UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

MAYO – SEPTIEMBRE

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS

TEMA:

DIAGNÓSTICO DE LAS DEBILIDADES DE LA ESTRUCTURA DE LA RED INALÁMBRICA DEL GAD DEL CANTÓN MONTALVO

EGRESADO:

JEFFERSON FRANCISCO JIMENEZ SANCHEZ

TUTORA:

ING. MARIA GONZALEZ

AÑO 2019

INTRODUCCIÓN

En el Ecuador se evidencia el masivo incremento de las redes inalámbricas o también conocida como redes Wireless Fidelity (Wi-Fi), debido que hoy en día estamos viviendo en un mundo interconectado y hace que las persona prefieran este tipo de red por su funcionalidad que es la de permitir la conectividad inalámbrica a los dispositivos electrónicos de manera fácil, rápida y su vez la compartir información entre ellos.

Por tal motivo se pretende por medio de este estudio proporcionar un contenido ecuánime que está centrado en el diagnóstico de las debilidades de la estructura de la red inalámbrica del Gobierno Autónomo Descentralizado (GAD) del Cantón Montalvo, aplicando teorías, metodología, métodos e instrumentos de investigación para la elaboración de la investigación.

Este estudio se centró en el análisis de la red inalámbrica del GAD del Cantón Montalvo con el objetivo de verificar el comportamiento de la red en el momento que exista algún incidente provocado por algún tipo de amenaza ya sea interna como externa, además conocer los diferentes tipos de vulnerabilidades que pueda presentar la red y conocer los efectos que puede causar a la estructura de la red antes mencionada por cualquier evento adverso.

Para las pruebas del estudio se usó herramienta MITM (Man in the middle), sus siglas traducida al español significa ataque de hombre en el medio, esta terminología se refiere al robo de datos a través de las redes inalámbricas, por lo tanto, a través de este ataque los usuarios son engañado mediante autentificación de la red falsa e inconscientemente el usuario le facilitara las credenciales, en esto se basa el manejo de la herramienta MITM.

Este caso de estudio se encuentra asociado con la sublínea de investigación de los procesos de transmisión de datos y telecomunicaciones, a través de un análisis a la red inalámbrica del GAD del Cantón Montalvo.

DESARROLLO

El presente estudio se lo realizó en el Gobierno Autónomo Descentralizado que se encuentra en el Cantón Montalvo a 35 km de la provincia Los Ríos, ubicado en la Avenida Antonia de las Bastidas Y 10 de agosto. Actualmente se encuentra bajo la administración del Msc Oscar Aguilar, tiene el compromiso de desempeñar a cabalidad su plan de trabajo propuesto en su mandato (2019-2023). El GAD es una entidad gubernamental que está dedicada a la administración de manera independiente al estado ecuatoriano, por medio de la administración pública atrevez de las distintas recaudaciones de impuesto de rodaje vehicular, permiso de construcción, pagos prediales rural. Está regido para todas las personas del mismo Cantón con el objetivo de satisfacer las inquietudes de las diferentes localidades de los recintos aledaño perteneciente al Cantón Montalvo.

Su infraestructura de red es inalámbrica puesto que para cubrir la municipalidad cuenta con 6 subredes ubicada en lugares estratégica para la cobertura del área.

Tabla 1. *Subredes del GAD*

SSID	ROUTER	PROCOLO DE SEGURIDAD	PROVEEDOR	VELOCIDAD	CANAL DE TRANSMISIÓN	BANDA
ALCALDIA	QPCOM WR154N	WPA2	CNT	1 MBps	3	2.4 GHz
TIC	TPLINK MR3420			3 MBps		
GAD_MUNICIPIO	DLINK DIR-600			1 MBps		
WifiPlanta2-4	DLINK DIR-615			1 MBps		
Talento Humano	TPLINK MR3420			1 MBps		
ZONA WIFI GADMCM	TPLINK WR841N	Ninguno(Abierta)		2 MBps		

Elaborado por Jefferson Jiménez

Las 5 subredes son destinadas para el personal que laborar en los diferentes departamentos, a diferencia de una la subred ZONA WIFI GADMCM que está destinada para todas las personas en general como son los trabajadores obreros, ciudadanos, etc. Cada departamento cuenta con computadores de escritorio con adaptadores wifi USB de marca TP-LINK modelo TL-WN822N para que los pc puedan conectarse a la red inalámbrica.

La red inalámbrica del GAD se la puede catalogar como insegura por no regular el alcance de la señal emitida por la red inalámbrica que sobrepasen el área de la edificación además se puede visualizar los SSID de las subredes que con que cuenta la municipalidad, por lo tanto, no se puede evitar intercepción de la información que es transmitida a través del aire y la señal podría ser detecta a larga distancia e introduciéndose en la red siendo un usuario no autorizado.

Existe desconocimiento por parte de los usuarios de la red inalámbrica del GAD de los nuevos métodos, técnica, herramientas de seguridad informática que hay hoy en día, por tal motivo se puede llegar a colocar en situación de riesgo la información, ya que las redes inalámbricas presentan una desventaja que los datos son transmitidos a través del aire dado que queda expuesta a terceras personas.

Se planteó realizar un diagnóstico de las debilidades de la estructura de la red inalámbrica del GAD de Cantón Montalvo ya que es de vital importante mantener los pilares de la seguridad informática como son la integridad, confidencialidad y la autenticidad, ya que por medio de las redes viaja información de suma importancia, de la misma manera es precisó mejorar la seguridad para evitar cualquier ataque. Los favorecidos será principalmente los usuarios de la red inalámbrica del GAD considerando que se proporcionará una conexión mucho más segura de esta manera estamos ayudando con la disminución de vulnerabilidades.

La metodología de investigación que se usó para la elaboración del estudio es la investigación Cualitativa para lo cual se utilizó dos de sus técnica como es la entrevista y la observación

para diagnosticar la situación actual de la problemática que inicialmente hemos indicado, las cuales se emplearon en el departamento de las Tics y la entrevista se la realizó al encargado del departamento y de la misma manera ser realizo la observación de los dispositivos que conforman la red inalámbrica con previas autorización de él, mediante las técnicas que se aplicaron se recopilo gran cantidad de información y así se pudo conocer los problemas actuales que presenta la red inalámbrica del GAD. Además de las técnicas también se usó instrumentos mediante la entrevista el instrumentó fue una guía de entrevista de tipo estructurado, así mismo mediante la observación el instrumento fue registros anecdóticos de tipo participante.

REDES INALÁMBRICAS

Las redes inalámbricas son de tipo no guiados, no necesitan cable para la trasferencia y compartición de información entre los dispositivos, lo realizan mediante ondas electromagnéticas a través del canal de comunicación que es el aire. (Salazar, 2016)

Las redes inalámbricas nos proporcionan la facilidad de poder conectar dispositivos electrónicos a unos o varios metros en algún caso hasta kilómetros de distancia. Este tipo de red no necesita ningún tipo de instalación, por lo tanto, no requiere de daño en adecuaciones para su uso. Esto hace muy popular a esta tecnología que en la actualidad se está expandiendo de manera muy rápida. (Salazar, 2016)

Las redes inalámbricas nos proporcionan tanto ventajas como ventajas.

Ventajas:

- Es más económica y fácil de instalar.
- La escalabilidad es mucho más fácil.
- Movilidad con los dispositivos electrónico dentro de un rango de cobertura de red.

Desventajas:

- Disminución de velocidad de transferencia.

- .facilidad de hackeo de seguridad. (Huidobro & Ordoñez, 2014) .

NORMAS DE RED INALÁMBRICA 802.11

La norma 802.11 en la actualidad es el estándar más usado para la creación de redes de área local inalámbrica o también llamado **Wi-Fi** (wireless-fidelity). Creada en 1999 esto dio paso para que dos compañías de desarrollo de teléfonos móviles como son Nokia y Symbol Technologies crearan una alianza de compatibilidad de internet de manera inalámbrica llamada WECA. En 2003 la agrupación paso a llamarse Wi-Fi Alliance, el principal objetivo la creación de una marca que permita la facilidad de conexión de manera inalámbrica y la impulsar compatibilidad entre los dispositivos. (Dordoigne, 2015)

802.11 a

La norma 802.11 a fue publicada en septiembre de 1999, utiliza la banda de 5 GHz y su velocidad máxima de transferencia en teoría es de hasta 54Mbps. Esta norma en la práctica puede alcanzar velocidad de transferencia de 48, 36, 24, 18, 12, 9 y 6 Mbps. (Dordoigne, 2015)

802.11 b

Esta norma es la sucesora de la 802.11 a, así mismo se creó año 1999. Esta norma trabaja en una banda distinta que es la de 2,4 GH u su velocidad de transferencia es de 11 Mbps. La norma 802.11 b no es compatible con la norma 802.11 a por que trabajan en bandas distintas. (Dordoigne, 2015)

802.11 g

La norma 802.11g fue publicado en el año 2003. Al igual que la norma 802.11 b también trabaja en la banda de 2.4 GH y su velocidad de trasferencia máxima es de 54 Mbps. Esta norma tuvo una mejora en la velocidad de transferencia. (Dordoigne, 2015)

802.11 n

La norma 802.11n a diferencia de los otros estándares, este estándar trabaja en las dos bandas

en la 2,4 GH y en la 5G. Por lo cual este estándar es compatible con a, b, g es decir con los estándares anteriores. Su velocidad de transferencia mínima es de 300 Mbps y como máxima es de 600Mbps .Este estándar fue publicado en el año 2009. (MIRANDA, 2019)

802.11 ac

La norma 802.11ac fue publicado en enero del 2012, su velocidad máxima que puede alcanzar hasta 1 Gbps. Este estándar trabaja por la banda de 5 GHz, todos los estándares anteriores que trabajan en la misma banda son compatibles. (TERNERO, y otros, 214)**.**

802.11 ad

La norma 802.11 ad fue publicado en el año 2014, su velocidad máxima que puede alcanzar hasta 6.7 GHz. Este estándar trabaja puede trabajar en tres bandas como son la de 2,4, 5, 60 GHz. La banda 60GHz obviamente tiene mayor velocidad de transferencia, pero su alcance es reducido a diferencia de las demás bandas. (TERNERO, y otros, 214)

Tabla 2. *Estándares 802.11*

802.11	Velocidad	Frecuencia	Año	Compatibilidad
A	54 Mbps	5 GHz	1999	No
B	11 Mbps	2,4 GHz	1999	No
G	54 Mbps	2,4 GHz	2003	802.11b
N	600 Mbps	2,4 GHz o 5 GHz	2009	802.11a/b/g
AC	1Gbps 1000 Mbps	2,4 GHz y 5 GHz	2012	802.11a/n
AD	7 Gbps 7000 Mbps	2,4 GHz , 5 GHz y 60 GHz	2014	802.11a/b/g/n/ac

Elaborado por Jefferson Jiménez

PROTOCOLOS DE SEGURIDAD INALÁMBRICA

WEP (Wired Equivalent Privacy)

Fue el primer cifrado creado en 1999 con el objetivo de darle seguridad a las redes

inalámbricas. Funciona de dos maneras como cifradas y algoritmo. En la actualidad este cifrado ya casi no es utilizado por que es débil, vulnerable por lo tanto no es recomendable su uso. Este tipo de cifrado usa el algoritmo RC4.

Este cifrado tenía dos formas de encriptación:

WEP 64: Permitía que la contraseña tenga como máximo 5 caracteres (40 bits).

WEP 128: Permitía que la contraseña tenga como máximo 13 caracteres (104 bits). (Santos, 2014)

WPA (Wi-Fi Protected Access)

Nació con la necesidad de cubrir las vulnerabilidades que presentaba el cifrado Wep, es decir todas las deficiencias que se prestaba con el otro cifrado se intentó cubrir con este nuevo cifrado. Se publicaron 2 versiones la WPA como sucesor de la WEP y WPA2 es la que actualmente está siendo más usada por las personas. Con la aparición de este cifrado trajo consigo el algoritmo TKIP en español Protocolo de integridad de clave temporal como una forma de garantizar la integridad del mensaje, por lo cual esté protocolo es mucho más robusto que el cifrado de encriptación WEP (RC4).este algoritmo de encriptación se lo puede usar en todos los dispositivo ya sea gama baja, media y alta. (ORUETA, ARMENDÁRIZ, RUIZ, & GIL, 2014).

WPA2 (Wi-Fi Protected Access2)

Esta es la versión dos de WPA, Este protocolo cuando lo lanzaron así mismo crearon un algoritmo propio para el WPA2 como es el AES, es mucho más sólido y complejo. Por lo cual casi los dispositivos de gama baja y media no lo soportan solo gama alta por lo que se requiere un hardware con mayores recursos para su implementación. La versiones de WPA pueden hacer uso de los algoritmos de encriptación de la otra versión porque son compatible. (Santos, 2014)

MÉTODOS DE CONEXIÓN A LAS REDES INALÁMBRICAS

● **Autenticación abierta:** como en su nombre lo indica, en este tipo de autentificación es abierta no posee contraseña, solo se necesita saber el SSID para poderse conecta a la red inalámbrica y navegar a través de ella. (Astudillo, 2017)

● **Clave compartida o PSK (Pre-Shared Key):** este tipo de autentificación es mediante clave establecida y compartida entre las dos partes, es decir para poderse conectar a la red inalámbrica tendría que ingresar la contraseña, por lo que solo los que conocen la contraseña podrán tener acceso a la red. Este esquema es apoyado por el WEP, WPA, y Protocolos de seguridad WPA2. (Astudillo, 2017)

ATAQUES INFORMÁTICOS

Son técnicas que se usa con el objetivo de desequilibrar y tomar el control tanto de redes como de sistemas informáticos ajenos.

Existen dos tipos de ataque:

Activo este tipo de ataque es detectables por lo que la información que viaja atreves de la red sufrirá algún tipo de alteración de los datos que son trasferidos, receptados y guardados. (BRIHUEGA, 2014)

Pasivo a diferencia del ataque activo, este no realiza ninguna modificación a la información que viaja atreves de la red, en conclusión, se puede decir que este ataque basa en el monitoreo del tráfico para sacar información relevante para el atacante. (BRIHUEGA, 2014)

Tabla 3. *Tipos de Ataques a Redes Inalámbricas*

Nombre del Ataque	Tipo de ataque	Descripción
Man-in-the-middle:	Activo	Este tipo de ataque consiste en posicionarse en medios dos equipos que se están comunicado con el objetivo que todo el tráfico que se genere pase atreves de él y así poder desencriptar la información. (Rodriguez, 2019)

MAC SPOOFING:	Activo	Este tipo de ataque consiste en la clonación de la dirección física de un equipo como es la MAC por otra de otro equipo para así obtener todos los privilegios del MAC clonada. (Johns, 2015)
ATAQUES POR FUERZA BRUTA	Pasivo	Es un método para descubrir la contraseña que consiste ir probando un sinnúmero de combinaciones que sean posible con la finalidad de encontrar la combinación correcta. Este ataque usan la técnica de prueba y error por lo este ataque demorara mucho tiempo, siempre este ataque lo combinan con el ataque de diccionario. (Incibe, 2017)
DENEGACIÓN DE SERVICIO (DOS)	Activo	Consiste en la saturación de peticiones al AP por lo cual la infraestructura inalámbrica colapsa e imposibilita recibir más peticiones por lo cual deniega el servicio a usuarios legítimos. (Vieites, 2014)
EAVESDROPPING	Pasivo	Este tipo de ataque consiste en interceptar el tráfico de una red no autorizado por medio de algún software mediante el uso de una antena wifi para tener mayor alcance. Si la información captura tiene encriptación busca patrones de comportamiento para la desencriptación. (Vieites, 2014)

Elaborado por Jefferson Jiménez

WIFISLAX: Es un sistema operativo basado en Linux, fue desarrollado específicamente para la realización de auditoria a las redes inalámbricas. Esta distribución cuenta con un sinnúmero además es Open Source es decir que no se necesita licencia para su uso. (Cruz, 2015)

Herramientas

Linset

Es una herramienta está enfocada a las auditoria de las redes inalámbricas. (Cruz, 2015)

Wifimosys

Es una herramienta que trabaja de manera similar a Linset. A diferencia de Linset esta herramienta está en constante actualización por motivo es la preferida por las personas. (Cruz, 2015)

Aircrack-ng

Es un conjunto de herramientas destinada a auditar la seguridad inalámbrica. Cada herramienta cumple una función en especifica como por ejemplo para activar el modo monitor, escaneo de redes, ataques de denegación de servicios, etc. (Cruz, 2015)

CommView for Wifi

Es una herramienta muy completa destinada para Windows, cabe señalar que esta herramienta permite realizar monitoreo, exploraciones y análisis de redes inalámbrica. (Cruz, 2015)

Uso de la herramienta CommView for Wifi

Se da clic en iniciar captura para realizar la búsqueda de las subredes y luego se selecciona la red inalámbrica ALCALDE.

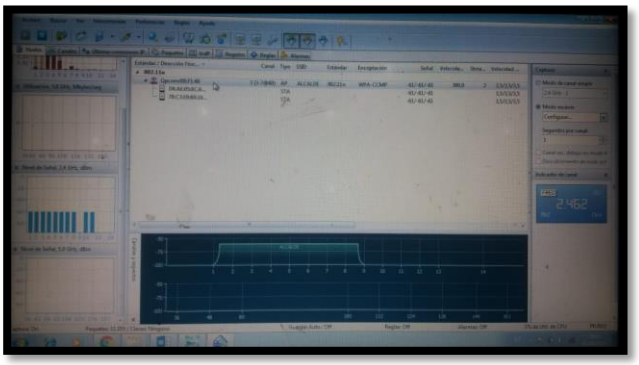


Ilustración 1.Seleccion de Red

Elaborado por Jefferson Jiménez

Se da clic derecho sobre la red inalámbrica y se elige la opción generar reporte. Como se visualiza en la ilustración 2.

Con la creación del reporte se tendrá una visión más detallada del estado, problemas, puertos y debilidades de la red inalámbrica, mediante grafico estadístico, tablas, etc. Como muestra en la ilustración 3 mediante un gráfico estadístico en forma de pastel mostrando en porcentaje del tráfico generado atreves de los puertos. Se debe agregar que los puertos que se encontrado abierto fueron 80(HTTP) ,110(POP3) ,21(FTP), 587(SMTP),23 (TELNET),53(DNS). Además, el reporte que se generó muestro mucha información relevante y permitió detectar otras vulnerabilidades que presentan en la red.

Uso de la herramienta LINSET

Linset ya viene instalado solo le damos clic y automáticamente detecta las tarjetas de redes inalámbricas conectada al computador, en mi caso me detecta la tarjeta nativa seleccionamos la opción 1.

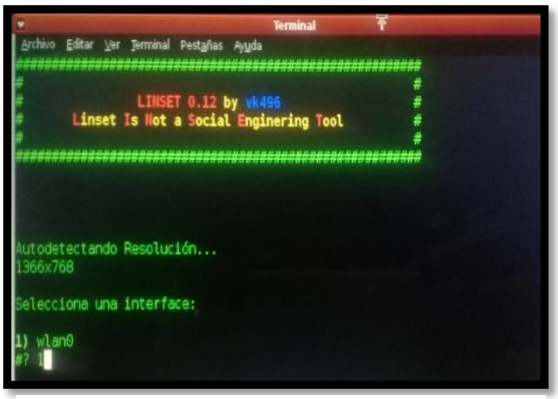


Ilustración 2.Seleccon de Interface

Elaborado por Jefferson Jiménez

Después aparecerá una nueva venta donde da la opción de seccionar los todos los canales o un canal en específico para realizar la búsqueda de las redes inalámbrica. Se selecciona la opción uno, como se puede observar en la ilustración 5.

Luego se seleccionarla la red que se desea atacar, en este caso escogemos la subred ALCALDE. Como se puede visualizar en la ilustración 6.

Posteriormente muestra una ventana donde nos da elegir el método que se va a utilizar para engañar al usuario mediante la creación de Fake AP. Se selecciona la opción recomendada que es la opción uno, como se puede ver en la ilustración 7.

De la misma manera nos da la opción de seleccionar la forma de desautentificacion de los clientes que están conectado a la red. Se selecciona la opción uno, como se puede visualizar en la ilustración 8.

Luego nos aparece una ventana con la red seleccionada en este caso ALCALDE con el objetivo de capturar el handshake. Como podemos visualizar la ilustración 9 el handshake ha sido capturado, así mismo elegimos la opción uno.

Además, tenemos que seleccionar el idioma para que las victima entienda el ataque por otra parte se elige la opción dos la cual es español. Como podemos ver en la ilustración 10

Luego nos aparece una ventana con 4 terminales donde se visualizan todos los usuarios que han realizado la conexión a red falsa. Como se muestra en la ilustración 11.

Como se puede visualizar hemos obtenido la contraseña de la Subred ALCALDE es decir algún cliente cayo en el ataque y automáticamente Linset desmonta el ataque y los a todos conecta la red.

Ilustración 3.Visualización de la contraseña por medio de la herramienta Linset

Elaborado por Jefferson Jiménez

Uso de la herramienta AIRCRACK-NG para vulnerar el filtrado MAC

Se activa el modo monitor con el comando airmon-ng para la búsqueda de las redes

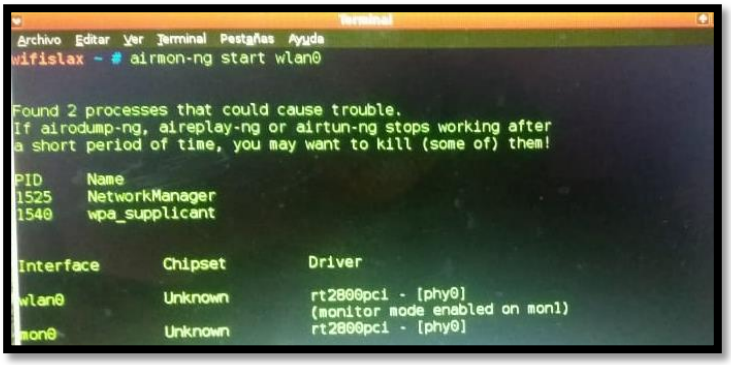


Ilustración 4.Activar Modo Monitor con Airmon-ng

Elaborado por Jefferson Jiménez

Seleccionamos la red con el comando airdump-ng para poder visualizar a los usuarios que están conectados a la red. Ver ilustración 14.

Luego nos aparecerá la red selecciona con todos sus clientes para nuestro caso será ALCALDE y nos aparecerá los clientes que están conectado a la red. Con el comando aireplay lanzamos el ataque de desautenticaficacion al usuario. Ver ilustración 15

Abrimos una nueva terminal para clonar la MAC de unos de los clientes en nuestro. La MAC del usuario que se colono es MAC D4: AE: 05: 8C: 64: A7. Ver ilustración 16

Nos parece una nueva terminal denegando el acceso al usuario de MAC D4: AE: 05:8C:64: A7. Ver ilustración 17.

Y nosotros nos procederemos a conectar y tendremos acceso a la red y podremos navegar.

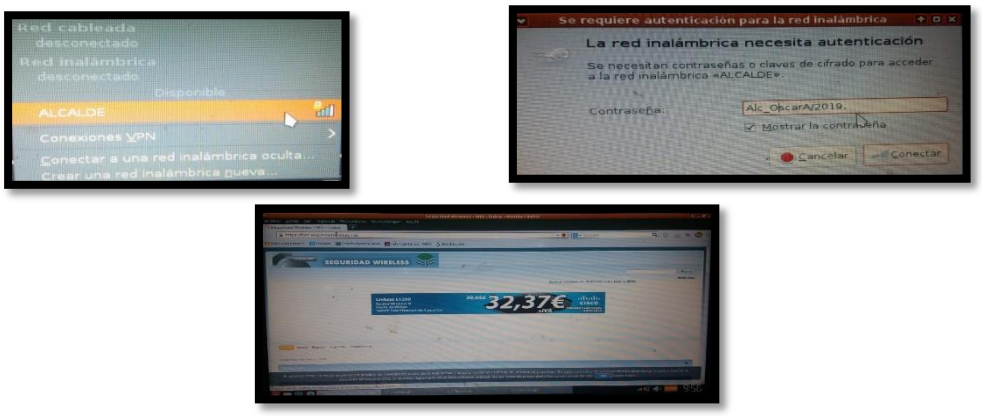


Ilustración 5.Conexión a la Red Inalámbrica ALCALDE

Elaborado por Jefferson Jiménez

Uso de la Herramienta Wifimosys

Descargamos el archivo Zip git hub de la siguiente dirección https://github.com/Vodker/wifimosys

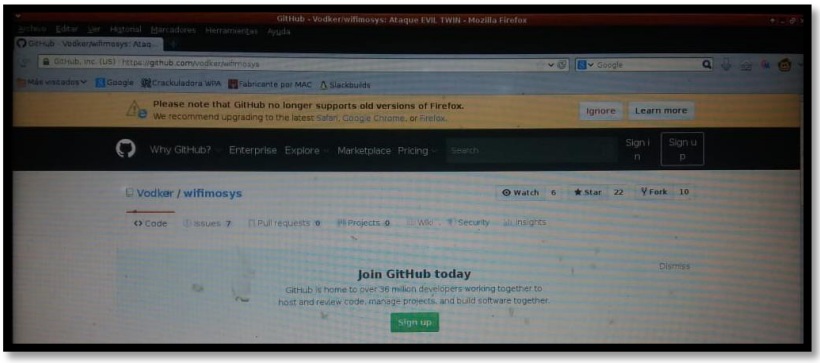


Ilustración 6.Descargar Wifimosys

Elaborado por Jefferson Jiménez

Extraemos el archivo Zip seleccionamos la carpeta y damos clic derecho para abrir una terminal

dentro de esa ruta. Y escribimos el siguiente comando para abrir Wifimosys. Ver ilustración 20

Luego nos aparece una ventana para elegir el canal para que haga una busque total elegimos la opción uno. Ver ilustración 21.

Elegimos la Red inalámbrica Alcalde para esta prueba y damos enter para que capture el handshake. Ver ilustración 23.

Lugo que nos captura nos muestra una ventana para realizar el de manera automática a diferencia de Linset. Seleccionamos la opción 1.

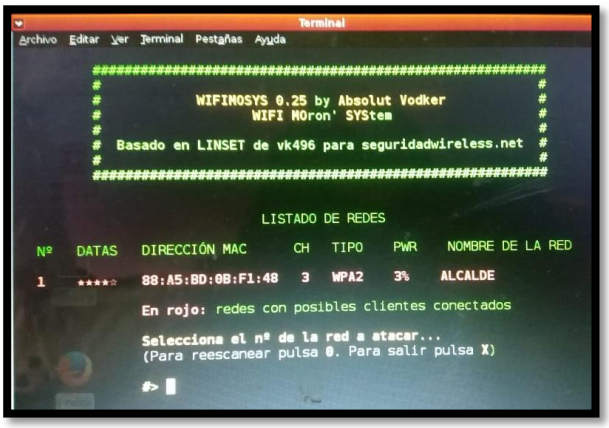
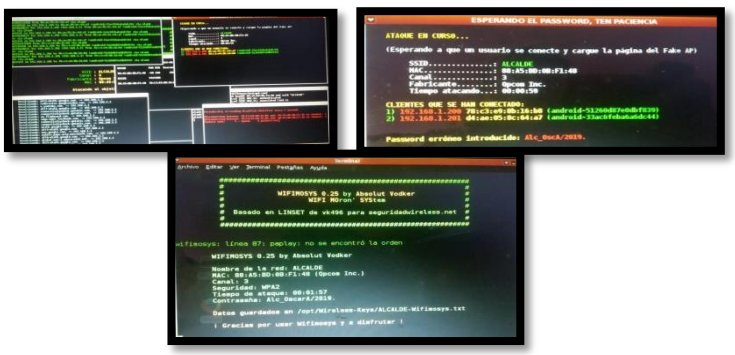


Ilustración 7.Lanzamiento de Ataque de Manera Automática

Elaborado por Jefferson Jiménez

Se lanza el ataque y nos muestra unas series de ventanas y cuando el usuario ingrese la contraseña y terminara el ataque de manera automática. Además, nos mostrara información adicional del ataque.



Elaborado por Jefferson Jiménez

Ilustración 8.Fases del Ataque y Obtención de la Contraseña de la Red

CONCLUSIONES

Se concluye que las redes inalámbricas del GAD son vulnerable dado que no cuentan un sistema de detección de Intruso o un firewall para la protección correcta de los datos, por cual la red puede ser atacada muchas veces mediante ataques de tipo pasivo, es muy difícil para el administrador de red detectar esos tipos ya que no se cuenta con los mecanismos de autodefensa para proteger la red inalámbrica. Además, el desconocimiento de los nuevos métodos de la seguridad informática por parte de los usuarios de la red hace que sea mucho más fácil la vulneración de la red ya que no toman las medidas de precaución para protegerse de estos ataques.

Con el uso de la herramienta CommView for Wfi se pudo realizar el diagnóstico de la red inalámbrica del GAD a diferencia de otras herramientas esta es mucho más completa, cabe señalar que esta aplicación nos permite generar reportes de tipo HTML y PDF para una mejor visualización mucho más completa del diagnóstico de la red. Gracias a esta herramienta se pudo constatar que las redes están a alrededor del GAD transmite por la misma banda de 2,4 GHz y también por el mismo canal que es el 3, a casusa de esto se puede afirmar existe una saturación de canal y esto hace la velocidad de transferencia baje porque hay mucha interferencia a través del canal.

Se debe agregar que adicionalmente también se detectó que existen 6 puertos abiertos como son el 80(HTTP), 110(POP3),21(FTP), 587(SMTP),23 (TELNET),53(DNS). Algunos de estos puertos abiertos pueden ser atacados mediante la herramienta Metasploit que ya instalado en Wfislax. Metasploit es herramientas de código abierto, la cual está formado por una bitácora scripts que se actualiza de manera semanal específicamente para detectar y atacar esas vulnerabilidades que presenta la red, además, acabe recalcar que está herramienta

es usada por los mejores hackers del mundo por tal motivo se recomienda que los puertos 21, 23,110 deben mantener los cerrados y si se requiere hacer uso esos puertos, se los habilite de manera manual, luego de finalizar su uso sean cerrado. Dado que de esta manera estaríamos previniendo los ataques dirigidos a los puertos y así protegeríamos la información sabiendo que es el activo más importe de una empresa.

Con ambas herramientas tanto como Linset y Wfimosys se logró obtener la contraseña de la red, pero como la red inalámbrica presentaba la seguridad de filtrado por MAC, para vulnerar esa seguridad se usó la herramienta Aircrack-ng para obtener acceso a la red denegando el acceso a aun usuario en específico que esté conectado a la red, clonado su dirección MAC y hacer uso de su privilegio como si fuera él.

Se pudo a través de esa investigación constatar que esta red inalámbrica usaba la mejor encriptación que existe actualmente y la mejor opción que nos ofrece el router que es el filtrado MAC y aun así se pudo vulnerar la red inalámbrica del GAD. Por tal motivo se recomienda hacer uso de un sistema de detección de Intruso o también conocido como IDS, pero de tipo NIDS (Network Intrusion Detection System) ya que este tipo está basado específicamente para la red realizando operaciones como control de acceso usuario, analizar el tráfico, puertos y un sin número de opciones que ofrece este tipo de sistema. Específicamente el programa Snort ya que encuentra posicionado como el programa número 1 para realizar esta tarea, adicionalmente es Open Source por ende no requiere una licencia para su funcionamiento.

Además, se debe agregar que para una protección mucho más completa se deber hacer uso de un firewall, actualmente existen muchos, pero hay uno que posicionado como el mejor en

estos últimos años como el firewall Palo Santo Networks, este tipo de firewall es de tipo hardware tiene algunos modelos para todas las necesidades que se requiera. Adicionalmente ofrece mucha seguridad tanto a las redes, como bases de datos y adicionalmente a las aplicaciones, por este motivo hace que esta aplicación se la considere robusta.

BIBLIOGRAFÍA

Astudillo, K. (2017). *Wireless Hacking 101.* BABELCUBE INC.

BRIHUEGA, D. A. (2014). *BACKTRACK 5. HACKING DE REDES INALÁMBRICAS.* España: RA-MA S.A.

Cruz, H. B. (2015). *HACKING & CRACKING.* Peru: MAcro.

Dordoigne, J. (2015). *Redes informáticas - Nociones fundamentales (5ª edición): (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6 ...).* ENI.

Huidobro, J. M., & Ordoñez, j. L. (2014). *Comunicaciones por Radio. Tecnologías, redes y servicios de radiocomunicaciones.* Madrid,: RA-MA.

Incibe. (27 de Febrero de 2017). *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

INCIBE. (14 de Mayo de 2019). *INCIBE.* Obtenido de https://www.incibe.es/protege-tu-empresa/blog/seguridad-redes-wifi-guia-aproximacion-el-empresario

Johns, A. (2015). *Mastering Wireless Penetration Testing for Highly Secured Environments.* Birmingham: Packt .

MIRANDA, C. V. (2019). *Comunicaciones industriales.* Madrid: Paraninfo.

ORUETA, G. D., ARMENDÁRIZ, I. A., RUIZ, E. S., & GIL, M. A. (2014). *Procesos y herramientas para la seguridad de redes.* Madrid: UNED.

Perez, P. G., Garces, G. S., & Camara, J. M. (2015). *Pentesting con Kali 2.0.* Madrid: 0xWORD.

Rodriguez, G. G. (2019). *Manual del Hacker Ético: Proyectos prácticos de seguridad informática.* Buenos Aires : Six.

Salazar, J. (2016). *TECHPedia.* Obtenido de https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

Santos, J. C. (2014). *Seguridad y Alta Disponibilidad* . España: RA-MA S.A.

TERNERO, M. D., CONCEJERO, J. B., MONDÈJAR, J. B., ROMERO, O. R., RODRIGUEZ, J. R., ANTON, G. S., & CASTILLO, F. S. (214). *REDES LOCALES* . Madrid: Paraninfo,SA.

Vieites, Á. G. (2014). *Seguridad en Equipos Informáticos* . Madrid: RA-MA S.A.

ANEXOS

Grafica 1.GAD del Cantón Montalvo

Elaborado por Jefferson Jiménez

Grafica 2. Realizando las Pruebas

Elaborado por Jefferson Jiménez

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

LUGAR A ENTREVISTAR: DEPARTAMENTO DE TIC DEL GAD DEL CANTÓN MONTALVO.

ENTREVISTADO: ING. RICHARD GUERRERO

Entrevista

1. **¿El GAD cuenta con redes inalámbricas?**

   Si

2. **¿Con cuentas Subredes cuenta el GAD?**

   Se cuenta con 6 subredes como son: Talento Humano, ALCALDE, TIC, GAD_MUNICIPIO, WifiPlanta2-4, ZONA WIFI GADMCM, las cuales cubren toda la edificación.

3. **¿Cómo considera el nivel de seguridad de la contraseña que usa en las redes inalámbricas?**

   Se la puede catalogar como alta ya que está compuesta de letras mayúscula, minúscula, caracteres especiales, símbolos y número.

4. **¿Qué tipo de cifrado usa en la configuración de la red inalámbrica? ¿Por Qué?**

   Se usa el cifrado WPA2 porque tiene un algoritmo de encriptación mucho más robusto actualmente es el que ofrece mayor seguridad.

5. **¿Qué método de seguridad usted usa para proteger las redes inalámbricas?**

   Se usa dos métodos que ofrece el router mediante contraseña y además la de filtrado por MAC.

6. **¿Han existido ataques a la red inalámbrica?**

   Si ha existido, pero han sido más ataque de tipo pasivo que activo, ya que estos tipos de ataque actúan en segundo plano y casi no son no son detectado

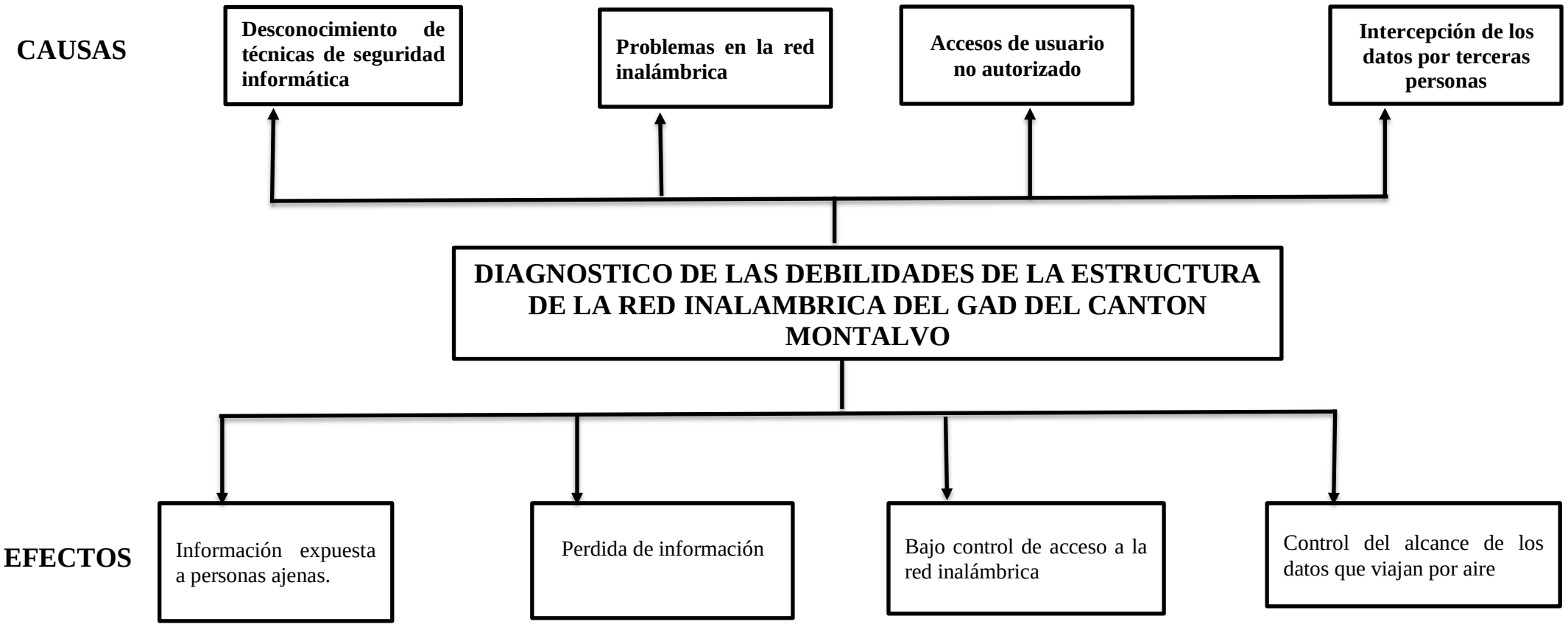
7. **¿Considera usted cual sería la debilidad de la red inalámbrica?**

   Sería la seguridad ya que el GAD no cuenta un Firewall (hardware o software) es decir no se cuenta con un sistema de autodefensa ya que podemos ser atacado cada vez y cuando.

8. **¿Considera usted cual es el motivo porque los usuarios del GAD caen en estos tipos de ataque?**

   El principal motivo es el desconocimiento de los nuevos método y técnica de la seguridad informática actualmente.

ÁRBOL DE PROBLEMAS



ANÁLISIS FODA

FORTALEZA	OPORTUNIDADES
• Se cuenta con el personal suficiente para realizar las actividades diarias. • Se cuenta un Departamento de Sistema para la administración de la información del GAD. • Buen Ambiente de Trabajo.	• Surgimiento de los nuevos mecanismos para aprovechar mejor los recursos. • Implementación de nuevas tecnologías y procesos para aumentar la eficiencia. •Aplicación Normas Internacionales WLAN a la red inalámbrica del GAD.
DEBILIDADES	**AMENAZAS**
•Cuentan con un presupuesto limitado para realizar mejora en la infraestructura . •No cuentan con un Sistema de Detección de Intruso (IDS). •Desconocimiento de los usuarios sobre las diferentes técnicas, herramienta y métodos que existen para vulnerar las redes inalámbricas.	•Falta de recurso para renovar la infraestructura tecnológica. •Aparición de nuevas herramientas y método de ataque a las redes inalámbricas • Contar con políticas definidas para los usuarios de la red y no aplicarlas adecuadamente.

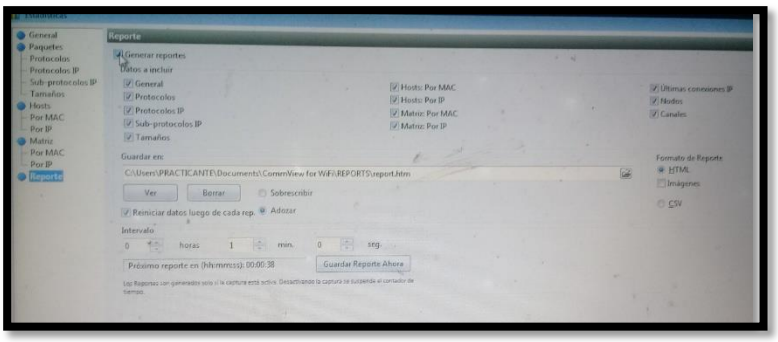


Ilustración 9.Generación de Reporte`

Elaborado por Jefferson Jiménez

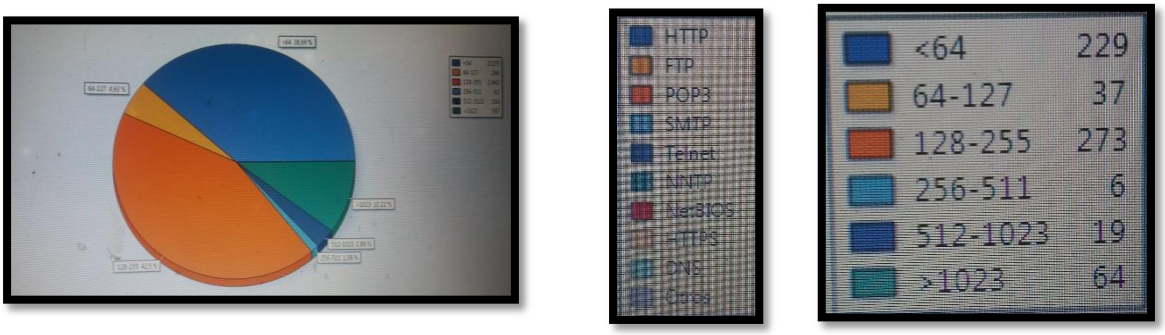


Ilustración 10.Grafica de Trafico de Puertos

Elaborado por Jefferson Jiménez

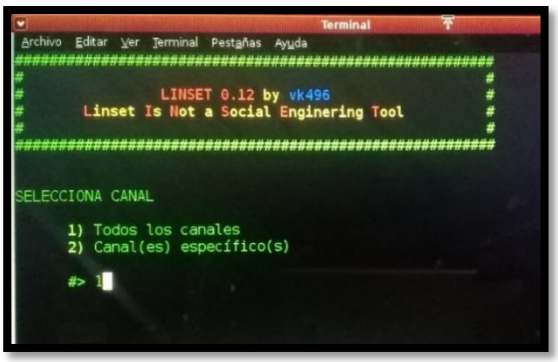


Ilustración 11.Seleccion del Canal

Elaborado por Jefferson Jiménez

Ilustración 12.Selección de Red

Elaborado por Jefferson Jiménez

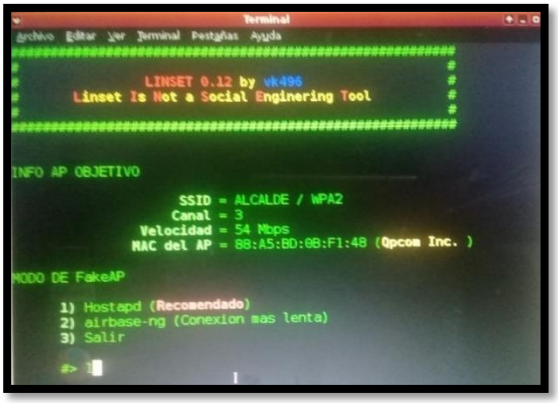


Ilustración 13.Seleccionar Método de Ataque

Elaborado por Jefferson Jiménez

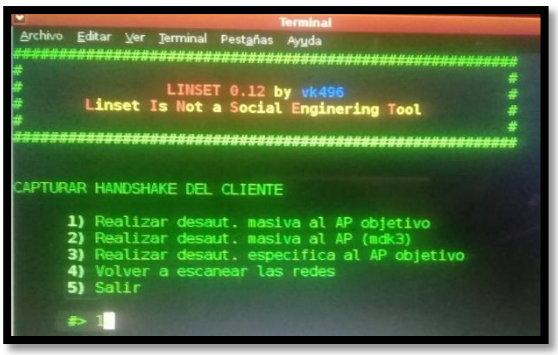


Ilustración 14.Seleccion de Método de Desautentificacion de Clientes

Elaborado por Jefferson Jiménez

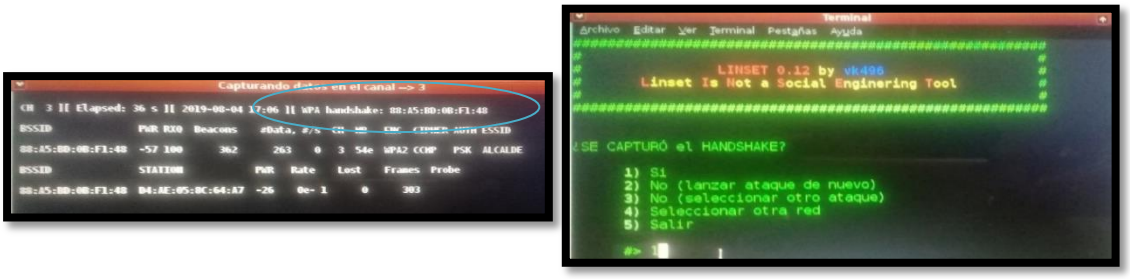


Ilustración 15. Captura de Handshake

Elaborado por Jefferson Jiménez

Ilustración 16.Seleccion del Idioma

Elaborado por Jefferson Jiménez

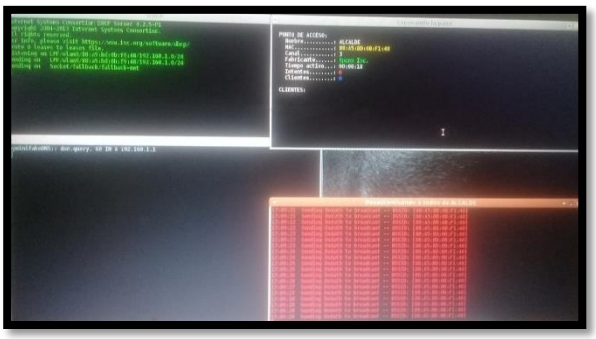


Ilustración 17.Ventanas que Muestran el Acceso de las Personas a la Red Falsa

Elaborado por Jefferson Jiménez

Ilustración 18.Seleccion de Red con Airdump-ng

Elaborado por Jefferson Jiménez

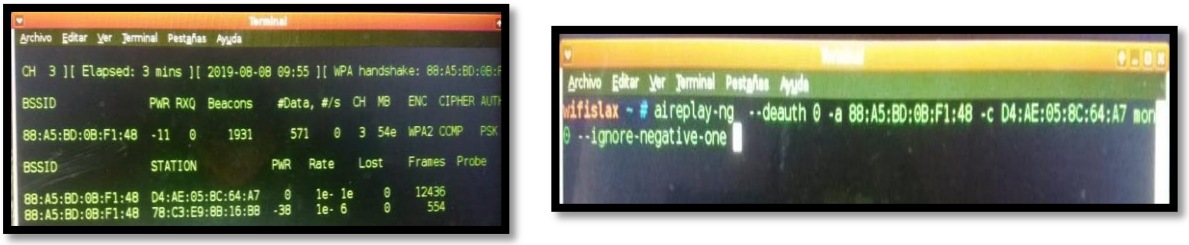


Ilustración 19.Desautentificacion de Usuario con Aireplay-ng

Elaborado por Jefferson Jiménez

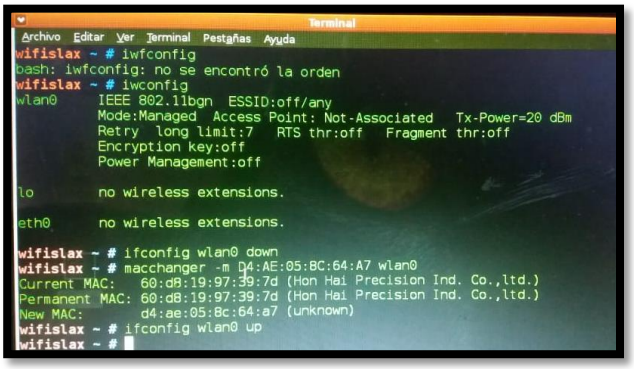


Ilustración 20.Clonación de dirección MAC de Usuario de la Red

Elaborado por Jefferson Jiménez

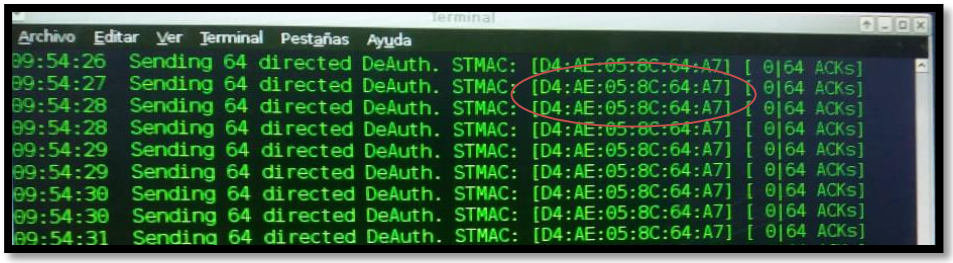


Ilustración 21.Ventana Denegando el Servicio a Usuario de la Red

Elaborado por Jefferson Jiménez

Ilustración 22.Ejecucion de Comando para Abrir Wifimosys

Elaborado por Jefferson Jiménez

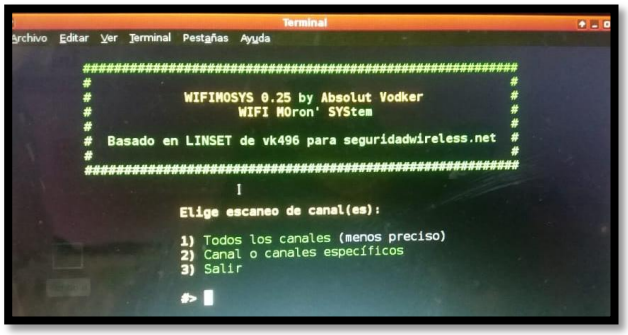


Ilustración 23.Seleccion de Canales

Elaborado por Jefferson Jiménez

Ilustración 24.Seleccion de Red

Elaborado por Jefferson Jiménez