,

UNIVERSIDAD ESTATAL DE MILAGRO

FACULTAD CIENCIAS DE LA INGENIERÍA

TRABAJO DE TITULACIÓN DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS COMPUTACIONALES

PROPUESTA PRÁCTICA DEL EXAMEN DE GRADO O DE FIN DE CARRERA (DE CARÁCTER COMPLEXIVO)

INVESTIGACIÓN DOCUMENTAL

TEMA: ANÁLISIS DE LA VULNERABILIDAD EN EL WPA2 USANDO LA METODOLOGÍA PMKID EN PUNTOS DE ACCESOS DEL CANTÓN NARANJITO

AUTOR:

SANTOS RAMÍREZ JIMMY ABELARDO

ACOMPAÑANTE:

MGTI. BRAVO DUARTE FREDDY LENIN

Milagro, ENERO DEL 2018

ECUADOR

DERECHOS DE AUTOR

Ingeniero.
Fabricio Guevara Viejó, PhD.
RECTOR
Universidad Estatal de Milagro
Presente.

Yo, **JIMMY ABELARDO SANTOS RAMIREZ** en calidad de autor y titular de los derechos morales y patrimoniales de la propuesta práctica de la alternativa de Titulación – Examen Complexivo: Investigación Documental, modalidad presencial, mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor de la propuesta practica realizado como requisito previo para la obtención de mi Título de Grado, como aporte a la Línea de Investigación **REDES, SEGURIDAD DE LA INFORMACIÓN** de conformidad con el Art. 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, concedo a favor de la Universidad Estatal de Milagro una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Milagro para que realice la digitalización y publicación de esta propuesta practica en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Milagro, a los 14 días del mes de Enero del 2019

Firma del Estudiante
Jimmy Abelardo Santos Ramírez
CI: 1206809871

APROBACIÓN DEL TUTOR DE LA INVESTIGACIÓN DOCUMENTAL

Yo, **FREDDY LENIN BRAVO DUARTE** en mi calidad de tutor de la Investigación Documental como Propuesta práctica del Examen de grado o de fin de carrera (de carácter complexivo), elaborado por el estudiante **JIMMY ABELARDO SANTOS RAMIREZ**, cuyo tema de trabajo de Titulación es **ANÁLISIS DE LA VULNERABILIDAD EN EL WPA2 USANDO LA METODOLOGÍA PMKID EN PUNTOS DE ACCESOS DEL CANTÓN NARANJITO**, que aporta a la Línea de Investigación **REDES, SEGURIDAD DE LA INFORMACIÓN** previo a la obtención del Grado **INGENIERO EN SISTEMAS COMPUTACIONALES**; trabajo de titulación que consiste en una propuesta innovadora que contiene, como mínimo, una investigación exploratoria y diagnóstica, base conceptual, conclusiones y fuentes de consulta, considero que el mismo reúne los requisitos y méritos necesarios para ser sometido a la evaluación por parte del tribunal calificador que se designe, por lo que lo APRUEBO, a fin de que el trabajo sea habilitado para continuar con el proceso de titulación de la alternativa de del Examen de grado o de fin de carrera (de carácter complexivo) de la Universidad Estatal de Milagro.

En la ciudad de Milagro, a los 14 días del mes de Enero del 2019.

FREDDY LENIN BRAVO DUARTE
Tutor
C.I.: 0913170528

APROBACIÓN DEL TRIBUNAL CALIFICADOR

El tribunal calificador constituido por:

FREDDY LENIN BRAVO DUARTE

MIRELLA AZUCENA CORREA PERALTA

JAVIER RICARDO BERMEO PAUCAR

Luego de realizar la revisión de la Investigación Documental como propuesta practica, previo a la obtención del título (o grado académico) de **Ingeniero en Sistemas Computacionales** presentado por el señor **Jimmy Abelardo Santos Ramírez**.

Con el tema de trabajo de Titulación: **ANÁLISIS DE LA VULNERABILIDAD EN EL WPA2 USANDO LA METODOLOGÍA PMKID EN PUNTOS DE ACCESOS DEL CANTÓN NARANJITO**.

Otorga a la presente Investigación Documental como propuesta práctica, las siguientes calificaciones:

Investigación documental	[80]
Defensa oral	[20]
Total	[100]

Emite el siguiente veredicto: (aprobado/reprobado) APROBADO

Fecha: 14 de Enero del 2019.

Para constancia de lo actuado firman:

	Nombres y Apellidos	Firma
Presidente	FREDDY LENIN BRAVO DUARTE	
Secretario /a	MIRELLA AZUCENA CORREA PERALTA	
Integrante	JAVIER RICARDO BERMEO PAUCAR	

DEDICATORIA

Dedico este trabajo a mis padres, quienes fueron parte fundamental en este largo proceso, mi papá Víctor Santos que nunca dejó de apoyarme tanto económicamente y emocionalmente, por impulsarme a continuar en esta carrera y a mi madre Glenda Ramírez por su apoyo incondicional y paciencia, por nunca perder la fe en mí y acompañarme durante todo este proceso de formación profesional.

Jimmy Santos Ramírez

AGRADECIMIENTO

Agradecido de Dios en primer lugar porque sin él no hubiese podido llegar hasta este momento, ha sido mi guía y mi fuerza para continuar.

Agradezco a mi familia por su apoyo y palabras de aliento, en especial a quienes se convirtieron en el pilar fundamental y mi motivación para culminar este gran reto que son mis hermanos Sheyla y Jeremy.

Quiero agradecer de manera muy especial a mi mejor amiga Ruth que siempre estuvo apoyándome, viajando de muy lejos para ayudarme en este trabajo y darme ánimos en todo tiempo, también por tener mucha paciencia conmigo.

A mis compañeros de salón de clases a Roxana, Julio y Juan que se convirtieron en grandes amigos, por los cientos de horas que pasamos juntos solucionando problemas e ir superando asignaturas y sobre todo por la gran amistad que brindaron durante todo este tiempo, en especial a Juan Cañar que siempre estuvo presto para colaborar con este trabajo.

A los docentes que siempre tuvieron la buena voluntad de ayudar e impartir sus conocimientos, aquellos que motivan a que se puede llegar a ser un gran profesional con ética y responsabilidad, sobre todo por los grandes retos que impartieron en el transcurso de la carrera y motivaron a amar más la profesión que se escogió.

Y por ultimo y no menos importante agradecer al resto de mis amigos y compañeros que hicieron que este tiempo en la universidad sea mas que un centro de estudio, una segunda casa.

Y todo lo que hagan, de palabra o de obra, háganlo en el nombre del Señor Jesús, dando gracias a Dios el Padre por medio de él. Colosenses 3:17

Jimmy Santos Ramírez

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ANÁLISIS DE LA VULNERABILIDAD EN EL WPA2 USANDO LA METODOLOGÍA PMKID EN PUNTOS DE ACCESOS DEL CANTÓN NARANJITO

RESUMEN

En la última década se ha visto la evolución de diferentes mecanismos de seguridad para la protección de información, por tal motivo el IEEE (Institute of Electrical and Electronics Engineers) ha desarrollado estándares de protección de datos que impulsó a la aparición de uno de los protocolos más confiables el cual es WPA/WPA2 que desde su aparición hasta la actualidad no había sido vulnerada. En agosto del 2018 Jens 'Atom' Steube desarrollador principal de Hashcat descubrió que este protocolo tenía sus fallas y que solo basta con capturar el PMKID para acceder al área de red local inalámbrica.

Es necesario conocer qué tan expuestos están nuestros enrutadores, cuáles son los que se encuentran con mayor exposición al ataque y si hay alguna manera de prevenir esta arremetida, razón por la cual se ha procedido a la realización de diversas pruebas en distintos routers, de manera que verificaremos la magnitud de alcance que tiene esta nueva técnica de craqueo de contraseñas.

La exploración de distintos puntos de acceso en diferentes partes del cantón Naranjito, permitió tener una visión mucho mas amplia en lo que concierne a la obtención del identificador de clave PMKID y el debido análisis corroborado con las pruebas realizadas durante este período, así como la debida documentación de estos procesos.

Estudios realizados anteriormente revelan la importancia de seguir actualizándose en lo que a seguridad informática se refiere, estos ataques de intento de robar contraseña han ido evolucionando a medida que el tiempo avanza, desde su primera aparición como lo fue WEP hasta el día de hoy, todos estos ataques han sido publicados en diferentes medios, sean en blogs, revistas o foros, algunos libros también nos enseñan como craquear contraseñas, todo esto con la finalidad de proteger nuestros datos.

PALABRAS CLAVE: PMKID, Vulnerabilidad, WPA2, Enrutador.

ANALYSIS OF VULNERABILITY IN THE WPA2 USING THE PMKID METHODOLOGY IN THE CANTON NARANJITO ACCESS POINTS

ABSTRACT

In the last decade we have seen the evolution of different security mechanisms for the protection of information, for this reason the IEEE (Institute of Electrical and Electronics Engineers) has developed data protection standards that led to the emergence of one of the protocols most reliable which is WPA / WPA2 that since its appearance until now had not been violated. In August 2018, Jens 'Atom' Steube, the main developer of Hashcat, discovered that this protocol had its faults and that it is enough to capture the PMKID to access the local wireless network area.

It is necessary to know how exposed our routers are, which are the ones that are most exposed to the attack and if there is any way to prevent this attack, which is why we have proceeded to carry out various tests on different routers, in a way that we will verify the magnitude of reach that this new technique of cracking of passwords has.

The exploration of different access points in different parts of the Naranjito, allowed to have a much wider vision regarding the obtaining of the PMKID key identifier and the due analysis corroborated with the tests carried out during this period, as well as the due documentation of these processes.

Previous studies reveal the importance of continuing to update in terms of computer security, these attempts to steal password have evolved as the time progresses, from its first appearance as it was WEP to today, all These attacks have been published in different media, whether in blogs, magazines or forums, some books also teach us how to crack passwords, all with the purpose of protecting our data.

KEY WORDS: PMKID, Vulnerability, WPA2, Router.

INTRODUCCIÓN

La seguridad informática es un tema muy poco tratado a nivel de hogares o pequeños negocios, en vista de que la tecnología ha invadido nuestras vidas, es importante conocer los riesgos que existen en la actualidad, teniendo en cuenta que cada dispositivo que poseemos sean estos tablets, smartphones, televisores, laptops, etc., están conectados al internet y por consiguiente el puente que usan estos dispositivos para interconectarse es el router. En la actualidad existen hogares digitales que usan enrutadores para que todos los medios que se encuentren dentro estén conectados entre sí.

Los puntos de acceso en su mayoría vienen con una configuración estándar y muy poca segura en lo que a protección de la misma se refiere, tal motivo ha hecho que muchas personas con conocimientos básicos en redes quieran robar contraseñas sean estas de un hogar o de una pequeña empresa, muchos de los atacantes solo buscan la contraseña para poder tener acceso al internet, pero si el caso es otro, donde nuestro atacante busque causar daños como robo de información o tener control de los dispositivos conectados a esta red, es por tal motivo que debemos prevenir que nuestra seguridad sea burlada.
Es razón por la cual necesitaremos estar conscientes del nivel de seguridad que ofrecen dichos mecanismos.

Entre los estándares que el IEEE desarrollo se encuentra el WPA2 que se considera uno de los protocolos más seguros en la actualidad, es por esto por lo que se buscará analizar la vulnerabilidad a través de un ataque de captura de PMKID.

El siguiente estudio este compuesto por cinco capítulos que están conformados por:

Capítulo 1: encontraremos nuestro problema, objetivo general, objetivo específico y la justificación del problema.

Capítulo 2: está constituido por el marco teórico conceptual en el que encontraremos todo lo referente a terminología que usaremos en el proyecto presente, antecedentes históricos de estudios similares al nuestro en el que nos apoyaremos.

Capítulo 3: se encuentra la metodología que usamos al realizar nuestro trabajo, que son la metodología descriptiva, documental y de campo.

Capítulo 4: tenemos el desarrollo del proyecto donde encontraremos el análisis de las pruebas realizas en los distintos puntos de acceso en el cantón Naranjito.

Capítulo 5: se concluye con los resultados obtenidos en nuestro análisis de vulnerabilidad en el WPA2 capturando el PMKID.

CAPÍTULO 1

PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

En la actualidad la necesidad de tener acceso al Internet forma parte de la vida cotidiana de las personas, desde su creación hasta el día de hoy se han desarrollado múltiples modos de conectarse a la misma, uno de los medios para el acceso al Internet es a través de las redes inalámbricas (Wireless).

Para que un dispositivo tenga acceso al internet de manera inalámbrica, es a través de un router inalámbrico, que por consiguiente la entrada a la red está protegida por una contraseña, la que nos servirá para controlar a quien se le dará autorización de que pueda conectarse a la red. Con el transcurso de los años esta ha sido víctima de diversos tipos de ataques que han intentado robar la clave, en muchos casos teniendo éxito, por tal motivo se sumó la necesidad de desarrollar diferentes mecanismos de protección para la integridad y privacidad de la información, como lo es el protocolo WPA2 (Wireless Protected Access 2).

En una red inalámbrica local también denominada WLAN (Wireless Local Area Network) que usa WPA2, un estándar del IEEE (Institute of Electronical and Electronics Engineers) protocolo de seguridad que se consideraba uno de los más seguros hasta el día de hoy, se ha visto vulnerable ante un nuevo ataque, el cual deja al descubierto que luego de 14 años desde su creación (desde el 2004) tiene sus fallas (Hashcat, 2018).

Desafortunadamente hasta el día de hoy muchos de estos enrutadores que usan WPA/WPA2 se han visto violentados y así lograr su objetivo de obtener la contraseña, motivo por el cual es necesario analizar qué tan vulnerables son los router ante esta nueva amenaza, que pone en peligro el robo de información de los usuarios conectados a una WLAN.

1.2 Objetivos

1.2.1 Objetivo general

Analizar los distintos routers en el cantón Naranjito que puedan ser susceptibles a la vulnerabilidad del ataque al protocolo WPA2 mediante la captura del PMKID.

1.2.2 Objetivos específicos

1. Enumerar las herramientas adecuadas que permitan la captura del identificador de clave PMKID.
2. Analizar distintas redes con las herramientas que permiten la captura del PMKID.
3. Identificar qué tipo de routers aún son vulnerables en el método de captura del PMKID del protocolo WPA2.

1.3 Justificación del problema

Dado a que vivimos en mundo lleno de tecnología y con más usuarios conectados al internet mediante una red inalámbrica, ya sean estos por dispositivos móviles, tabletas o televisores, el intento de robar la contraseña presente en los enrutadores se ha vuelto cada vez más popular, por lo cual se ha visto en la necesidad de tener un conocimiento mucho más amplio en lo que respecta a la seguridad informática, en este caso, protegernos ante posibles ataques y tomar medidas necesarias.

Es decir, analizar una parte de las marcas conocidas de routers modernos, para verificar si estos son propensos a ser vulnerables frente a esta nueva amenaza, y la probabilidad de que no se violente nuestra WLAN.

Ante el intento de forzar la seguridad de este protocolo las redes inalámbricas han hecho que más personas con conocimientos técnicos intenten usar estas vulnerabilidades para acceder a robar contraseñas e información dentro de una red, es por tal razón que se ha decidido analizar las vulnerabilidades que existen en el protocolo WPA2.

CAPÍTULO 2

MARCO TEÓRICO CONCEPTUAL

2.1 Antecedentes históricos

La red inalámbrica tuvo su origen en 1997 con el estándar 802.11. Dos años más tarde en 1999, fue presentado un algoritmo de seguridad para redes inalámbricas Protección de equivalencia a cableado (WEP) siendo el primer intento de brindar seguridad. Por el año 2001 hallan un fallo importante y crítico en WEP. Siendo así que en el 2003 se incluyó Wi-Fi Protected Access (WPA) una medida momentánea para el fallo de WEP, la cual dio paso en el año 2004 a WPA2, siendo este protocolo que utilizó en su totalidad el estándar 802.11i (Méndez, Mosquera, & Rivas, 2015).

En una primera versión del protocolo 802.11 que fue el protocolo WEP dejó de ser seguro, ya que, en el 2001, salió a la luz el software aircrack-ng, que logro adivinar la contraseña de una red Wi-Fi con un WEP en cuestión de minutos.

La unión de varias compañías de tecnología de la comunicación dio paso a la creación de una organización que sería la responsable específicamente de los protocolos de comunicación inalámbrica allá por el año de 1999. Dicha organización se llamó WECA, pero en el 2002 fue reconstruida como Wi-Fi Alliance, quien es el propietario de Wi-Fi y sobre quien recae la definición, promoción y emisión de la tecnología Wi-Fi, y el encargado de crear sistemas de seguridad para dicha tecnología.

Wifi Alliance se vio en la necesidad de sacar un protocolo llamado WPA (acceso protegido a Wi-Fi) en 2003. La misma que fue tomada como una medida temporal, ante la falla que presentó WEP. Por consiguiente, en el 2004, extrajo WPA2, que desde aquel entonces ha sido usado como un protocolo estándar de seguridad para redes Wi-Fi.

Los autores (Verbel & Alvarez, 2016) nos mencionan algunos tipos de protocolos que son utilizados en la seguridad de WiFi.

- WEP (Wired Equivalent Privacy o Privacidad Equivalente al Cable). Un sistema cifrado asociado al protocolo 820.11. Utiliza una clave simétrica. Considerado el menos seguro de todos, debido a que romperlo es fácil, siempre y cuando la persona tenga los conocimientos informáticos adecuados.
- WPA (WiFi Protected Access o Protección de Acceso WiFi). La evolución del WEP, un poco más robusto que el anterior, a pesar de que la longitud de claves es inferior a la de su antecesor, el método que utiliza para el cifrado es más robusto.
- WPA2 (WiFi Protected Access o Protección de Acceso WiFi, versión 2). Un método que es considerado uno de los más seguros por su algoritmo de cifrado AES (Advanced Encryption Standard), por esta razón tratar de romperla es mucho más complicada.
- WPA PSK (WiFi Protected Access Pre-Share Key o Protección de Acceso con Clave Pre compartida). A diferencia del otro método anterior es que existe una clave compartida por todos los que forman la red previamente a la comunicación.

El WPA2 ha sido considerado como un buen sistema, porque no se localizó ningún agujero de seguridad grave, puesto que han pasado muchos años desde su inicio se ha mantenido seguro. Pero al mismo tiempo, como todo en el mundo tecnológico nada es perfecto, se descubrieron que tienen varios errores. Para ilustrar mejor estos errores daremos un ejemplo, si la contraseña que el usuario asigna es corta o débil, utilizando el software aircrack-ng se puede encontrar fácilmente. No obstante, si sabemos la contraseña, toda la información que viaje en mensajes cifrados con esta contraseña se pueden descifrar antes y después, lo cual se interpreta que cualquier persona puede ver los mensajes en hoteles, cafés y otros lugares públicos. Asimismo, han evidenciado que el sistema WPS el cual se conecta a dispositivos pequeños también tiene sus desperfectos.

La figura 1 evidencia como las normas inalámbricas han ido evolucionando desde 1999 hasta la actualidad.

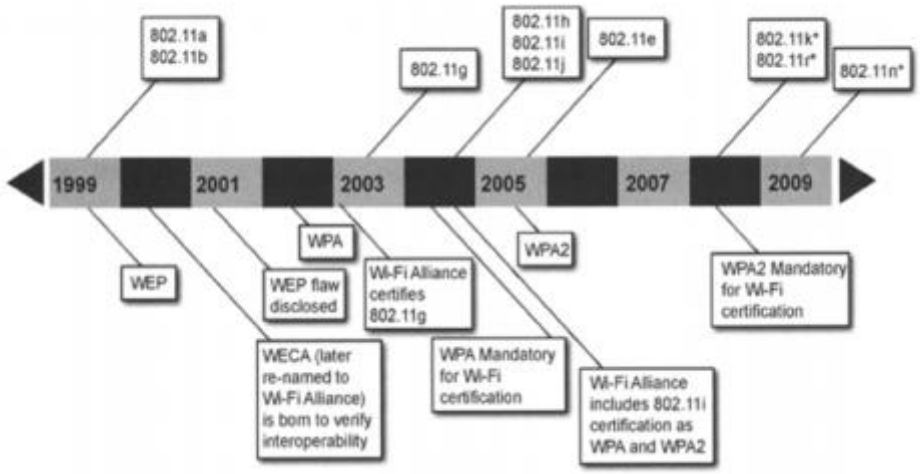

Figura 1. Línea del tiempo de evolución de normas inalámbricas.

Fuente: Adaptado de Méndez, Mosquera y Rivas (2015)

2.2 Antecedentes de la investigación

Según (Cuchillac, 2014) la vulnerabilidad en WPA dependerá única y exclusivamente del tipo de clave o contraseña que se le asigne, puesto que si el usuario asignó una clave que esté contenida en diccionarios, en efecto el riesgo que tiene de que un atacante la encuentre será notablemente alta.

```
root@kali:~# aircrack-ng -b  B8:A3:86:AA:BB:01
          -w /usr/share/wordlists/sqlmap.txt /root/capturaWPA-01.cap

                              Aircrack-ng 1.2 beta3

                [00:07:26] 594600 keys tested (3983.79 k/s)

                          KEY FOUND! [ q123456789 ]

     Master Key     : 07 BD BB C8 AA 07 E2 DB 04 25 97 F8 BE 78 FC 3A
                      6C 6D E6 67 B9 98 8C 84 BB 0F 3D 06 90 17 F1 83

     Transient Key  : 63 79 C3 27 22 0B B6 24 59 09 95 0A 1A FF D0 EC
                      5A 90 40 21 05 92 07 39 9C FA 92 B5 37 B4 7D BA
                      D1 5C 24 DE CC 01 27 E0 4D B9 F0 80 AA 55 FF 5A
                      E8 B4 06 6C 83 16 10 54 82 C8 47 0B D4 5B C4 32

     EAPOL HMAC     : A7 29 85 25 48 B0 DD 99 27 97 A9 2C 4E 18 06 83
```

Figura 2. Desencriptación de la clave WPA.

Fuente: Adaptado de Cuchillac (2014)

Para (Monsalve Pulido, Aponte Novoa, & Chaparro Becerra, 2015) el tiempo que puede tardar en descifrar WPA es aproximadamente 6 horas en el caso de que no se cuente con un diccionario el cual permita comparar la llave de entrada con esta base de datos, de cierto modo WPA nos presenta un método más eficaz en cuanto a la seguridad de nuestros datos en una red Wifi. Por otra parte, un ataque de denegación de servicio con la intención de capturar la llave pre compartida hace que este método sea más transcendente, puesto que se obliga a que el usuario original se desconecte.

Para considerar segura una red Wifi con WPA2 se debe considerar una clave que supere 12 dígitos en las que se incorporen números, letras y símbolos. Encontrarla es casi imposible por esta razón podemos llamarla segura. El termino segura en este caso, es porque sería una pérdida de tiempo tratar de descifrar una clave que puede tener millones de combinaciones (Díaz, 2016).

Por consiguiente, dado que vivimos en un mundo donde todos estamos conectados a Internet de alguna forma u otra, desde nuestros dispositivos móviles o pc, no es difícil localizar un dispositivo de acceso Wifi como un enrutador, de tal forma es frecuente encontrar a personas escaneando redes para obtener una conexión Wifi disponible (Verbel & Alvarez, 2016).

Los autores (Monsalve Pulido et al., 2015) muestran que según el estudio realizado las redes analizadas arrojaron como resultado que un 68.67% tienen una autenticación WPA, cuya distribución está en un 44.64% y WPA2 en un 24%, de manera que el 31.1% de las redes que fueron sometidas a estudios presentan un nivel bajo de seguridad, que es representado en un 22% con autenticación WEP.

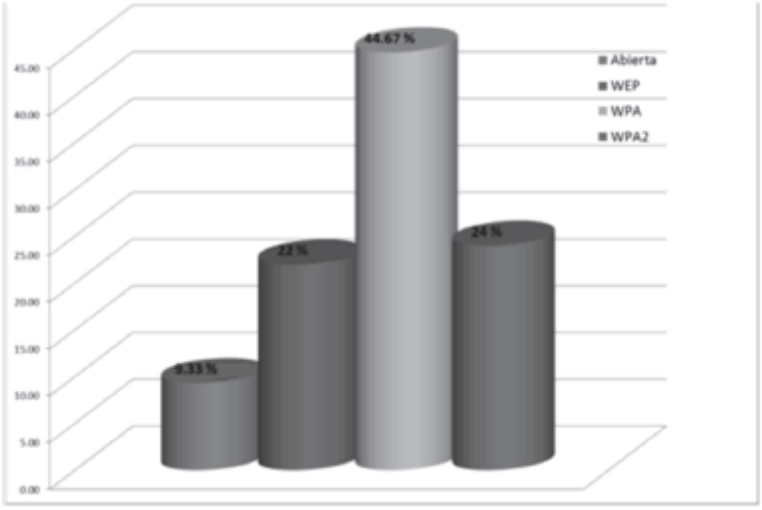

Figura 3. Distribución de la seguridad en Wlan.

Fuente: Adaptado de Monsalve, Aponte y Chaparro (2015).

Según (Motyka, 2017) la seguridad WPA2 se ha visto expuesta ante un nuevo ataque, la cual deja en duda la seguridad que este protocolo presentaba, la forma que se empleaba para proteger la conexión no es tan inaccesible como se consideraba, puesto que ha quedado descubierto la forma de saltársela, para de esta manera interceptar todos los datos que pasan por tu Wifi.

Hemos llegado al punto en donde decimos que la seguridad en internet ya no es tan segura, puesto que cada vez se descubren nuevos ataques a los protocolos que considerábamos seguros, es por tal razón que próximamente estará disponible el protocolo WPA3.

La definición de red inalámbrica, según (Machicao, 2015) nos dice que," Es la interconexión de distintos dispositivos con la capacidad de compartir información entre ellos, pero sin un medio físico de transmisión, Wi-Fi ("Wireless Fidelity"): en lenguaje español significa literalmente fidelidad sin cables. También se les denomina WLAN ("Wireless Local Area Network") o redes de área local inalámbricas" (p. 13).

Figura 4. Red inalámbrica

Fuente: https://tecnologia-informatica.com/que-es-red-inalambrica-seguridad-wifi/

"El IEEE 802.11 es un estándar que define como se utilizan las frecuencias de radio en las bandas de frecuencia ISM (Industrial, Scientific, and Medical) no autorizadas para la capa física y la subcapa MAC de enlaces inalámbricos" (Lewis, 2009, p. 420).

El autor (Lewis, 2009) afirma que:

> Normalmente, la elección del estándar WLAN a utilizar depende de las velocidades de datos. Por ejemplo, el 802.11 a y g pueden soportar 54 Mbps, mientras que el 802.11 b solo llega a un máximo de 11 11Mbps. Esto hace que este estándar sea el más lento y que el 802.11 a y 802.11 g sean las principales elecciones. Un cuarto borrador de la WLAN, el 802.11 n, supera las velocidades de datos disponibles en la actualidad. EL IEEE 802.11 n debería ser ratificado a finales del 2009 o principios del 2010 (p. 420).

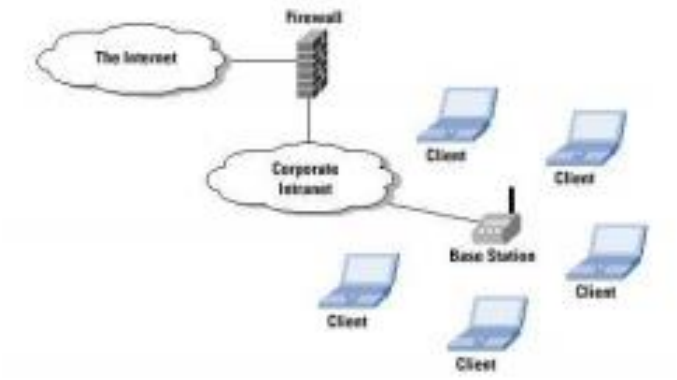

Figura 5. IEEE 802.11

Fuente: Adaptado de Vargas (2015)

El estándar 802.11b salió en 1999, que se diferenció de su antecesor por el uso exclusivo de la modulación DSSS (Direct Sequence Spread Spectrum) con un sistema de codificación CCK. Fue quien lideró el estándar de redes inalámbricas, con velocidades de transmisión: 1, 2, 5.5 y 11 Mbps (Verbel & Alvarez, 2016).

DRS (Dynamic Rate Shifting) fue una de las características que éste estándar presentó, haciendo que las velocidades de los adaptadores de red inalámbricos puedan ser reducidas para retribuir problemas de recepción presentes en el camino que le toca atravesar (paredes, ventanas, etc.).

Según (Machicao, 2015) el estándar 802.11a, utiliza una técnica de modulación de radio OFDM (Ortogonal Frequency Division Multiplexing) y cuya banda de frecuencia es de 5 GHz. La velocidad de transmisión puede llegar hasta 54 Mbps. También tiene una capacidad para hacer comunicaciones al mismo tiempo, del cual dispone de hasta 8 canales sin solapamiento.

Para (Amado, 2008) el estándar 802.11i viene a ser un protocolo complejo y fiable, siempre y cuando sea usado de la forma correcta. Pero no está librado de un ataque de diccionario y fuerza bruta. Ya que el proceso de autenticación que emplea es el llamado saludo de cuatro

vías o “4 way-handshake”, el cual consta del intercambio de 4 paquetes para gestionar el acceso a la red.

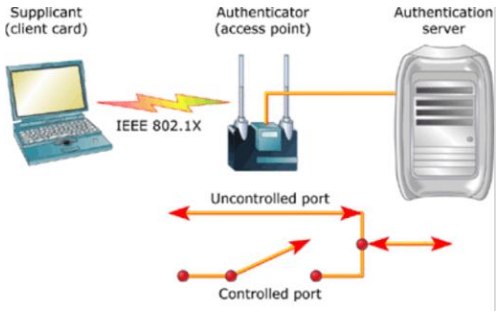

Figura 6. IEEE 802.11i

Fuente: https://www.timetoast.com/timelines/familia-de-estandares-ieee-802-11-81f2faf2-5945-4963-8bde-8dd3adb550fc

Para (Guerrero-Ibáñez, Flores-Cortés, Barba Marti, & Reyes, n.d.) el estándar IEEE 802.11p que fue publicada en el 2010, trabaja en frecuencias de 5.90GHz y 6.20GHz. Este estándar es especialmente para automóviles, cuya comunicación e intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

El estándar IEEE 802.11r cuya aparición fue en el 2010 es también conocido como Fast Basic Service Set Transition, que tiene como principal característica otorgar a la red fijar protocolos de seguridad que reconozcan al dispositivo en el nuevo punto de acceso antes de que desista del actual. El tiempo que esta función permite la transición entre los nodos es de menos de 50 milisegundos (Peñaranda, 2010).

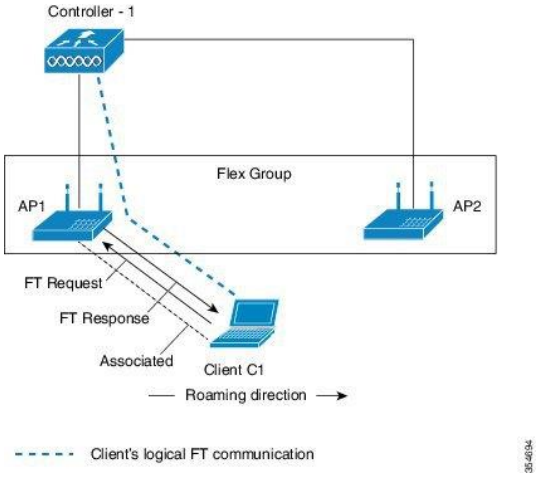

Figura 7. IEEE 802.11r

Fuente: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html

El autor (Romero, 2013) ha compilado un glosario que nos ayudará a entender mejor los acrónimos citados en esta investigación, como también los significados de cada término al que hace referencia, aquí una breve descripción:

- **AAA:** Authentication, Authorization and Accounting, usado en sistemas distribuidos, hace mención de una arquitectura de seguridad cuyo objetivo es el de establecer las medidas de seguridad para el control de autenticación, autorización y auditoria de los usuarios. Su significado también puede estar ligado a un servidor que implemente ciertos mecanismos de seguridad. También puede hacer referencia a una clave que se deriva de la MSK, que es generada a partir de la autenticación EAP. Esta clave AAA concede que se derive una clave temporal de sesión de alguna manera depende de la suite de cifrado usada.
- **ACK:** Acknowledgment, este se refiere a un tipo de trama de control por la cual una estación afirma que la trama de datos, de gestión o incluso una trama de tipo PS-Poll (en el caso de un AP) ha llegado a su destino, es así que un ejemplar de trama es dirigido hacia el emisor de la trama recibida.
- **AP:** Access Point, traducido es un punto de acceso la cual se lo conoce como nodo (estación) distinguido de una red 802.11 que trabaja en modo Infraestructura. Es por medio de este punto de acceso, que las demás estaciones pueden acceder al sistema de distribución de la red, pero que también puede desempeñar otras funciones.

- **BSS:** Basic Service Set, se denomina al conjunto de estaciones 802.11, que comparten la misma función de coordinación, es decir, todas las estaciones que pertenecen a una red 802.11 opera en modo Ad-Hoc.
- **BSSID:** BSS Identification, es un identificador de 48 bits, muy parecida a una dirección MAC con el formato IEEE 802, que hace que se identifique de una forma que nadie más se le parezca. A diferencia del BSS que opera en modo Infraestructura, el BSSID coincide con la dirección MAC del AP que pertenece al BSS, por el contrario, un IBSS lo realiza a partir de un numero aleatorio de 46 bits.
- **CCK:** Complementary Code Keying, es una técnica de modulación que se basa en la codificación a través de espectro expandido, que tiene una modulación digital por medio de DQPSK el cual también hace uso de un código de Walsh-Hadamard de 8 chips, siendo así que puede llegar a obtener una velocidad de transmisión de 5.5 o de 11 Mbps, en función del código de expansión que aplica.
- **CCM:** Counter mode with Cipher-block chaining Message authentication code, modo de cifrado para algoritmo de cifrado en bloque mediante clave simétrica que a su vez se vale de otros modos de cifrado en bloque diferentes para que la información no sea alterada ni robada, estos otros modos de cifrado son: modo Contador que cuida la privacidad de los datos y el modo CBC-MAC, para conservar la integridad y autenticidad del origen de los datos.
- **CCMP:** Counter mode with CBC-MAC Protocol, protocolo de seguridad incorporado en la enmienda 802.11i, la cual se debe implementar obligatoriamente en todas las estaciones compatibles con las RSNs, de modo que utiliza el algoritmo de cifrado AES en modo CCM con una clave de 128 bits para dar abastecer la seguridad necesaria a los datos que se encuentren vinculados a una asociación de seguridad que se fundamenta en este protocolo.
- **DQPSK:** Differential Quadrature Phase Shift Keying, modulación que utiliza desplazamiento diferencial de fase en cuadratura, es decir, una técnica en la cual cada bit está interpretado por una diferencia de fase de 0° o bien de 180° que están en medio de dos elementos seguidos de la señal.
- **EAP:** Extensible Authentication Protocol, protocolo que simplifica la autenticación de usuarios o dispositivos a causa de que establece un marco de trabajo para la autenticación, el cual puede ser extendido a través de la agregación de métodos nuevos o procedimientos de autenticación.

- **EAPOL:** EAP Over Lan, es el formato de paquetes de red definido en el estándar IEEE 802.1X que transportan los paquetes EAP que se interaccionan entre un Cliente (Supllicant) y un Autenticador, las cuales también abarcan datos transmitidos por ambos tipos de entidades con la finalidad de originar material de claves.
- **IEEE:** Institute of Electrical and Electronics Engineers, esta organización promueve la innovación y excelencia teconológica que se compone de profesionales que impulsan el desarrollo de estándares en distintos ámbitos industriales.
- **KCK:** Key Confirmation Key, clave de 128 bits el cual pertenece a la PTK y se emplea para la verificación de autenticidad/integridad de paquetes tipo EAPOL-Key que trasladan algunos mensajes del 4-Way Handshake o del Group Key Handshake, con la ayuda de la función hash basada en clave HMAC-MD5 o HMAC-SHA1-128.
- **MAC:** Medium Access Control, de las dos subcapas que se divide la capa de enlace esta viene a ser la subcapa inferior. El control de acceso y direccionamiento de los nodos que comparten el medio de transmisión, empaquetamiento y fragmentación de MSDUs a través de MPDUs y el control de errores de estas últimas vienen a ser una de las funciones que desempeña esta subcapa.
- **PKI:** Public Key Infraestructure, hace referencia a una estructura, que incluye sistemas, aplicaciones, personas, políticas y procedimientos, que se dedican a originar, gestionar, distribuir, usar y revocar certificados digitales. La asociación de entidades de un conjunto u otras entidades a las claves públicas asignadas es el objetivo primordial de dicha infraestructura.
- **PMK:** Pairwise Master Key, derivada de la clave MSK es una llave maestra de 256 bits, a través de la autenticación 802.1X, que solo es válida durante la sesión en la que dicha autenticación tiene vigencia, o que coincide con una clave estática que es configurada gracias a un método "fuera de banda", conocida también como PSK. En dichos casos, la PMK es utilizada para la generación de la PTK.
- **PSK:** Pre-Shared Key, es una clave maestra de 256 bits que es utilizada para el intercambio de datos bajo la protección de WPA o WPA2 que a su vez puede ser configurada en dos o más estaciones de un BSS. Esta configuración de dos estaciones de la misma instancia de la PSK funciona como mecanismo de autenticación implícita entre dichas estaciones. También, la PSK ejerce el rol de la PMK en las estaciones que haces uso de este tipo de autenticación.

- **PTK:** Pairwise Transient Key, es una colección de claves momentáneas con una longitud de 384 o 512 bis, que según la suite de cifrado unicast que se use sea esta CCMP o TKIP respectivamente. Esta colección derivada del PMK mediante el 4-Way Handshake contiene claves llamadas KCK, KEK y TK, por lo cual es válida en tanto que la sesión este vigente.
- **SSID:** Service Set Identifier, identificador lógico, es una cadena de caracteres que esta codificada en ASCII que no sobrepasa los 32 bytes, que identifica una red 802.11.
- **STA:** Station, es un nodo de red implementada conforme al estándar 802.11, es decir, un dispositivo compatible con las todas las especificaciones de este estándar e integrado en una red de esta clase.
- **TK:** Temporal Key, es una clave incluida en un PTK o un GTK, que es usada para el cifrado y la verificación de autenticidad/integridad de los datos correspondientes al tráfico unicast o de broadcast/multicast, respectivamente. El tamaño de esta clave actualmente puede estar entre 128 o 256 bits, dependiendo de que la PTK o la GTK que la contiene se encuentre vinculada a la suite de cifrado CCMP o TKIP.
- **TKIP:** Temporal Key Integrity Protocol, es un protocolo de seguridad que fue introducida en WPA para mejorar las debilidades de WEP. TKIP protege la privacidad mediante una clave RC4 de 128 bits y la autenticidad mediante el algoritmo Michael y dos claves de 64 bits.

Hashcat es una herramienta de craqueo de hash de contraseña multiplataforma, de código abierto y gratuita, optimizada para aprovechar al máximo la capacidad de procesamiento de las GPU en las tarjetas gráficas modernas y en la CPU. Puede descargar el hashcat desde https://hashcat.net/hashcat/ (Burrough, 2018).

Jhon the Ripper también es principalmente un programa de descifrado de contraseñas de UNIX, pero difiere de Crack porque puede ejecutarse no solo en UNIX SYSTEMS, sino también en Windows NT / 9x. John the Ripper se usa principalmente para las contraseñas de UNIX, pero tiene una opción para romper los hashes de Windows NT LM (Russell, 2000).

PMKID

Al referirnos del PMKID, se dice que solo se requerirá el primer mensaje de handshake. Es decir, el primer mensaje en handshake contiene un campo llamado PMKID (identificador de PMK). El valor de este identificador se calcula utilizando el algoritmo sha1 de HMAC derivado de la clave maestra de Pairwise (PMK). PMK se deriva del algoritmo PBKDF2 utilizando la clave de frase de contraseña real y el ESSID de la red como sal. Bueno, en una declaración lógica básica, la compilación PMKID debería escribirse de esta forma:

PMKID = HMAC-SHA-128 (PMK, Nombre de PMK "+ AP MAC + STA MAC)

Básicamente, es la función HMAC de las PMK derivadas como la clave y la concatenación de una cadena fija y los MAC de AP y el Cliente como los datos para funcionar.

Entonces, la tarea básica que tenemos es hacer que el AP envíe un mensaje de saludo. El EAPOL se lleva a cabo después del proceso de autenticación y asociación entre STA y AP, que en resumen es verificar la compatibilidad de ambos lados. Sin embargo, dependiendo de la intensidad de la señal STA y otras capacidades, el AP puede elegir no responder con los marcos EAPOL.

CAPÍTULO 3

METODOLOGÍA

3.1 Metodología descriptiva

El tipo de investigación descriptiva nos dice que lo principal, es la descripción de ciertas características básicas del sujeto, por ende, este tipo de investigación nos pone en manifiesto como es el comportamiento del fenómeno a estudio, es decir cuando su objetivo se basa en describir, calcular o pronosticar algo relacionado al sujeto de estudio (Namakforoosh, 2000).

Un estudio descriptivo según (Hernández Sampieri, Fernández-Collado, & Baptista, 2006) nos manifiestan que, "busca especificar las propiedades, las características y los perfiles de personas, (…) o cualquier otro fenómeno que se someta a un análisis" (p. 82). Por lo que podemos decir que esta metodología es quien ayudará a recolectar la información necesaria. Ya que nuestra investigación se basa al análisis de vulnerabilidades, es adecuada para que nuestro estudio se vea respaldado al mostrar con exactitud qué enrutadores son más propensos a este ataque de PMKID con la herramienta Wifibroot y cómo podemos defendernos ante el mismo.

3.2 Metodología documental

Este tipo de investigación es quien nos ayudará a analizar la información escrita, cuyo fin será el de detectar, obtener y consultar distintos materiales, aquellos que nacen de otros conocimientos. Con la finalidad de que estos sean útiles para nuestro estudio (Bernal, 2006).

La revisión de informes y estudios hará que nuestro principal objetivo sea el de conocer los riesgos, ataques y soluciones que se han dado. La misma nos será útil para conocer que herramientas ya están descontinuadas y a cuáles se les ha dado una mejora, si las mismas son gratuitas o son de paga. Conocer a fondo su funcionamiento y su estructura.

3.3 Investigación de campo

Una investigación de campo (Arias, 2012) lo define como, "la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes" (p. 31).

Debido a que nuestra investigación se basa en el análisis de los resultados que obtendremos al atacar los enrutadores usando las herramientas ya antes seleccionadas, este tipo de investigación es fundamental para la obtención de datos sin alteraciones.

CAPÍTULO 4

DESARROLLO DEL TEMA

Como punto esencial en este capítulo empezaremos el análisis de vulnerabilidades, estudios anteriores como (Cuchillac, 2014) nos deja abierta la posibilidad de hacer ataques a protocolos WPA2, utilizando el sistema operativo Kali Linux, en donde nos indican las herramientas que se usaron para este ataque a las redes inalámbricas, a continuación, vemos

como el autor hizo uso de un sniff o detector de tramas inalámbricas tipo Wi-Fi, la cual se utilizó Kismet. En este caso se espera a que un cliente se conecte para mostrar el SSID que este utilizó para asociarse al AP oculto, otro caso es la de desasociar a un cliente ya conectado, para que haga el reenvió obligatorio de parámetros de conexión.

Según el estudio de (Díaz, 2016) nos dice que, otro método para atacar WPA2 PSK es el Key Cracking a través de un ataque de diccionario y para el caso de WPS se lo puede realizar con "Reaver" o ataque "Pixie Dust", aunque para que sea exitoso es necesario capturar primero el "handshake".

El intercambio de paquetes de datos entre AP y cliente en el instante que se realiza la autenticación mutua se lo denomina 4way-handshake, a pesar de que lo deseado sería un "handshake" completo para iniciar el ataque por diccionario, por otro lado, se lo puede realizar con un "handshake" a medias, es decir, cuando el cliente inicia la autenticación con un AP y este proceso ha fracasado. Tanto el "handshake" a medias o completo sirve para un ataque por diccionario (Díaz, 2016).

La vulnerabilidad del protocolo WPA2 fue descubierta en primera instancia en octubre del 2017 por Mathy Vahoef, y hoy los creadores de Hashcat (herramienta para el testeo de seguridad para crackear contraseñas) descubrieron una nueva vulnerabilidad, la cual ataca directamente al router, que de manera remota permite acceder al identificador de clave maestra de pares (PMKID). Esta nueva forma de ataque no necesita ningún cliente conectado y tampoco requiere full handshake. Esta funciona contra redes 802.11i / p / q / r con funciones de itinerancia habilitadas, que cubren la mayoría de los enrutadores modernos.

El descubrimiento de este nuevo ataque sucedió de forma accidental, ya que los desarrolladores de Hashcat buscaban posibles fallos del nuevo protocolo WPA3 que se dice que va a ser mucho más difícil atacar. Para esto se toma en cuenta tres herramientas las cuales son:

- hcxdumptool v4.2.0 o superior.
- hcxtools v4.2.0 o superior.
- hashcat v4.2.0 o superior.

Hcxdumptool

Una herramienta para la captura de paquetes en los dispositivos wlan, permitiendo ejecutar pruebas para establecer si los puntos de acceso o clientes son inseguros. Para comprobar si la aplicación o cliente son vulnerables en el uso de diccionarios, convierta el cap a hccapx o a WPA-PMKID-PBKDF2 hashline (16800) con hcxpcaptool (hcxtools) y se verifica si wlan-key o plainmasterkey pasó sin encriptar.

Esta herramienta la podemos descargar desde https://github.com/ZerBea/hcxdumptool.

Compilar

Para que se ejecute hacemos lo siguiente:

make

make install (siempre como super usuario)

Requerimientos:

- Sistema operativo: Arch Linux (estricto), Kernel> = 4.14 (estricto). También debería funcionar en otros sistemas Linux (notebooks, computadoras de escritorio) y distribuciones (no hay soporte para otras distribuciones). No utilice Kernel 4.4 (regresión de controlador rt2x00).
- libpthread y pthread-dev instalados.
- Raspberry Pi: adicionalmente libwiringpi y wiringpi dev instalados (soporte GPIO de Raspberry Pi).
- El conjunto de chips debe poder ejecutarse en modo monitor (estricto según: ip y iw). Recomendado: chipset RALINK (buena sensibilidad del receptor), controlador rt2x00 (estable y rápido).
- Raspberry Pi A, B, A +, B + (Recomendado: A + = muy bajo consumo de energía o B +), pero las computadoras portátiles y de escritorio también podrían funcionar.
- Se recomienda mod GPIO hardware.

Adaptadores soportados (obligatorio)

- ID 148f: 7601 Ralink Technology, Corp. Adaptador inalámbrico MT7601U.
- ID 148f: 3070 Ralink Technology, Corp. Adaptador inalámbrico RT2870 / RT3070.
- ID 148f: 5370 Ralink Technology, Corp. Adaptador inalámbrico RT5370.

- ID 0bda: 8187 Adaptador inalámbrico Realtek Semiconductor Corp. RTL8187.
- ID 0bda: 8189 Realtek Semiconductor Corp. RTL8187B Adaptador de red inalámbrico 802.11g 54Mbps.
- ID 148f: 2573 Ralink Technology, Corp. Adaptador inalámbrico RT2501 / RT2573.
- ID 0cf3: 9271 Qualcomm Atheros Communications AR9271 802.11n (TP-LINK TL-WN722N v1).
- ID 7392: a812 Edimax Technology Co., Ltd (Edimax AC600 USB / Fabricante: Realtek).

Advertencia

Se debe usar la herramienta hcxdumptool solo en redes que tengan permiso para realizar esto, debido a que:

- hcxdumptool puede evitar el tráfico completo de WLAN.
- hcxdumptool puede capturar PMKID desde puntos de acceso (solo se requiere un único PMKID desde un punto de acceso).
- hcxdumptool es capaz de capturar handshakes de clientes no conectados (solo se requiere un único M2 del cliente).
- hcxdumptool puede capturar handshakes de clientes de 5GHz a 2.4GHz (solo se requiere un único M2 del cliente).
- hcxdumptool es capaz de capturar EAPOL extendido (RADIUS, GSM-SIM, WPS).
- hcxdumptool es capaz de capturar contraseñas del tráfico WLAN.
- hcxdumptool es capaz de capturar plainmasterkeys del tráfico wlan.
- hcxdumptool es capaz de capturar nombres de usuario e identidades del tráfico wlan.
- No utilice una interfaz lógica y deje la interfaz física en modo administrado.
- No use hcxdumptool en combinación con aircrack-ng, reaver, bully u otras herramientas que tengan acceso a la interfaz.
- Detenga todos los servicios que tengan acceso a la interfaz física (NetworkManager, wpa_supplicant).
- No utilice herramientas como macchanger, ya que son inútiles, porque hcxdumptool utiliza su propio espacio de direcciones mac aleatorias.

Hcxtools

En primer lugar, definimos las siglas (h = hash, c = captura, conversión y cálculo de candidatos, x = diferentes hashtypes), esta permite convertir los paquetes de captura para que pueda ser utilizado con el ultimo hashcat. Esta herramienta es compatible en su totalidad con haschat y John the Ripper.

Fue diseñado para que se ejecute en Raspberry Pi con Arch Linux instalado, aunque también debería funcionar en otros sistemas Linux y distribuciones.

Es compatible con los modos de hash de hashcat: 2500, 2501, 4800, 5500, 12000, 16100, 16800, 16801.

Es compatible con los modos de hash de John the Ripper: WPAPSK-PMK, PBKDF2-HMAC-SHA1, chap, netntlm, tacacs-plus.

Para descargar esta herramienta lo podemos hacer mediante e siguiente enlace https://github.com/ZerBea/hcxdumptool.

Requerimientos

- Linux (se recomienda Arch Linux, pero otras distribuciones también deberían funcionar (no se admiten otras distribuciones).
- libopenssl y openssl-dev instalados.
- librt y librt-dev instalado (deberían instalarse por defecto).
- zlib y zlib-dev instalados (para archivos comprimidos / pcap / pcapng de gzip comprimidos).
- libcurl y curl-dev instalado (utilizado por whoismac y wlancap2wpasec).
- libpthread y pthread-dev instalados (utilizados por hcxhashcattool).
- Para instalar los requisitos en Kali use el siguiente 'apt-get install libcurl4-openssl-dev libssl-dev zlib1g-dev libpcap-dev'.

Hashcat

Es la herramienta que ayuda a la recuperación de contraseñas más rápida y avanzada del mundo, del cual admite cinco métodos de ataques únicos para más de 200 algoritmos de hash altamente optimizados. Actualmente admite CPU, GPU y otros aceleradores de hardware en

Linux, Windows y macOS, y cuenta con instalaciones para ayudar a habilitar el descifrado de contraseñas distribuidas.

Hashcat está bajo la licencia de MIT, para más información acerca de la licencia podemos ver aquí https://github.com/hashcat/hashcat/blob/master/docs/license.txt.

Instalación

Para descargar esta herramienta lo hacemos desde https://github.com/hashcat/hashcat, para luego descomprimirla y ubicarla donde se desee colocarla, se sugiere utilizar 7z x al desempaquetar el archivo desde la línea de comandos para asegurarse de que las rutas de archivo completas permanezcan intactas.

Otras herramientas

Se debe recalcar que las herramientas antes mencionadas no son las únicas ya que existen otras herramientas las cuales hemos probado para este tipo de ataques que son Wifite y WiFiBroot, que a continuación se detallan:

Wifite

Wifite es una herramienta de prueba de penetración inalámbrica automatizada que utiliza las herramientas asociadas con aircrak-ng y las herramientas de línea de comandos Reaver y Pixie WPS. Esto le permite a Wifite la capacidad de capturar tráfico y revertir las credenciales de autenticación para redes inalámbricas de tipo WEP, WPA y WPS.

Wifite se diseñó para emplear los métodos conocidos para recuperar la contraseña de puntos de acceso inalámbricos. Los cuales incluyen:

- **WPS:** Ataque sin conexión Pixie-Dust.
- **WPS:** Ataque de PIN por fuerza bruta en línea.
- **WPA:** Captura del Handshake + crack sin conexión.
- **WPA:** Captura del hash PMKID + crack sin conexión.
- **WEP:** Algunos ataques conocidos contra WEP, los cuales incluyen fragmentación, chop-chop, aireplay, etc.

Al ejecutar Wifite se selecciona los objetivos y la herramienta comenzara automáticamente a intentar capturar o descifrar la contraseña.

Sistemas Operativos Soportados

Está diseñado para trabajar con la última versión de Kali Linux, también es compatible con ParrotSec (es una distribución de GNU/ Linux basada en Debian Testing y diseñada teniendo en cuenta la seguridad el desarrollo y la privacidad).

Otras distribuciones de pentesting (como BackBox o Ubuntu) tienen versiones ya obsoletas de las herramientas que utiliza Wifite.

Herramientas requeridas

Se necesitará una tarjeta inalámbrica para el "Modo monitor" e inyección de paquetes.

A continuación, para que Wifite funciones se necesitará las últimas versiones de los siguientes programas que son compatibles con esta herramienta las cuales son:

- Python: Wifite es compatible con python2 y python3.
- Iwconfig: Para identificar dispositivos inalámbricos que ya están en modo monitor.
- Ifconfig: Para iniciar o detener dispositivos inalámbricos.
- Aircrack-ng suite, incluye:
    - Airmon-ng: Para enumerar y habilitar el modo monitor en dispositivos inalámbricos.
    - Aircrack-ng: Para descrifrar archivos .cap WEP y capturas de reconocimiento WPA.
    - Aireplay-ng: Para almacenar los puntos de acceso, la reproducción de archivos WEP.
    - Airodump-ng: Para escaneo de destino y generación de archivos de captura.
    - Packetforge-ng: Para forjar archivos de captura.

Esta herramienta la podemos conseguir desde https://github.com/derv82/wifite2.git.

Instalación

Para instalar desde el pc se abre un terminal y se ejecuta:

```
sudo Python setup.py install
```

Características

- PMKID captura de hash (activada de forma predeterminada, la fuerza con: --pmkid)
- WPS offline ataque de fuerza bruta también conocido como "Pixie-Dust". (activada de forma predeterminada, la fuerza con: --wps-only --pixie)
- WPS Online ataque de fuerza bruta también conocido como "ataque PIN". (activada de forma predeterminada, la fuerza con: --wps-only --no-pixie)
- WPA / 2 offline ataque de fuerza bruta a través de 4-Way Handshake captura (activada de forma predeterminada, la fuerza con: --no-wps)
- Valida handshakes contra pyrit, tshark, cowpatty, y aircrack-ng (cuando esté disponible)
- Varios ataques WEP (replay, chopchop, fragment, hirte, p0841, caffe-latte)
- Automáticamente encubre puntos de acceso ocultos mientras escanea o ataca.
    - Nota: Solo funciona cuando el canal es fijo. Utilizar-c <channel>
    - Deshabilita esto usando --no-deauths
- Soporte de 5Ghz para algunas tarjetas inalámbricas (a través de -5 switch).
    - Nota: algunas herramientas no funcionan bien en canales de 5 GHz (por ejemplo, aireplay-ng)
- Almacena contraseñas y handshakes crackeados en el directorio actual (--cracked)
    - Incluye información sobre el punto de acceso agrietado (Nombre, BSSID, Fecha, etc.).
- Fácil de tratar de romper apretones de manos o hash PMKID contra una lista de palabras (--crack)

WiFiBroot

A continuación, se va a utilizar WiFiBroot porque en comparación con las herramientas ya antes mencionadas esta resulta ser una de las más fáciles de aplicar debido a que, al momento de ejecutarla nos realiza todo el proceso de obtención de hash sin tener que estar escribiendo más líneas de código para la obtención de la misma, entonces podemos decir que es una herramienta WiFi-Penetest-Cracking para WPA / WPA2, la cual depende en sobremanera de scapy una biblioteca de manipulación de paquetes bien caracterizada en Python. Casi todos los procesos internos dependen de alguna manera de las capas de scapy y otras

funciones, excepto para operar la interfaz inalámbrica en un canal diferente. Eso se hará a través del comando nativo de linux iwconfig para el que quizás necesite los privilegios de súper usuario.

Actualmente proporciona cuatro Modos de trabajo independientes para tratar con las redes objetivo. Dos de ellos son métodos de craqueo en línea mientras que el otro se ejecuta en modo fuera de línea. El modo fuera de línea se proporciona para romper hashes guardados de los dos primeros modos. Uno es para el ataque de autenticación en la red inalámbrica y también se puede utilizar como un conductor de interferencias.

Instalación

Como se ha dicho, esta herramienta depende principalmente de scapy. Por lo tanto, es necesario tener instalado scapy, así que debemos asegurarnos de tener instalado una versión de scapy 2.4.0 o superior ya que en versiones anteriores pueden arrojar errores desconocidos.

Scapy ya viene instalado por defecto, pero si este no es nuestro caso se lo puede realizar aplicando el siguiente comando:

apt-get install scapy-python

Las dependencias que faltarían serán las librerías para el crack WPA, las cuales se instalan ejecutando el siguiente comando:

apt-get install Python-pbkdf2

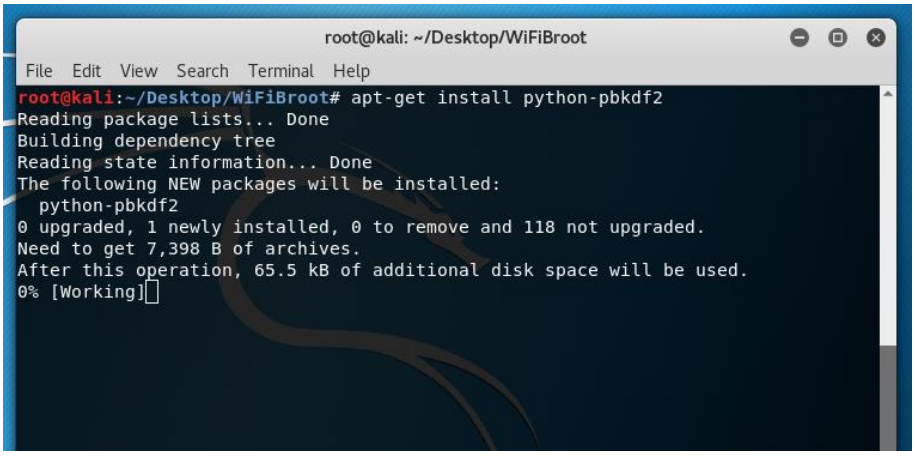

Figura 8. Instalación de librería pbkdf2

Una vez instalado scapy para ejecutar la herramienta se necesita descargar la herramienta desde https://github.com/hash3liZer/WiFiBroot.git, lo podemos hacer desde una terminal de Kali Linux:

git clone https://github.com/hash3liZer/WiFiBroot.git

Ejecución

A continuación, se tendrá que colocar la tarjeta inalámbrica en modo monitor. Puede usar un adaptador que admita la inyección de paquetes, así como el modo promiscuo, sin necesidad de un adaptador Alpha, solo se necesitara estar lo suficientemente cerca del objetivo:

Comando para poner nuestra tarjeta de red en modo monitor:

airmon-ng start wlan0

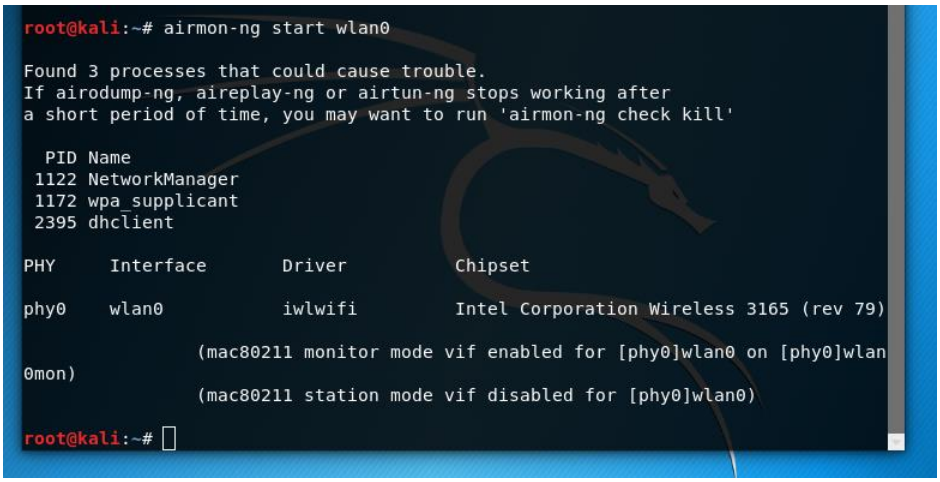

Figura 9. Tarjeta inalámbrica en modo monitor.

Debemos tener en cuenta que antes de ejecutar el comando para cambiar a modo monitor, se deberá conocer el nombre de nuestra tarjeta de red inalámbrica, en nuestro caso será wlan0.

WiFiBroot usa modos para identificar qué ataques se quiere realizar, hay tres modos disponibles el uso de cada modo se lo puede visualizar con la opción –help o -h justo después de la opción -m o -mode.

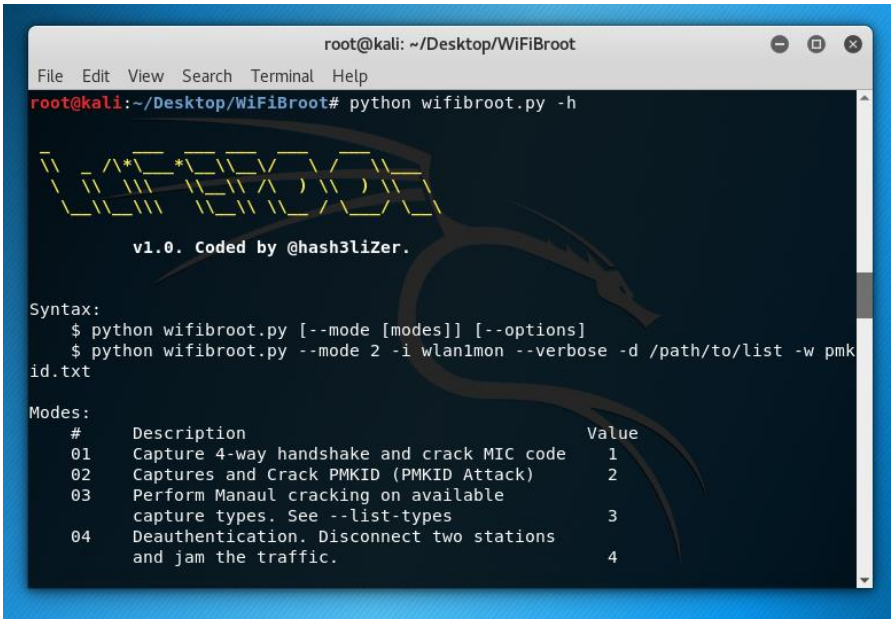

Figura 10. Visualización de ayuda.

Vamos a utilizar el modo 2.

python wifibroot.py –mode 2 -i wlan0mon –verbose -d dicts/list.txt

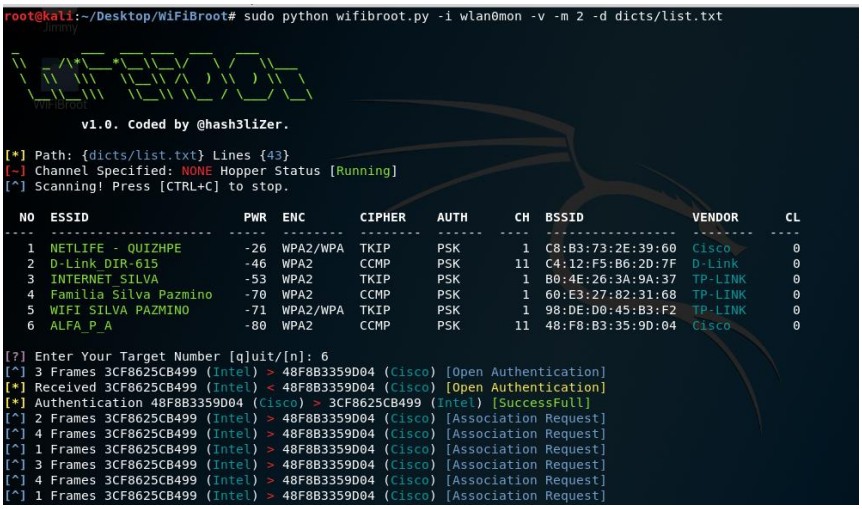

Figura 11. Ejecución de la herramienta WiFiBroot

- **-m, --modo:** Modo de uso. Valores posibles: 1, 2
- **-i, --interfaz:** Interfaz de monitor para usar.
- **-d, --diccionario:** Lista de palabras para craqueo.
- **-w, --write:** escribe la salida en un archivo.
- **-v, --verbose:** Imprime mensajes detallados.

Comenzará a escanear el área en busca de redes disponibles. Una vez seleccionado el objetivo en pantalla, se presiona **CTRL + C** para detener el escaneo y continuar con la ejecución. Inmediatamente se ingresa el número de destino que aparece en el lado izquierdo de la consola:

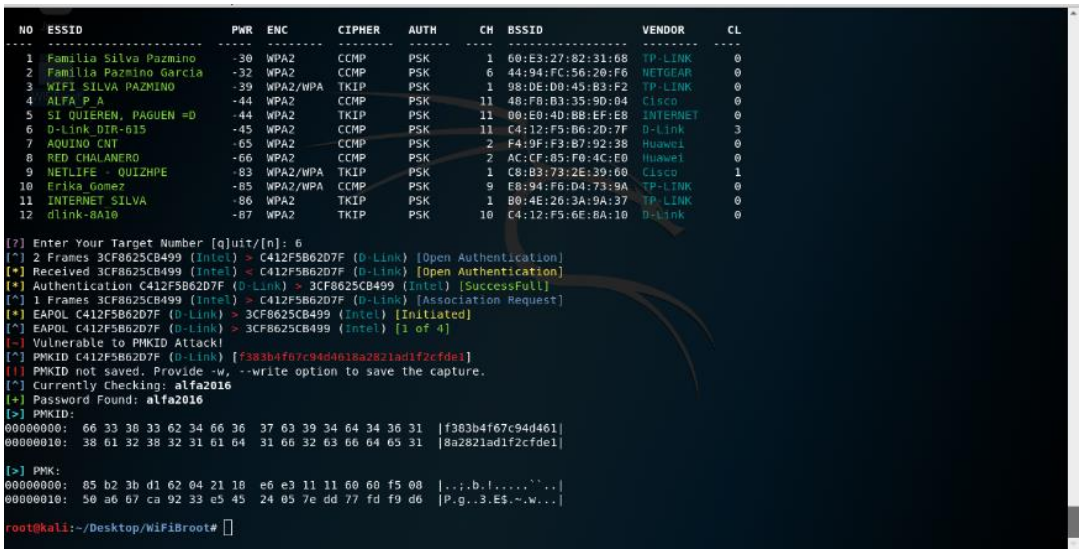

Figura 12. Selección red víctima.

Fuente: Propia.

Lo siguiente es esperar el EAPOL, solo se debe esperar para una autenticación exitosa con el punto de acceso (AP). Tan pronto como se emita un EAPOL a la STA, el script buscará el campo PMKID.

Si tenemos éxito nos mostrara el PMKID.

Una vez que se almacene en cache el PMKID, iniciará el proceso de craqueo e imprimirá la frase de la contraseña si esta se encuentra en el diccionario con los hashes usados, respectivamente PMKID y PMK, si se ejecuta en modo detallado:

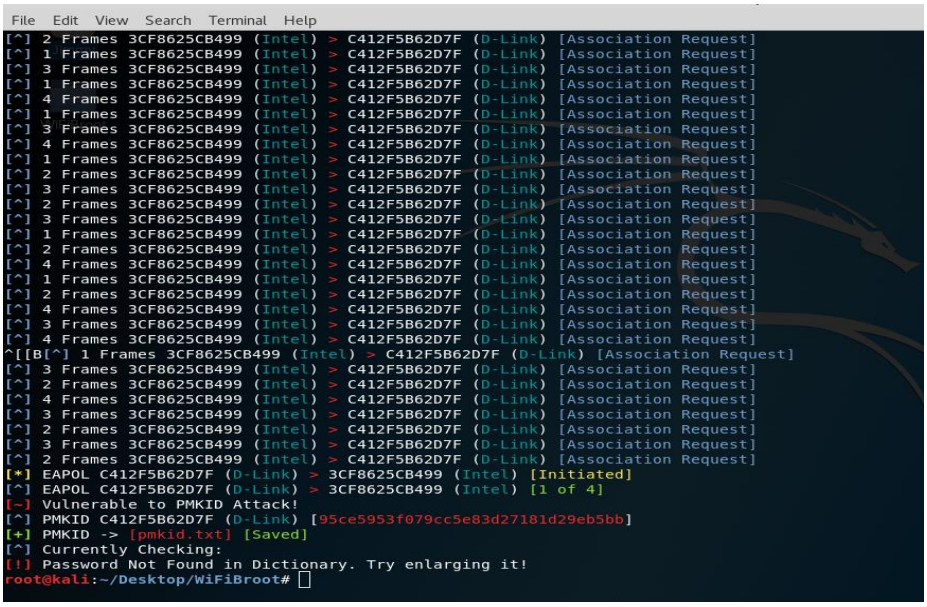

Figura 13. Resultado del ataque.

A continuación, se mostrarán los resultados del análisis que se realizaron a diferentes enrutadores en distintos puntos del cantón Naranjito.

Tabla 1. Routers analizados por sectores.

Sector	Fecha	Marca	Modelo	Vulnerable	Cifrado
Centro	06/11/2018	Cisco	Linksys E900	SI	CCMP
Centro	06/11/2018	D-Link	DIR-615	SI	CCMP
Centro	06/11/2018	NETGEAR		SI	CCMP
Cdla. San Elías	06/11/2018	Fiberhome		NO	CCMP
Cdla. San Enrique	07/11/2018	TP-Link	TL-WR740N	NO	TKIP
Cdla. San Enrique	07/11/2018	Qpcom		SI	CCMP
Cdla. Roldós	07/11/2018	Nexxt		SI	CCMP
Cdla. Roldós	07/11/2018	Huawei	EchoLife HG8245H	NO	TKIP
Cdla. Roldós	07/11/2018	Samsung		NO	CCMP
Centro	07/11/2018	Huawei		NO	TKIP
Centro	07/11/2018	TP-Link		NO	CCMP

Fuente: Elaboración propia.

Podemos ver el cuadro comparativo (Tabla 1) de los enrutadores que fueron analizados en diversos sectores del cantón Naranjito entre los cuales, obtuvimos diversos resultados, algunos no fueron vulnerables a este ataque como se lo refleja en la figura 14 por lo que se puede hace énfasis que a pesar del tipo de cifrado (TKIP) que este dispositivo (router) se encuentra configurado es inaccesible o no contiene este campo.

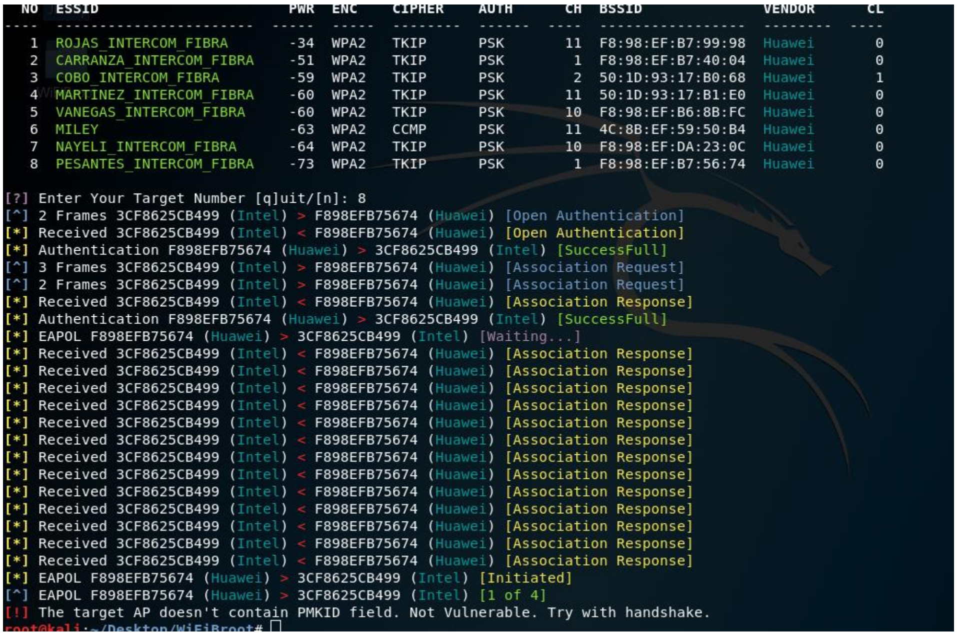

Figura 14. Equipo no vulnerable

Los equipos puestos a prueba a este ataque cuyos resultados fueron positivos (figura 15) entre los que encontramos marcas reconocidas en el medio como es el caso de CISCO, NETGEAR, se evidenció que son vulnerables a este método de obtención de PKMID, de modo que, si tenemos un buen diccionario, el craqueo de esta contraseña será cuestión de minutos, dejando así en evidencia que el protocolo WPA/WPA2 no es del todo seguro, en definitiva la única forma de proteger nuestra red local inalámbrica es colocando una contraseña que contenga letras mayúsculas y minúsculas, combinadas con números y símbolos con una longitud mínima de 12 caracteres.

Hay que mencionar, además que, en el caso de algunos puntos de accesos como Ubiquiti y Zte no se pudo conocer el resultado de vulnerabilidad, en vista que el tiempo de respuesta era demasiado alto en comparación con el resto de dispositivo analizados, esto debido a que

su proximidad no era relativamente cercana para su análisis u otros factores como pared, ventanas, vidrios, etc., que interrumpían la intensidad de itinerancia de los puntos de acceso.

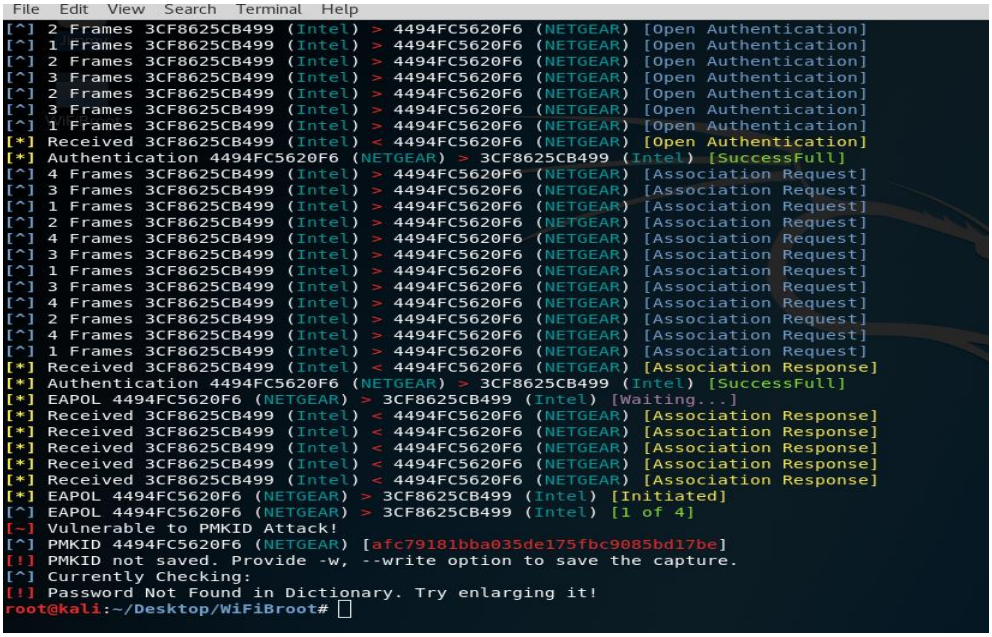

Figura 15. Obtención de PMKID

CAPÍTULO 5

CONCLUSIONES

En la búsqueda de herramientas que se necesitaron para efectuar las distintas pruebas en los routers, la herramienta WiFiBroot nos resultó una de las amigables a la hora de ejecutarla y manejarla, a diferencia de las demás herramientas enumeradas ya que su manejo resultó ser más complejo debido a una serie de pasos que se tienen que realizar hasta conseguir el objetivo.

Luego de analizar diferentes redes inalámbricas se concluye que, muchos de los routers analizados son vulnerables a este tipo de ataques que captura el PMKID, sea esto porque la mayoría de las víctimas utilizaban enrutadores modernos con itinerancia continua.

En otros casos, tales como aquellos routers que no pudieron ser vulnerados ante este ataque se debió a que no contenían este campo, sean estos porque en muchos de los casos el tipo de encriptado ya está en desuso (TKIP) y en otros el tipo de router eran de modelos antiguos, debemos recordar que esta técnica de craqueo de contraseña está orientada a enrutadores modernos que tienen roaming activado y usan una clave pre compartida PSK.

La cantidad de routers analizados que se refleja en nuestra investigación no es numerosa debido a que, en los sectores donde se realizaron las pruebas muchos de los dispositivos ya habían sido analizados anteriormente y el motivo de nuestra investigación es buscar vulnerabilidades en distintos equipos, teniendo en cuenta que el ataque se lo realizó en las calles de distintos sectores del cantón Naranjito donde sólo se pudo conocer la marca mas no el modelo, en algunos casos si se muestra el modelo dado que contábamos con el router en nuestras manos.

REFERENCIAS BIBLIOGRÁFICAS

Bibliografía

Amado, R. (2008). El Talón de Aquiles del estándar 802.11i: Proceso de autenticación PSK (y III) - Security Art Work. Retrieved October 31, 2018, from https://www.securityartwork.es/2008/02/12/el-talon-de-aquiles-del-estandar-80211i-proceso-de-autenticacion-psk-y-iii/

Arias, F. (2012). *EL PROYECTO DE INVESTIGACIÓN* (6ta ed.). Caracas: Editorial EPISTEME, C.A. Retrieved from https://www.researchgate.net/publication/301894369

Astaiza-Hoyos, E., Bermúdez-Orozco, H. F., & Méndez-Suárez, D. A. (2013). Evaluación del Desempeño de un Modelo Autosimilar para el Tráfico en Redes 802.11. *TecnoLógicas*, (31), 13–36. Retrieved from http://www.redalyc.org/articulo.oa?id=344234334002

Bernal, C. (2006). *Metodología de la investigación Para administración, economía, humanidades y ciencias sociales* (2da ed.). Mexico: Pearson Education.

Burrough, M. (2018). *Pentesting Azure Applications: The Definitive Guide to Testing and Securing Deployments*. No Starch Press. Retrieved from https://books.google.com.ec/books?id=orgrDwAAQBAJ

Cisco Systems Inc. (2006). *Fundamentos de redes inalámbricas*. Madrid: Pearson Education.

Colina, A., & Nuñez, S. (2007). ANÁLISIS DE ALGORITMO DE SEGURIDAD EN REDES WIMAX. *Revista Electrónica de Estudios Telemáticos*, *6*, 15–27. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=2964886

Costas, J. (2014). *Seguridad Informática*. *Editorial RA-MA*. Madrid: RA-MA.

Cuchillac, V. (2014). Metodología para la verificación de la seguridad en redes WI-FI residenciales y PYME. *Realidad y Reflexión*, (40), 80–105.

Díaz, A. (2016). *Análisis de vulnerabilidades de redes inalámbricas Wifi-Direct*. Universidad Carlos III de Madrid. Retrieved from https://e-archivo.uc3m.es/handle/10016/27145

García, C., & Reyes, J. (2015). *IEEE 802.11n como estándar óptimo para la transmisión de video en una red inalámbrica (tesis pregrado)*. Instituto Politécnico Nacional.

Retrieved from https://tesis.ipn.mx/bitstream/handle/123456789/21319/Proyecto IEEE802.11.pdf?sequence=1&isAllowed=y

Guerrero-Ibáñez, J., Flores-Cortés, C., Barba Marti, A., & Reyes, A. (n.d.). XXIII Congreso Nacional y IX Congreso Internacional de Informática y Computación 13, 14 y 15 de Octubre. *Análisis de desempeño de estándar 802.11p en situaciones de handoff dentro de un entorno de redes vehiculares* (pp. 148–154). Puerto Vallarta. Retrieved from https://www.researchgate.net/profile/Juan_Guerrero-Ibanez/publication/49242231_Analisis_de_desempeno_de_estandar_80211p_en_situaciones_de_handoff_dentro_de_un_entorno_de_redes_vehiculares/links/02bfe5115207793d99000000/Analisis-de-desempeno-de-estandar-80

Hashcat. (2018). New attack on WPA/WPA2 using PMKID. Retrieved November 1, 2018, from https://hashcat.net/forum/thread-7717.html

Hernández Sampieri, R., Fernández-Collado, C., & Baptista, P. (2006). *Metodología de la investigación* (4th ed.). Mexico. Retrieved from https://investigar1.files.wordpress.com/2010/05/1033525612-m

Hernandez, C., Rodríguez, L., & Aguilar, M. (2016). Análisis de seguridad en redes inalámbricas de las MiPyME y propuesta de mejora. *Revista Iberoamericana de Producción Académica y Gestión Educativa*, *4*(7). Retrieved from http://www.pag.org.mx/index.php/PAG/article/view/647

Johansen, G., Allen, L., Heriyanto, T., & Ali, S. (2016). *Kali Linux 2 -- Assuring Security by Penetration Testing*. Packt Publishing. Retrieved from https://books.google.com.ec/books?id=VoFcDgAAQBAJ

Horn, J. (2008). *Estudio Sobre Situación Actual De Iluminación De WLAN En Valdivia Y Análisis De Sistemas De Encriptación De Datos Utilizados En Wi-Fi (tesis pregrado)*. Universidad Austral de Chile. R

Leturia, I. (2018). WPA3 protokoloa, WiFiak behar zuen eguneraketa - Elhuyar Aldizkaria. Retrieved November 1, 2018, from https://aldizkaria.elhuyar.eus/mundu-digitala/wpa3-protokoloa-wifiak-behar-zuen-eguneraketa/

Lewis, W. (2009). *LAN inalámbrica y conmutada, Guía de estudio de CCNA Exploration*. Madrid: Pearson Education.

Luaces, J. (n.d.). *Seguridad en redes inalámbricas de área local (WLAN) (tesis pregrado)*. Universitat Oberta de Cataluña. Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

Machicao, S. (2015). *ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA Y SU INFLUENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE LAS COOPERATIVAS DE AHORRO Y CREDITO (CAC), REGION PUNO 2014-2015 (tesis pregrado)*. UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ." Retrieved from

http://repositorio.uancv.edu.pe/bitstream/handle/UANCV/469/45585175.pdf?sequence=1&isAllowed=y

Méndez, W., Mosquera, D., & Rivas, E. (2015). WEP, WPA and WPA2 encryption protocols vulnerability on wireless networks with Linux platform. *Tecnura*, 79–87. https://doi.org/10.14483/udistrital.jour.tecnura.2015.SE1.a06

Meneses, M., & Llanos, A. (2016). *Diseño de un protocolo para la detección de vulnerabilidades en los principales servidores de la superintendencia de puertos y transportes (tesis pregrado)*. Universidad Católica de Colombia. Retrieved from https://repository.ucatolica.edu.co/bitstream/10983/14013/4/Proyecto de Grado.pdf

Monsalve Pulido, J. A., Aponte Novoa, F. A., & Chaparro Becerra, F. (2015). Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia. *DYNA*, *82*(189), 226–232. https://doi.org/10.15446/dyna.v82n189.43259

Motyka, J. (2017). Descubre si tu WiFi está protegido frente al ataque Krack de WPA2. Retrieved November 1, 2018, from https://computerhoy.com/noticias/software/descubre-si-tu-wifi-esta-protegido-frente-ataque-krack-wpa2-69683

Namakforoosh, M. N. (2000). *Metodología de la investigación* (2a ed.). Limusa/Noriega Editores.

Peñaranda, R. (2010). *Interfaz de comunicaciones java para red inalámbrica*. Universidad Politécnica de Valencia. Retrieved from https://riunet.upv.es/bitstream/handle/10251/10165/PFC.pdf

Portantier, F. (2012). *Seguridad Informática*. Buenos Aires: FOX ANDINA.

Quiroz Zambrano, S. M., & Macías Valencia, D. G. (2017). Seguridad en Informática. *Dominio de Las Ciencias, ISSN-e 2477-8818, Vol. 3, Nº. Extra 3, 2017, Págs. 676-688*, *3*(3), 676–688. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Ríos, R. F. J. R. (2009). Análisis De Tráfico De Una Red Local Universitaria. *Revista Electrónica de Estudios Telemáticos*, *8*(2), 93–114. https://doi.org/ISBN:1856-4194

Romero, F. (2013). *Análisis Teórico y Experimental Sobre Seguridad en Redes Wi-Fi (tesis pregrado)*. Universidad De Málaga Escuela Técnica Superior De Ingeniería Informática. Retrieved from https://riu

Russell, R. (2000). *Hack Proofing Your Network*. Elsevier Science. Retrieved from https://books.google.com.ec/books?id=Fr9UOKzOjsAC

Tkal, E. (2009). *US12350649*. United State. Retrieved from https://patents.google.com/patent/US8281133B1/en

Vanhoef, M., & Piessens, F. (n.d.). *Denial-of-Service Attacks Against the 4-way Wi-Fi Handshake*. Retrieved from https://papers.mathyvanhoef.com/ncs2017.pdf

Vargas, Y. (2016). *ANALISIS DE LAS VULNERABILIDADES DE LAS REDES INALAMBRICAS DE LA UNIVERSIDAD PRIVADA LEONARDO DA VINCI (tesis pregrado)*. UNIVERSIDAD PRIVADA "LEONARDO DA VINCI." Retrieved from http://renati.sunedu.gob.pe/bitstream/sunedu/87744/1/VARGAS YEMPOL.pdf

Verbel, D., & Alvarez, H. (2016). *ESTUDIO DE ESQUEMAS DE SEGURIDAD EN REDES INALAMBRICAS: APLICACIÓN DE BUENAS PRACTICAS EN PYMES Y USUARIOS FINALES (tesis pregrado)*. Universidad de San Buenaventura Seccional Medellín. Retrieved from https://bibliotecadigital.usb.edu.co/bitstream/10819/3360/1/Estudio_Esquemas_Seguridad_Verbel_2016.pdf

Zha, X., & Ma, M. (2010). Security improvements of IEEE 802.11i 4-way handshake scheme. In *2010 IEEE International Conference on Communication Systems* (pp. 667–671). IEEE. https://doi.org/10.1109/ICCS.2010.5686489