Informe de Proyecto Redes de Computadores “ ELO 322 ” “Seguridad en Redes inalámbricas”

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Oscar Guajardo 201530016-K
Marcelo Villablanca 201530009-7

Resumen

En el presente proyecto que complementa la presentación, se volverá a explicar funciones de las redes inalámbricas, junto con detalles de sus protocolos de uso, dividiendo nuevamente las redes inalámbricas en sus categorías de áreas de extensión. Esta división es conformada por WPAN, WMAN y WWAN, las cuales son

indispensables para la vida que llevamos hoy en día y sin notarlo, de uso diario. Los protocolos de las redes son aquellos conjuntos de reglas que rigen a cada red, por lo tanto, debemos fijar que tipo de red vamos a hablar en cada tipo área de servicio, la cual será Bluetooth para WPAN, WI FI para WMAN y 4G para WWAN.

Introducción

Para comenzar este informe, daremos una mirada con mayor profundidad sobre las redes inalámbricas, así agregando más detalles con respecto a las funcionalidades de cada tecnología de redes inalámbricas, que las hace funcionar y porque es que su seguridad es tan importante dentro de la vida cotidiana, puesto que en sí es mucho más accesible atacar una red de este estilo. Pero a la vez son mucho más populares por sus baratos costos y fácil instalación, ¿Cómo proteger mejor tu red inalámbrica?, ¿es imprescindible adoptar costumbres para mejorar tu seguridad de red?.

Bluetooth

La tecnología Bluetooth se concibió en 1994 por Ericcson Mobile Comunication y se rige por el protocolo IEEE 802.15.1 , el cual posee medio físico y Control de medios de acceso (MAC), su uso se hace cada vez más masivo en conexiones de objetos en modalidad peer to peer (P2P), un ejemplo son los mandos de consolas de última generación. Opera en la banda libre ISM de 2.4 GHZ , para evitar la interferencias y pérdidas de información el transceptor realiza una transmisión-recepción de saltos de frecuencia (hops) y para minimizar su complejidad utiliza también modulación

binaria FM. Para realizar una transmisión FULL DUPLEX utiliza TDD, para controlar el canal. En cuanto a su seguridad, se le realizan ciertos cambios al paquete en el proceso de entramado, se le agrega al encabezado un HEC, los bits del encabezado son mezclados con una palabra de whitening, y se le aplica códigos FEC, que al ser recepcionados el receptor realizar el proceso inverso (FIGURA 1 del anexo).

Existen 3 modos primarios de seguridad.

- modo 1 : Sin seguridad, todos los mecanismos de seguridad están deshabilitados
- modo 2 : En la capa L2CAP, nivel de servicios. Los procedimientos de seguridad son inicializados luego de establecer un canal, entre el nivel LM y el de L2CAP. Un gestor de seguridad controla el acceso a servicios y dispositivos. Variando las políticas de seguridad y los niveles de confianza se pueden gestionar los accesos de aplicaciones con diferentes requerimientos de seguridad que operen en paralelo. Su interfaz es muy simple y no hay ninguna codificación adicional de PIN o claves.
- modo 3 : En el nivel de LINK. Todas las rutinas están dentro del chip Bluetooth y nada es transmitido en plano. Los procedimientos de seguridad son iniciados antes de establecer un canal.aparte del cifrado tiene autenticación PIN y seguridad MAC. Su metodología consiste en compartir una clave de enlace secreta entre dos dispositivos, esta se genera al inicializar el proceso de pairing (primera conexión entre dispositivos).

WI FI

La tecnología WI FI (wireless - fidelity) conforma una de las innovaciones líderes en comunicación a nivel mundial y cada vez más dispositivos poseen soporte para WI FI . es bueno acotar que este tipo de red inalámbrica esta al borde entre WPAN y WMAN, las cuales se diferencian por el alcance, sin embargo al ser tan popular, algunas grandes instituciones optan por instalar en sus edificios una red a

base de grandes cantidades de routers encadenados, lo que cumple el concepto de WMAN que es una red de gran tamaño (metropolitano). Esta tecnología se rige bajo el protocolo IEEE 802.11 x (sea x letras a, b , g, n, ac) que se diferencian por las diferentes tasas de transmisión en cada banda, la mas popular 2.4 GHZ. En cuanto a sus métodos de seguridad, existen 3 casos también, los cuales son:

- WEP : Suele ser la opción por defecto que suministra el fabricante para preconfigurar los routers, es compatible con todos los dispositivos y estándares de wi fi. Utiliza una clave única compartida (PSK) de seguridad para cifrar todas las conversaciones entre dispositivos, que tienen que conocerla. Baraja paquetes entre los AP (access points) y los clientes para cifrar transmisiones unicast y multicast, pero resulta sencillo interceptar paquetes y romper a través de métodos de fuerza bruta para obtener la clave de seguridad, WEP es muy básica.
- WPA : o WI FI PROTECTED ACCESS distribuye dinámicamente claves y utiliza de forma más robusta el algoritmo de vector de inicialización, cuenta con nuevas tecnologías para la integridad y autenticación como IEEE 802.1x que proporciona un control de acceso en redes mediante puertos (el punto de acceso mantendrá el canal bloqueado hasta que el usuario se autentifique), EAP, protocolo de autenticación extensible, realiza tareas de autenticación, autorización y contabilidad , TKIP (temporary key integration protocol), se encarga de generar claves para cada trama enviada y MIC (message integrity code) que verifica la integridad de los códigos en la trama, éste último reemplaza el CRC-32 usado en WEP.
- WPA2: este protocolo es el último usado en seguridad, denominado IEEE 802.11i incluye nuevas tecnologías que mejoran la seguridad del servicio de conexión, como por el nuevo algoritmo de cifrado AES (advanced encryption standard) que es un algoritmo de cifrado de bloque, a diferencia de los otros dos anteriores que usaban RC4, un algoritmo de cifrado de flujo, AES proporciona claves de 128 Bits. Para asegurar la integridad y autenticidad de los mensajes WPA2 ocupa CCMP (counter mode / cipher block channel / message authentication code protocol) en lugar MIC.

(FIGURA 2 DEL ANEXO).

4G LTE

La red 4G LTE es lo último en innovación comercializada con lo que respecta a redes y conectividad, es generalmente nueva y posee grandes capacidades de transmisión con una banda de 300 Mbps de bajada punta y 75 Mbps de subida punta. La idea está mayormente desarrollada en el protocolo IP (capa de tercer nivel), incluyendo soporte para IPV6. Arquitectura de 4G LTE anexada en FIGURA 3 . La seguridad de esta tecnología está basada en 3GPP, mejorando aquellos aspectos donde esta misma flaqueaba, su seguridad se divide en 5 puntos, estos son:

- Seguridad de acceso a la red: Provee al usuario un acceso seguro al servicio.
- Dominio de seguridad de la red: Para proteger los elementos de la red y asegurar la recepción de señal y el intercambio de usuarios.
- Seguridad del dominio del usuario: Controla el acceso seguro a estaciones móviles
- Seguridad del dominio de la aplicación: Establece una comunicación segura a través de la capa aplicación
- Visibilidad y seguridad de la configuración: Ofrece al usuario la oportunidad de revisar si sus sistemas de seguridad están en completa funcionalidad.

FIGURA 4 DEL ANEXO.

utiliza 3 métodos de seguridad los cuales son celular security que implica el proceso de autenticación entre la unidad móvil y el EPC, Handover security que permite el paso de un UE de una celda a otra y M2M que ejecuta revisiones de seguridad cuando las transmisiones de datos ocurren entre máquinas, Sin embargo al recordar que esta nueva tecnología se desarrolla en la capa de tercer nivel, es bueno acotar que posee métodos de seguridad al nivel de esta capa también, como Túneles IP, cortafuegos integrado. En cuanto a túneles, una pasarela SeGW debe soportar diferentes tipos de encapsulamiento y autenticación de túneles. Y para la seguridad

la pasarela debe proporcionar el cifrado correspondiente para tanto las nuevas conexiones de celdas de tamaño reducido como los puntos de acceso WI FI y también conexiones VPN. Los túneles proporcionan una conexión segura entre redes del operador móvil y redes nubes.

La pasarela también debe proporcionar un cortafuegos para proteger la red de ataques de denegación de servicios (DoS). Como los operadores móviles desplegarán diferentes arquitecturas de seguridad de la red móvil para proteger su red 4G/LTE, la pasarela SeGW debería ser flexible y soportar diferentes tipos de tráfico, ya sea en los mismos túneles IPSec o en unos diferentes, conjuntamente con una o varias asociaciones de seguridad IKEv2.

Una pasarela SeGW avanzada soporta todos las capacidades de seguridad necesarias de una red móvil, tales como la carga útil de configuración IKEv2, las autenticaciones de certificado multinivel, el servidor de AAA, y la gestión de recursos de IP y DHCP para soportar procedimientos IPSec de conectar y operar.

Parte Experimental

AIRCRACKING

Lo primero que haremos será ver las tarjetas de red inalámbricas que tenemos disponibles, y elegir la que utilizaremos, al ser posible se utilizará una que permita la inyección de paquetes, recomendable el chipset RTL8187L de ALFA INC.

Tecleamos en la terminal: iwconfig (imagen 1)

Vemos las interfaces inalámbricas disponibles, recordaremos el nombre de la interfaz que utilizaremos. Ahora vamos a ponerla en modo monitor, para poder

interceptar todos los paquetes, de manera opcional podemos cambiar la dirección MAC de nuestra tarjeta para más seguridad a la hora de auditar.

El modo monitor lo activaremos con airmong-ng de la siguiente manera, y siendo superusuario:

airmon-ng start [interfaz], en este caso wlan1 (imagen 2)

la interface wlan1 a pasado a modo monitor en la interfaz mon0.

Ya podemos capturar paquetes, ahora escaneamos a todas las redes al alcance,necesitaremos el canal, el BSSID (MAC del AP) del objetivo y opcionalmente el ESSID (Nombre del AP).

Para escanear las redes utilizaremos airodump-ng.

airodump-ng [interfaz-modo-monitor], en este caso sería mon0 (imagen 3)

En el momento de lanzar el comando, nos empezará a mostrar las redes al alcance.

Después de fijar el objetivo, sabemos su ESSID, su BSSID, su canal de emisión y además observamos que es una red en la cual existe un cliente conectado a ella puesto que existe tráfico.

Ya es momento de ir recolectando IVs en un archivo .PCAP para posteriormente crackearlo. (IVs , archivos de vector inicialización)

Para capturar utilizaremos airodump-ng con las siguiente opciones.

airodump-ng -c [canal] -b [BSSID] -w [archivo de captura] [interfaz], en este caso sería airodump-ng -c 1 -b D8:61:94:64:7D:47 -w capturahackpuntes.pcap mon0

Observamos cómo se crea un archivo, donde irá guardando los IVs. (imagen 4)

Para crackear la clave, es necesario capturar miles de IVs.

Conclusión

Para finalizar este informe, podemos concluir que a medida que se renuevan las versiones de cada tecnología o se crean nuevas, las seguridades que se implementan son de mayor desarrollo y más complejas, mejorando la calidad del servicio y confiabilidad siendo una gran ventaja, sin embargo, requieren mayor uso de hardware e incluso algunos algoritmos de seguridad son incompatibles con ciertos dispositivos, ya que requieren muchos recursos (memoria física), para ser ejecutados. Esto representa una desventaja, sin agregar que aún con nuevas tecnologías existen nuevas debilidades que explotar para los hackers, por lo tanto en un balance, quedándonos sólo con lo positivo, en un mejor futuro donde se siga el desarrollo de las redes inalámbricas sin la perversión de los malos usuarios, podremos generar un ambiente de comunicación pleno y eficiente, complementando el cableado como medio físico que comunique los nodos importantes y las redes inalámbricas como nodos de conexión en áreas metropolitanas, así como en 4G.

Además, se debe adoptar costumbres para mejorar la seguridad existente dentro de nuestras redes cotidianas, como apagar el receptor Wifi cuando no se esté utilizando la red. Aunque ya no estemos haciendo uso de internet nuestro dispositivo seguirá vinculado con el punto de acceso. Cifrar todo tipo de archivo confidencial o que contenga información sensible. Utilizar un cortafuegos debidamente configurado. No escribir información privada o sensible, como por ejemplo información bancaria o personal. En caso de que sea imprescindible enviar

información sensible asegurarse de que el sitio web receptor utiliza SSL (en caso afirmativo contará con un icono de candado en la esquina derecha de la barra del navegador o el nombre http terminará en s, es decir https). Desactivar Wi-Fi Ad-hoc, con el fin de evitar que nuestro dispositivo se conecte a otro dispositivo que no conocemos. Utilizar una red privada virtual o VPN. Evitar las conexiones automáticas a redes Wi-fi, ya que si no se correría el riesgo de conectarse a red Wifi abierta que fuese maliciosa. Instalar y configurar adecuadamente un antivirus. Desconfiar de posibles descargas de aplicaciones Wifi. Estas aplicaciones suelen ser programas maliciosos. No usar la misma contraseña en diferentes sitios, puesto que si una persona obtuviese esta contraseña podría entrar en varios sitios y no solo en uno.Utilizar autenticación de dos pasos, siendo esta mucha más segura que la autenticación por contraseña única. Así podremos tener un red mucho más segura.

Anexo

Figura 1.

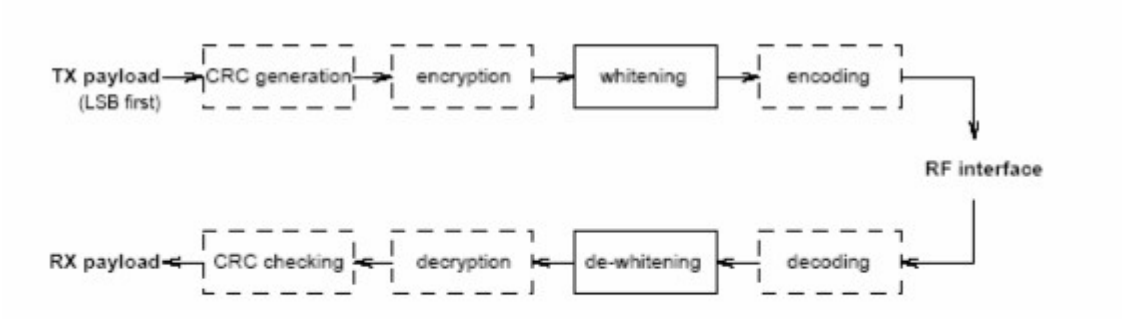


Figura 3.20 – Proceso de TX y RX de los bits de la carga de información [1].

Figura 2.

Protocolo	Año de aparición	Algoritmo de encriptación	Clave secreta	Vector de inicialización	Integración de claves
WEP	1999	RC4	De 40 o 104 bits	24 bits	Ninguna
WPA	2001	RC4	64 bits o 128 bits	48 bits	EAP
WPA2	2005	AES	128 bits	48 bits	EAP

Figura 3.

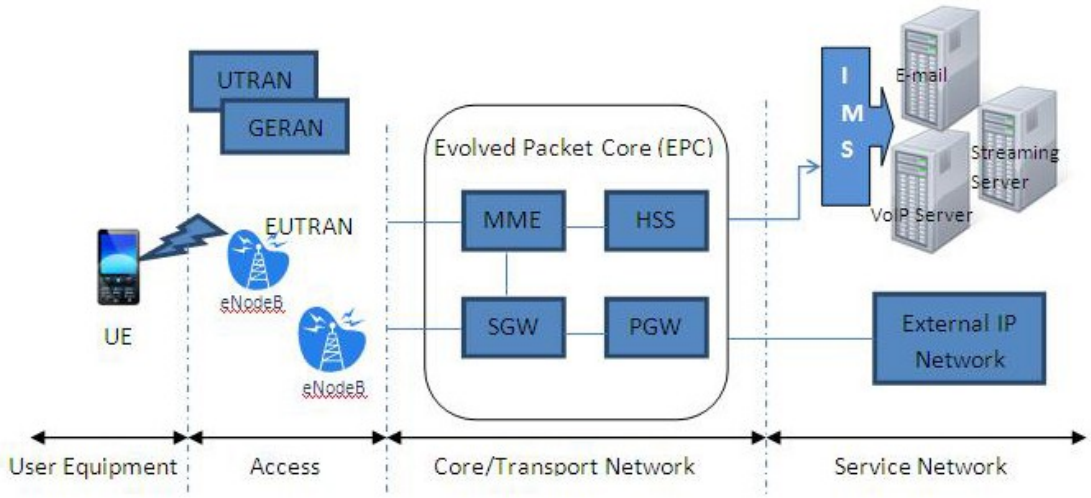


Figure 3: Basic LTE/SAE architecture

Figura 4.

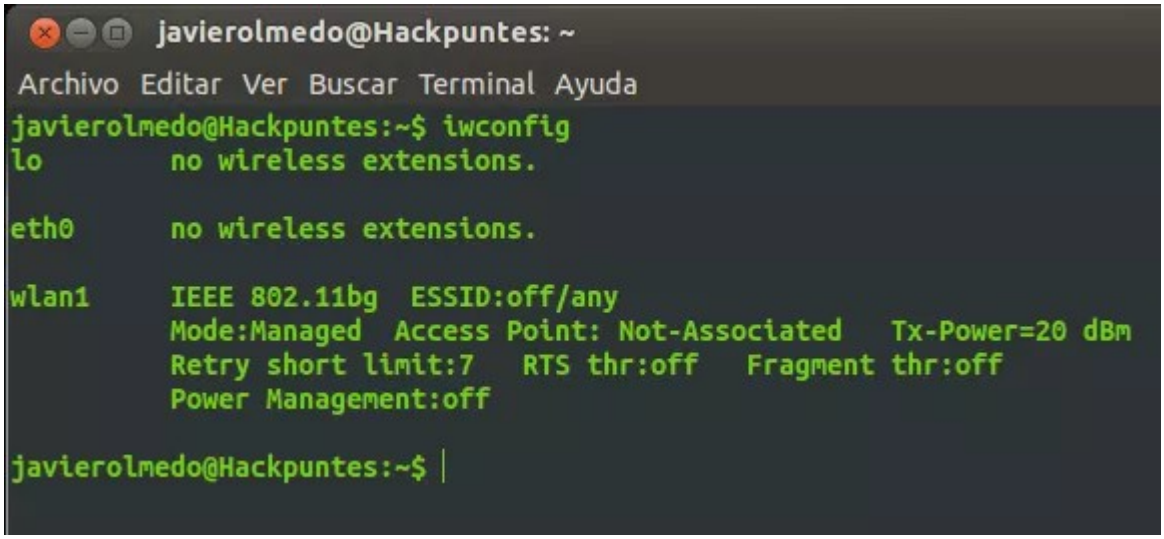
Links de Bibliografia

- http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/archundia_p_fm/capitulo3.pdf
- http://bluehack.elhacker.net/proyectos/bluesec/bluesec.html
- https://es.wikipedia.org/wiki/IEEE_802.15
- http://www.saulo.net/pub/inv/SegWiFi-art.html

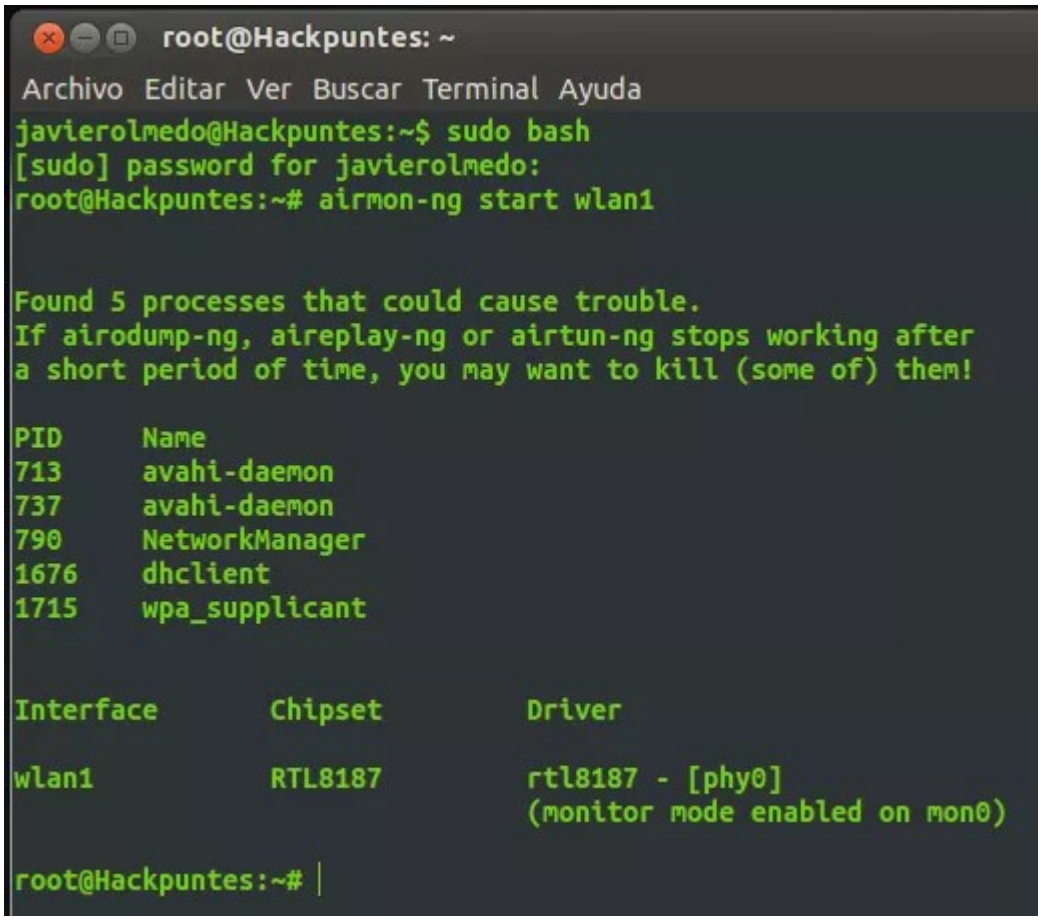
- http://www.academia.edu/9410313/WMAN_Wireless_Metropolitan_Area_Network_WLAN_Wireless_Local_Area_Network_Actividades_WPAN_Wireless_Personal_Area_Network_WPAN_WLAN_WMAN_WWAN_Est%C3%A1ndares
- http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
- https://www.csiac.org/journal-article/4g-lte-security-for-mobile-network-operators/
- http://es.slideshare.net/G0nzal0ve/4glte-38016203
- https://techzine.alcatel-lucent.com/es/seguridad-de-redes-moviles-para-4glte-y-wi-fi
- http://hackpuntes.com/hacking-wifi-parte-vii-seleccionar-el-objetivo-y-capturar-los-paquetes/

Parte EXPERIMENTAL

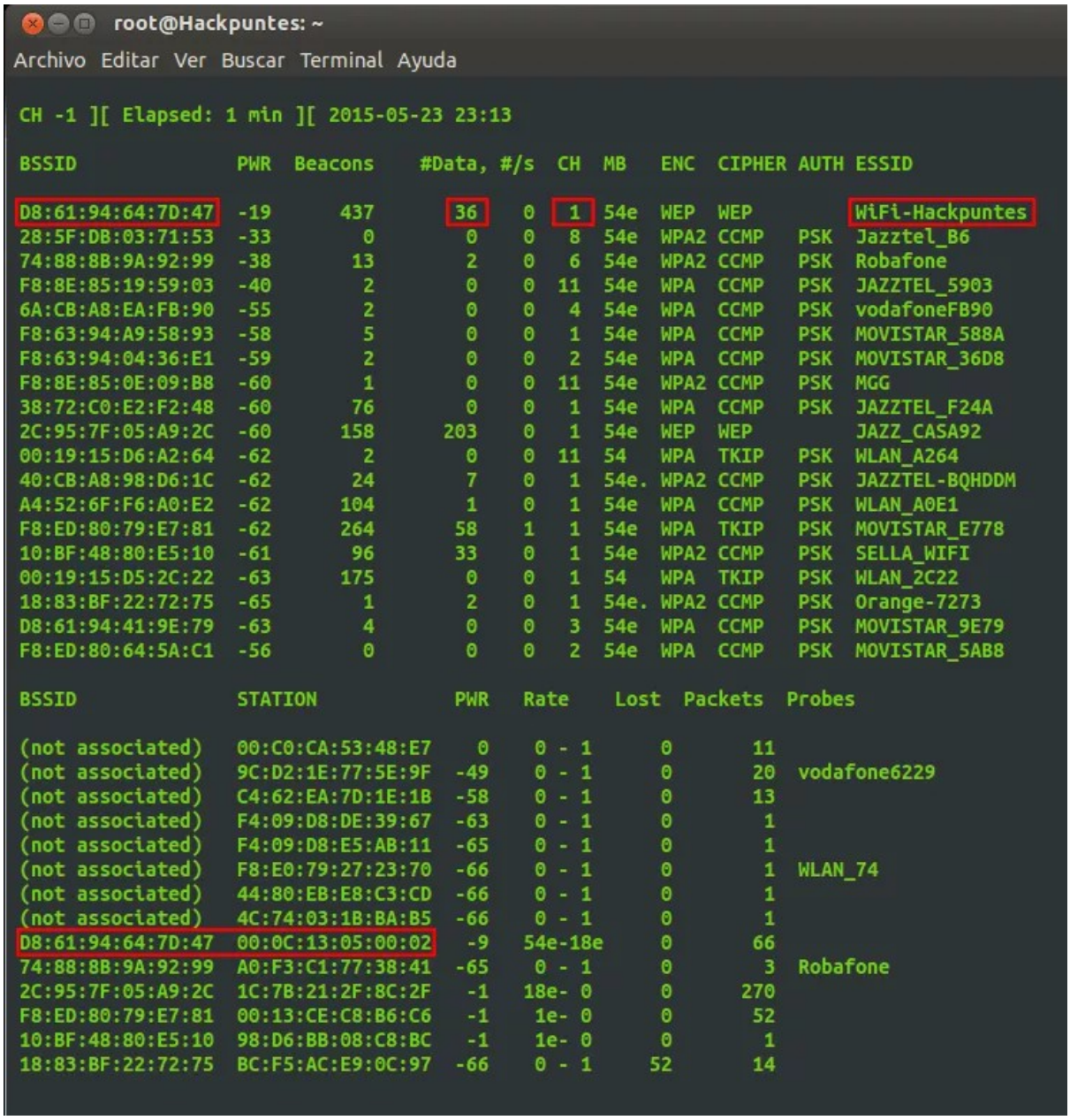
1

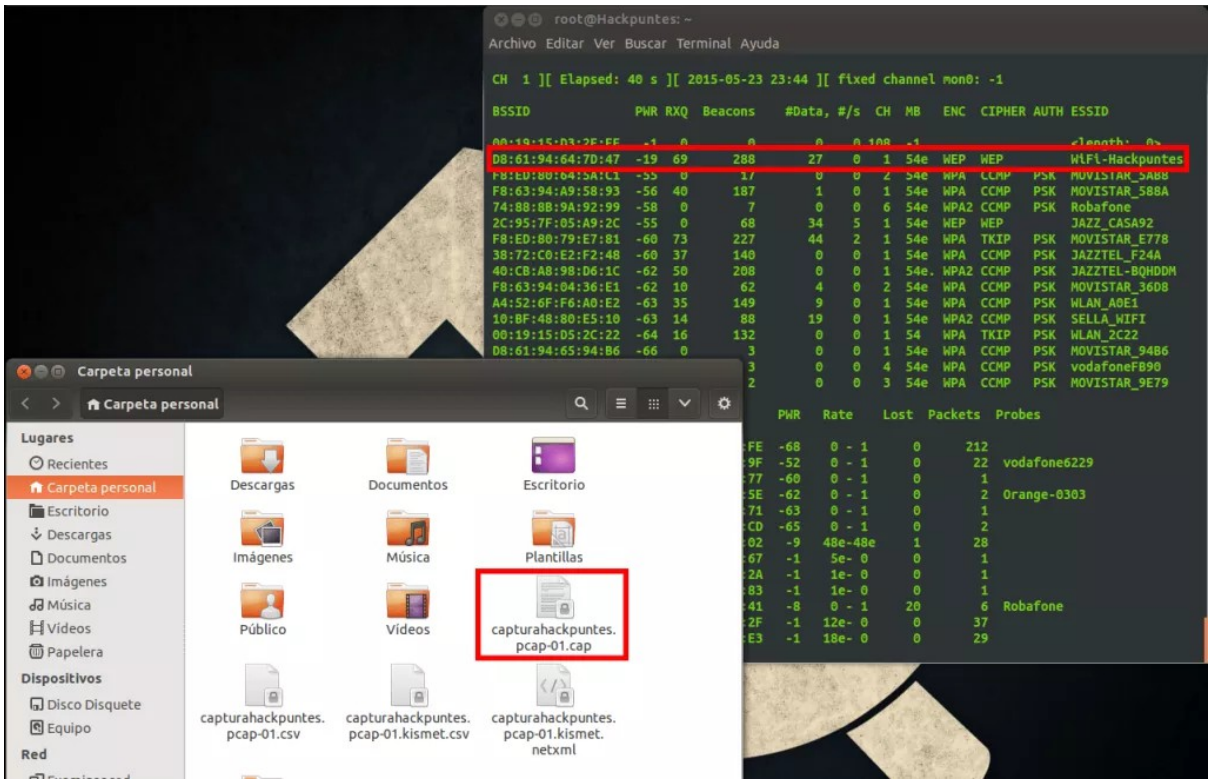


2


root@Hackpuntes: ~
Archivo Editar Ver Buscar Terminal Ayuda
javierolmedo@Hackpuntes:~$ sudo bash
[sudo] password for javierolmedo:
root@Hackpuntes:~# airmon-ng start wlan1
Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
PID Name
713 avahi-daemon
737 avahi-daemon
790 NetworkManager
1676 dhclient
1715 wpa_supplicant
Interface Chipset Driver
wlan1 RTL8187 rtl8187 - [phy0]
(monitor mode enabled on mon0)
root@Hackpuntes:~#

3


root@Hackpuntes: ~
Archivo Editar Ver Buscar Terminal Ayuda
CH -1][Elapsed: 1 min][2015-05-23 23:13
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
D8:61:94:64:7D:47 -19 437 36 0 1 54e WEP WEP WiFi-Hackpuntes
28:5F:DB:03:71:53 -33 0 0 0 8 54e WPA2 CCMP PSK Jazztel_B6
74:88:8B:9A:92:99 -38 13 2 0 6 54e WPA2 CCMP PSK Robafone
F8:8E:85:19:59:03 -40 2 0 0 11 54e WPA CCMP PSK JAZZTEL_5903
6A:CB:A8:EA:FB:90 -55 2 0 0 4 54e WPA CCMP PSK vodafoneFB90
F8:63:94:A9:58:93 -58 5 0 0 1 54e WPA CCMP PSK MOVISTAR_588A
F8:63:94:04:36:E1 -59 2 0 0 2 54e WPA CCMP PSK MOVISTAR_36D8
F8:8E:85:0E:09:B8 -60 1 0 0 11 54e WPA2 CCMP PSK MGG
38:72:C0:E2:F2:48 -60 76 0 0 1 54e WPA CCMP PSK JAZZTEL_F24A
2C:95:7F:05:A9:2C -60 158 203 0 1 54e WEP WEP JAZZ_CASA92
00:19:15:D6:A2:64 -62 2 0 0 11 54 WPA TKIP PSK WLAN_A264
40:CB:A8:98:D6:1C -62 24 7 0 1 54e. WPA2 CCMP PSK JAZZTEL-BQHDDM
A4:52:6F:F6:A0:E2 -62 104 1 0 1 54e WPA CCMP PSK WLAN_A0E1
F8:ED:80:79:E7:81 -62 264 58 1 1 54e WPA TKIP PSK MOVISTAR_E778
10:BF:48:80:E5:10 -61 96 33 0 1 54e WPA2 CCMP PSK SELLA_WIFI
00:19:15:D5:2C:22 -63 175 0 0 1 54 WPA TKIP PSK WLAN_2C22
18:83:BF:22:72:75 -65 1 2 0 1 54e. WPA2 CCMP PSK Orange-7273
D8:61:94:41:9E:79 -63 4 0 0 3 54e WPA CCMP PSK MOVISTAR_9E79
F8:ED:80:64:5A:C1 -56 0 0 0 2 54e WPA CCMP PSK MOVISTAR_5AB8
BSSID STATION PWR Rate Lost Packets Probes
(not associated) 00:C0:CA:53:48:E7 0 0 - 1 0 11
(not associated) 9C:D2:1E:77:5E:9F -49 0 - 1 0 20 vodafone6229
(not associated) C4:62:EA:7D:1E:1B -58 0 - 1 0 13
(not associated) F4:09:D8:DE:39:67 -63 0 - 1 0 1
(not associated) F4:09:D8:E5:AB:11 -65 0 - 1 0 1
(not associated) F8:E0:79:27:23:70 -66 0 - 1 0 1 WLAN_74
(not associated) 44:80:EB:E8:C3:CD -66 0 - 1 0 1
(not associated) 4C:74:03:1B:BA:B5 -66 0 - 1 0 1
D8:61:94:64:7D:47 00:0C:13:05:00:02 -9 54e-18e 0 66
74:88:8B:9A:92:99 A0:F3:C1:77:38:41 -65 0 - 1 0 3 Robafone
2C:95:7F:05:A9:2C 1C:7B:21:2F:8C:2F -1 18e- 0 0 270
F8:ED:80:79:E7:81 00:13:CE:C8:B6:C6 -1 1e- 0 0 52
10:BF:48:80:E5:10 98:D6:BB:08:C8:BC -1 1e- 0 0 1
18:83:BF:22:72:75 BC:F5:AC:E9:0C:97 -66 0 - 1 52 14


root@Hackpuntes: ~
Archivo Editar Ver Buscar Terminal Ayuda
CH 1][Elapsed: 40 s][2015-05-23 23:44][fixed channel mon0: -1
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
D8:61:94:64:7D:47 -19 69 288 27 0 1 54e WEP WEP WlFi-Hackpuntes
F8:63:94:A9:58:93 -56 40 187 1 0 1 54e WPA CCMP PSK MOVISTAR_588A
74:88:8B:9A:92:99 -58 0 7 0 0 6 54e WPA2 CCMP PSK Robafone
2C:95:7F:05:A9:2C -55 0 68 34 5 1 54e WEP WEP JAZZ_CASA92
F8:ED:80:79:E7:81 -60 73 227 44 2 1 54e WPA TKIP PSK MOVISTAR_E778
38:72:C0:E2:F2:48 -60 37 140 0 0 1 54e WPA CCMP PSK JAZZTEL_F24A
40:CB:A8:98:D6:1C -62 50 208 0 0 1 54e. WPA2 CCMP PSK JAZZTEL-BQHDDM
F8:63:94:04:36:E1 -62 10 62 4 0 2 54e WPA CCMP PSK MOVISTAR_36D8
A4:52:6F:F6:A0:E2 -63 35 149 9 0 1 54e WPA CCMP PSK WLAN_A0E1
10:BF:48:80:E5:10 -63 14 88 19 0 1 54e WPA2 CCMP PSK SELLA_WIFI
00:19:15:D5:2C:22 -64 16 132 0 0 1 54 WPA TKIP PSK WLAN_2C22
D8:61:94:65:94:B6 -66 0 3 0 0 1 54e WPA CCMP PSK MOVISTAR_94B6
3 0 0 4 54e WPA CCMP PSK vodafoneFB90
2 0 0 3 54e WPA CCMP PSK MOVISTAR_9E79
PWR Rate Lost Packets Probes
FE -68 0 - 1 0 212
9F -52 0 - 1 0 22 vodafone6229
77 -60 0 - 1 0 1
5E -62 0 - 1 0 2 Orange-0303
71 -63 0 - 1 0 1
CD -65 0 - 1 0 2
02 -9 48e-48e 1 28
67 -1 5e- 0 0 1
2A -1 1e- 0 0 1
83 -1 1e- 0 0 1
41 -8 0 - 1 20 6 Robafone
2F -1 12e- 0 0 37
E3 -1 18e- 0 0 29
Carpeta personal
Carpeta personal
Lugares
Recientes
Carpeta personal
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
Papelera
Dispositivos
Disco Disquete
Equipo
Red
Descargas
Documentos
Escritorio
Imágenes
Música
Plantillas
Público
Vídeos
capturahackpuntes.pcap-01.cap
capturahackpuntes.pcap-01.csv
capturahackpuntes.pcap-01.kismet.csv
capturahackpuntes.pcap-01.kismet.netxml