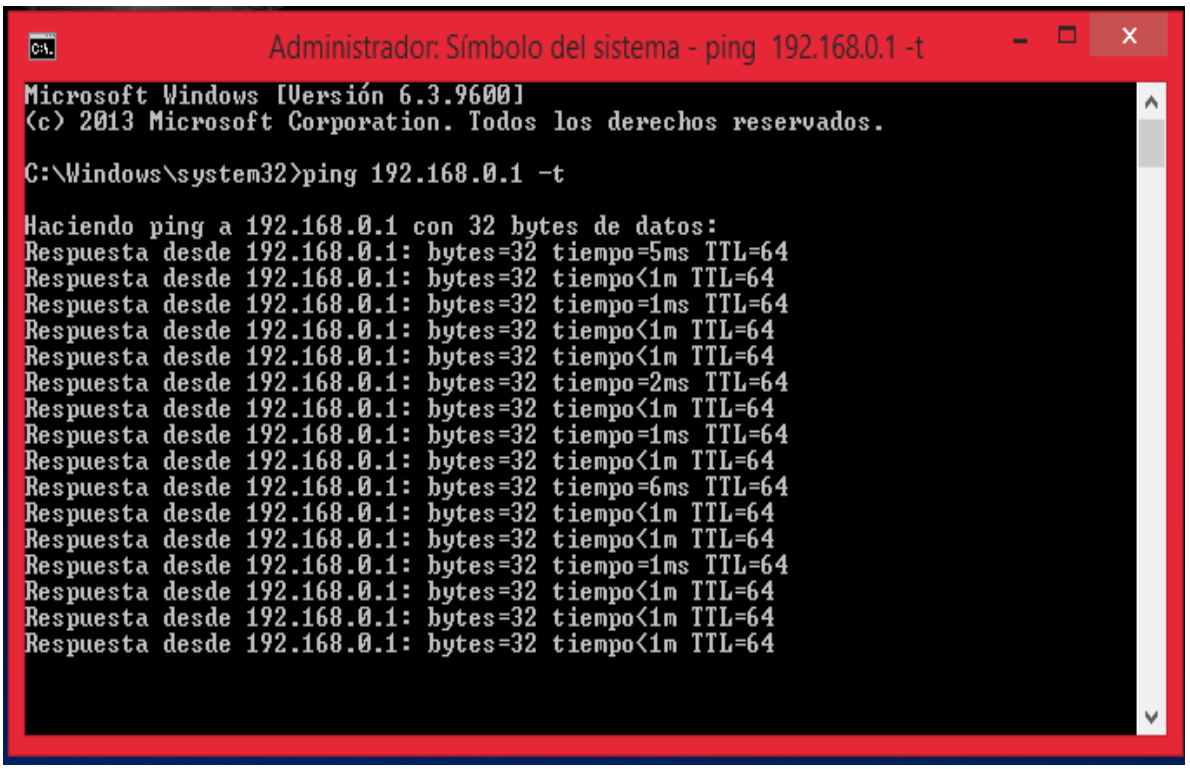

Figura 7. *Ping para ataque a un router.*

Fuente: Autor del proyecto.

- Por último se genera un ping de la muerte para el router que controla la red y la seguridad de un hogar inteligente al generar un ping con un tamaño mayor a 65507 bytes, una característica de este ataque es que los paquetes llegan al destino en forma fragmentada y se reconstruirán a medida que lleguen al sistema atacado, esto también se conocer como un buffer overflow el cual provoca que todo el sistema se bloquee por periodos de tiempo en donde se puede infectar con algún troyano.

  Para crear este ataque se hace necesario seguir estos pasos:
  Abrir un bloc de notas y escribir lo siguiente:
  :loop
  ping 192.168.0.1 -l 65500 -w 1 -n 1
  goto :loop
  guardar esto bajo el nombre que desee, pero con la extensión .bat. para que se convierta en un ejecutable como se observa en la figura **8**.

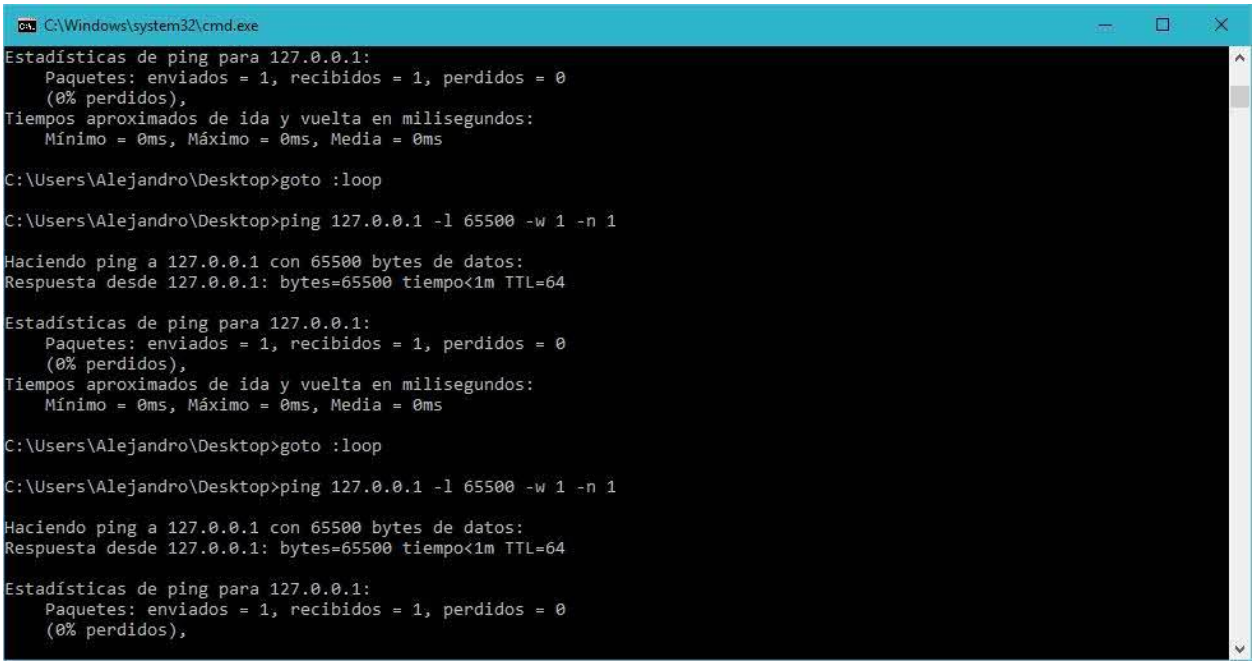

Figura 8. *Ping de la muerte.*

Fuente: Autor del proyecto.

- Como se observa, este ataque depende del ancho de banda desde donde se esté haciendo el ataque y del ancho de banda del que está recibiendo el ataque así como de las características del router del proveedor de servicios de internet; el atacante debe tener un ancho de banda superior al de la víctima para que logre saturar la capacidad de procesamiento de información en el router atacado; este ataque aunque es de los primeros usados es usado por los ciberdelincuentes mediante una red de bots para saturar el router y lograr que el hogar inteligente pierda la conexión con los dispositivos, lo que ocasionará que el usuario no pueda controlar las funciones que configuró inicialmente, y exponiendo el sistema ante otros ataques cibernéticos o físicos en caso de contar con cerraduras magnéticas inteligentes.

- Otras formas de causar daño a un sistema operativo, a una red y a un dispositivo inteligente, es mediante los códigos, se debe tener en cuenta que estos causan un daño de pérdida parcial o total de los dispositivos y su forma de ingreso al sistema es a través de correo electrónicos, descargas y/o actualizaciones en páginas falsas o phishing. El primer código que se presenta es un virus que entra al sistema como un ejecutable y causa que tanto el

ordenador como los dispositivos se congelen y no atiendan a las funciones que se apliquen y esto provoca que los sistemas que estén conectados a esta red se caigan, también puede llegar a dañar el hardware del ordenador.

Código: @echo off start winword start mspaint start notepad start write start cmd start explorer start control start calc goto x.

Este archivo se crea en un bloc de notas y se guarda con extensión .bat o .exe; cuando el archivo es ejecutado dentro de la red, es enviado a Alexa haciendo que el internet sea deshabilitado y el usuario deberá llamar a su proveedor para solucionar este problema generado.

Código: echo @echo off>c:windowswimn32.bat echo break off>c:windowswimn32.bat echo ipconfig/release_all>c:windowswimn32.bat echo end>c:windowswimn32.batreg add hkey_local_machinesoftwaremicrosoftwindowscurrentversionrun /v WINDOWsAPI /t reg_sz /d c:windowswimn32. bat /freg añadir hkey_current_usersoftwaremicrosoftwindowscurrentversionrun /v CONTROLexit /t reg_sz /d c: windowswimn32.bat /fecho ¡Has sido HACKED! PAUSA.

1.4.Ataques por fuera de red.

Los ataques desde las redes externas al hogar se pueden realizar por diferentes métodos, softwares y herramientas que de una u otra forma podrían afectar el funcionamiento de una red y de los diferentes dispositivos que pueden estar conectados a una red. Estos métodos no fueron usados en este estudio ya que requieren software y herramientas más complejas y difíciles de adquirir.

Para realizar estos ataques la mayoría de los ciberdelincuentes usan lo que se conoce como fuerza bruta, la cual consiste en atacar la red bajo un sistema de bots, lo que conlleva a que el router se sature de tanta información que entra y pueda colapsar, para realizar este ejercicio de simulación se utilizó un software libre conocido como WiFiSlax, el cual es un

sistema operativo basado en Linux y puede ser usado desde cualquier pc. Para realizar este ataque se debe seguir los siguientes pasos:

- Se debe tener el software en una memoria USB y que esté configurada como una memoria booteable, desde el BIOS de cualquier computador se debe configurar para que la memoria arranque y el dispositivo reconozca el sistema operativo que se encuentra en la memoria.
- Una vez arranque y reconozca el dispositivo se presentará la pantalla de inicio como la de la figura **9**.

Figura 9. *Pantalla de inicio WiFiSlax.*
Fuente: (WiFiSlax, 2021).

- Una vez en la pantalla de inicio la cual es muy parecida al funcionamiento del sistema operativo de Windows, se debe dar clic en el botón de inicio y dirigirse a la opción WiFiSlax, como se muestra en la figura 11, de ahí en

adelante el atacante puede tomar 4 distintos caminos, que se presentarán a continuación:

Usar la herramienta WPS pin la cual se ejecuta para aquellas redes que tengan el WPS activado, una característica de este ataque es que inicia a probar de forma masiva pines al azar o combinaciones de pines (fuerza bruta), cuando se establece la conexión con la red devuelve lo que es la clave WPA/WPA2 del router y ya se accedería a esta red.

Otra herramienta que viene integrada al WiFiSlax es la herramienta RouterSploit pues esta ayuda a encontrar las vulnerabilidades para atacar a los routers y elegir el método que menos tiempo tome.

La John The Ripper es otra forma de sacar contraseñas de una red, el funcionamiento de esta herramienta se basa en un algoritmo cifrado que cuenta con permisos de Hascat. Por eso lo hace una solución sumamente potente a la hora de generar caídas en la red o en el router.

Por último, se encuentra la herramienta WiFiPumpkin el cual es un framework que permite crear diversos puntos de acceso rogue, estos ataques tienen la característica de ejecución de tipo man in the middle.

Todos los métodos antes mencionados tienen el único objetivo de conocer la dirección IP tanto del router como la de los dispositivos conectados, de ahí en adelante el atacante puede mejorar su estrategia de ataque.

1.5.Ataques directos a Alexa

En el año 2017 investigadores belgas descubrieron versiones de Echo y Kindle vulnerables a KRACK, en el protocolo de seguridad de redes Wi-Fi WPA2 estos ataques son dirigidos al four-way handshake o saludo de cuatro vías, este método es usado con dos propósitos, el primero es confirmar que el cliente y el punto de acceso poseen las credenciales correctas y la segunda forma es que la negociación de la clave es usada en el cifrado del tráfico. Para esto los atacantes podían engañar al dispositivo para que se reiniciara y usará la

clave pairwise, para de esta forma elaborar y realizar retransmisiones de los mensajes de handshake criptográficos, por último, el atacante podría reconstruir el flujo del cifrado XOR y así de esa forma espiar el flujo de tráfico de la víctima. [3]

Las características de este ataque:

- Se pueden volver a transmitir paquetes de datos viejos al ejecutar un ataque de Denegación Distribuida de Servicio (DDoS).
- Permite descifrar la información que la víctima envió.
- Si se tiene una configuración débil tanto en los dispositivos como en la red se podría falsificar.
- Se puede interceptar cualquier información como contraseñas, correos, bases de datos e información personal del usuario.

La solución a este problema la encontró un grupo de investigación de ESET los cuales informaron que las vulnerabilidades CVE-2017-13077 y CVE-2017-13078 deberían ser parchadas para evitar que hubieran fugas de información.

Otra de las formas de atacar a Alexa de Amazon es por medio de un láser el cual puede calentar el diafragma del parlante. A esta falla la llamaron Light Commands u órdenes de luz y en sí es fácil de conseguir en diferentes portales de la web, con esto se garantiza que si se emite un sonido el cual viaja por el haz de luz se puede activar Alexa y darle cualquier orden, este método fue probado en otros dispositivos como Echo, Facebook portátil mini, Google home y hasta el IPhone XR fueron hackeados [4].

En un informe de Checkpoint, se encontraron que hay subdominios de Amazon/Alexa que son vulnerables pues esto se debe a la desconfiguración de recursos de origen cruzados (CORS) y tienen un mayor efecto si estas se combinan con las secuencias de sitios cruzados, se usó el Cross Site Scripting (XSS) y se obtuvo el símbolo Cross Site Request Forgery o falsificación de petición en sitios cruzados (CSRF) con este podía acceder a la información de la víctima. [5] Por medio de este ataque el delincuente puede instalar silenciosamente aplicaciones en la cuenta de Alexa del usuario; se puede obtener una lista detallada de todos las habilidades de la cuenta de los usuarios; se pueden desinstalar habilidades o funciones de Alexa; por último se puede conseguir el historial de voz y obtener la información personal de

la víctima. Ante todo, lo anterior Amazon emitió un comunicado en donde tranquilizan a los usuarios pues hasta el momento los dispositivos no habían recibido ese tipo de ataque además aclaró que por medio de actualizaciones habían arreglado y parchado esa vulnerabilidad.

En agosto de 2020 se encontró que la asistente virtual de Amazon, Alexa, tendría una vulnerabilidad de seguridad que le permitía a los atacantes eliminar o instalar recursos en la cuenta del usuario, accediendo a su historial y a sus datos personales, logrando incluso robar su información bancaria, así lo revela una investigación que realizó Check Point Research, proveedor especializado en ciberseguridad.

El ciberatacante enviaba un enlace malicioso que provenía supuestamente de Amazon y al darle clic e interactuar con Alexa por medio de la voz, tenía acceso a la información completa de la víctima, incluyendo el historial de datos bancarios, nombres del usuario, números de teléfono y dirección del domicilio, y también podía extra extraer el historial de voz de la víctima con Alexa, instalar o eliminar aplicaciones dentro de la cuenta sin ser detectado y ver la lista de recursos de la cuenta del usuario [6].

Recomendaciones:

Los datos personales que capturan los dispositivos IoT poseen un riesgo de privacidad que en la actualidad no se maneja de manera adecuada, en este sentido, se requiere una fuerte autenticación, la actualización del firmware de los dispositivos en las páginas autorizadas de los fabricantes y el seguimiento de las buenas prácticas con el fin de evitar el secuestro de datos, las inyecciones de códigos maliciosos, la interceptación de datos, entre otros.

Para evitar ser víctima de este tipo de ataques es importante evitar descargar aplicaciones que no son conocidas; adicionalmente el usuario debe tomar conciencia sobre la información está compartiendo con su dispositivo inteligente, en especial la información referente a contraseñas y credenciales bancarias.

Además, antes de descargar una nueva aplicación el usuario debe tomarse el tiempo de documentarse sobre el software con el que cuenta antes de instalarlo, verificar cuáles permisos requiere y que configuraciones de seguridad debe realizar antes de poner en operación el sistema.

Bibliografía

[1] E. Reyes, 26 Noviembre 2018. [En línea]. Available: https://expansion.mx/tecnologia/2018/11/26/tu-alexa-es-el-nuevo-blanco-del-ciber crimen. [Último acceso: 9 Julio 2021].

[2] A. Gomez Blanco, 8 Enero 2018. [En línea]. Available: https://www.bbva.com/es/ataques-ingenieria-social-evitarlos/. [Último acceso: 10 Julio 2021].

[3] M. Čermák , «Welivesecurity,» 18 Octubre 2019. [En línea]. Available: https://www.welivesecurity.com/la-es/2019/10/18/amazon-echo-kindle-vulnerable s-ataques-krack/. [Último acceso: 10 Julio 2021].

[4] El mundo, «Descubren cómo hackear Alexa y Siri con un láser situado a más de 100 metros,» *El mundo,* 5 Noviembre 2019.

[5] C. Otero, 17 Agosto 2020. [En línea]. Available: https://as.com/meristation/2020/08/14/betech/1597416149_123409.html. [Último acceso: 11 Julio 2021].

[6] P. E. Tiempo, 13 Agosto 2020. [En línea]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/vulnerabilidades-de-s eguridad-de-alexa-asistente-de-amazon-528992.

Anexos

Anexo 1. Seguridad de los dispositivos IOT.

Categoría	**Nivel de impacto**	**Tipos de activos afectados**	**Amenaza**	**Descripción**
Ataques o abusos.	Alto.	Dispositivos IoT. Backend o BaaS.	Malware.	Es un software de tipo malicioso, el cual está diseñado con malas intenciones para poder sacar información e infiltrarse sin que el usuario esté enterado, esta amenaza es la más usada por las organizaciones para robar información. [1]
		Dispositivos IoT. Instalaciones.	Kits de aprovechamiento.	Son amenazas las cuales se basan en explotar vulnerabilidades de los navegadores web, como objetivo principal es encontrar errores y puntos vulnerables para acceder al sistema IOT y de esta forma provocar un comportamiento atípico en el dispositivo. [2]

	Medio.	Instalaciones. Backend o BaaS. Información.	Ataques dirigidos.	Estas amenazas son diseñadas para que en ciertos periodos de tiempo se ejecuten y descontrolen el dispositivo. Para los autores del artículo “Hacia un ataque dirigido transferible” este ataque se hace en numerosas fases para permanecer oculto y poder obtener grandes bancos de información. [3]
	Alto.	Dispositivos IoT. Instalaciones. Backend o BaaS.	DDoS.	Este ataque busca restringir parcialmente o negar el acceso de usuarios legítimos provocando un fallo en la conectividad [4], para llevar a cabo este tipo de ataque se necesita una red de botnets.
	Medio.	Dispositivos IOT. Instalaciones.	Ataques a la privacidad.	Estas afectan la privacidad de los usuarios y están enfocados sobre todo con la ingeniería social del afectado.
		Dispositivos IOT.	Falsificación de dispositivos maliciosos.	Esto sucede cuando un dispositivo falso se hace pasar por uno original emulando un sistema IOT seguro, cuando en realidad estos tienen puertas traseras para dejar entrar al atacante.

		Dispositivos IOT. Información. Backend o BaaS.	Modificación de la información.	Es cuando el atacante manipula la información para sacar provecho y perjudicar al usuario.
Interceptación y secuestro de información.	Alto.	Dispositivos IOT. Información. Comunicaciones.	Man in the middle	En este método el atacante intercepta la información entre dispositivos y puede retrasmitir esta hacia servidores privados donde la analiza y puede sacar provecho de esta. [5]
	Medio.		Secuestro de protocolos de comunicación en la IOT	Esto sucede cuando el atacante tiene el completo acceso completamente a la información del usuario y le provoca fallos en la conexión y puede negar el servicio.
			Secuestro de sesión.	En esta modalidad el atacante asume la identidad del usuario legítimo y puede modificar o eliminar datos e información valiosa para el usuario suplantado.

		Dispositivos IOT. Información. Comunicaciones. Instalaciones.	Reconocimiento de red.	Por este medio el atacante hace un escaneo completo de todos los dispositivos que están conectados a una red y los logra identificar para irlos controlando uno a uno hasta lograr infectarlos todos.
	Medio.	Dispositivos IOT. Información. Comunicaciones.	Obtención de información.	Es un método pasivo para la obtención de información, con este se puede conocer el número de dispositivos conectados a la red y los protocolos para acceder a estos.
			Reproducción de mensajes.	Mediante una transmisión de datos se puede enviar repetitivamente o retrasar mensajes con el fin de dejar inoperativo el dispositivo.
Caídas.	Alto.	Información. Comunicaciones.	Caída de la red.	Es la interrupción involuntaria en el funcionamiento de la infraestructura de la red.

	Medio.	Dispositivos IOT. Backend o BaaS.	Fallos de dispositivos y sistemas.	Son los fallos en el sistema operativo que posee el dispositivo, provocando que no funcione ante las configuraciones que se le den.
	Alto.	Dispositivos IOT. Backend o BaaS. Información. Comunicaciones. Instalaciones	Pérdida del soporte o servicio.	En esta toda la infraestructura de la IOT se ve comprometida, pues ninguno de sus activos estará funcionando lo cual conlleva a que los dispositivos estén vulnerables a múltiples ataques.
Pérdida o daño de los activos.	Medio.	Dispositivos IOT. Backend o BaaS. Información.	Filtrado de datos.	Esto sucede cuando los datos confidenciales son expuestos en la red de forma intencional por terceros, todo esto sucede sin la autorización del usuario.

Averías o fallos.	Alta.	Dispositivos IOT. Backend o BaaS. Información. Comunicaciones.	Vulnerabilidad del software	Esto sucede sobre todo por fallos de seguridad en los softwares instalados dentro de los dispositivos.
	Medio.	Dispositivos IOT. Backend o BaaS. Información. Comunicaciones. Instalaciones.	Fallo en plataformas operadas por terceros.	Malas configuraciones de los dispositivos en uno o varios que estén conectados a la red.

Ataques físicos.	Medio.	Dispositivos IOT. Backend o BaaS. Instalaciones.	Modificación parcial o total de partes del dispositivo o sabotaje.	Esta amenaza puede suceder debido a una manipulación involuntaria o que no fue autorizada por el usuario pues se dejan los puertos expuestos y se puede acceder fácilmente al dispositivo principal y a su vez a los demás.