

**Instituto Politécnico Nacional**

**Escuela Superior de Cómputo**

**Soto Ramos Manuel Alejandro**

Administración de Servicios en Red

**Auditoria de Redes ESCOM.**

Grupo: 4CV4

**Jiménez Maruri Pedro**

**Romero Serrano Luis**

**Valencia Rodriguez Fernando**

# Índice

[**Índice**](#_23knnps4myxl) **2**

[**Antecedentes**](#_otxzzrjodis2) **3**

[**Aircrack-ng**](#_wlgubt14l4ww) **4**

[**Zenmap**](#_2h37t6smi2je) **6**

[**Access Point**](#_eugeoki7jm0g) **6**

[Extreme Mobility AP3917](#_2xa6dadnvyof) 7

[AeroHive AP1130](#_73hpf9ljip9u) 8

[**Análisis de los datos**](#_2y2ghyi506ir) **9**

[Servicios en Red](#_3av36mmlvgb6) 11

[**Conclusiones**](#_ieql4k6vrtad) **13**

[**Referencias**](#_3xjxx7o0syld) **13**

# 

# **Antecedentes**

Para empezar con el análisis ocupamos la herramienta Aircrack-ng, la cual consiste en un analizador de paquetes de redes, un crackeador de redes WEP y WPA/WPA2-PSK. Ocupando entre sus herramientas:

* **Airodump-ng:** escanea las redes y captura vectores de inicio
* **Airmon-ng:** establece la tarjeta inalámbrica en modo monitor, capturar e inyectar vectores

De igual manera utilizamos la herramienta Zenmap, que proporciona una interfaz gráfica para ejecutar comandos Nmap y mostrarlos de forma intuitiva usuarios menos experimentados.

Antes de analizar los puntos de acceso de la Escuela Superior de Cómputo, decidimos solo analizar ciertos puntos (o ciertos salones), con el fin de reducir los datos similares, ya que si se supervisaba salón por salón al estar muy pegados el radio de la señal Wi-Fi se sobre alteraban, dándonos una mayor inconsistencia en los resultados.

Para evitar esto, decidimos hacer el análisis en el piso de en medio, haciendo un salto de un salón. Los siguientes salones, son nuestros puntos de referencia para esta práctica:

**Edificio 1:**

* Salón 1103 - Sala de impresiones
* Salón 1106 - Laboratorio S4
* Salón 1110
* Salón 1113

**Edificio 2:**

* Salón 2103 - Unidad Politécnica de Integración Social (UPIS)
* Salón 2106 - Laboratorio S2
* Salón 2110.
* Salón 2113.

**Edificio Central o Edificio de Laboratorios:**

* Departamento de ingeniería en Sistemas Computacionales.
* Departamento de Ciencias e ingeniería de la computación.
* Comisión Académica de Trabajos Terminales (CATT).
* Laboratorio de Sistemas Digitales y Teoría de Señales.



Localización de los salones donde se analizó la red inalámbrica

# **Aircrack-ng**

Esta suite de herramientas ya se encuentra instalada dentro del sistema operativo Kali Linux. Pero en caso de que se requiera instalar en otro sistema operativo Unix se hará de la siguiente manera.

Primero hay que instalar la herramienta usando el siguiente comando

sudo apt-get install -y aircrack-ng

sudo apt-get

Después tenemos que habilitar el modo monitor con el siguiente comando

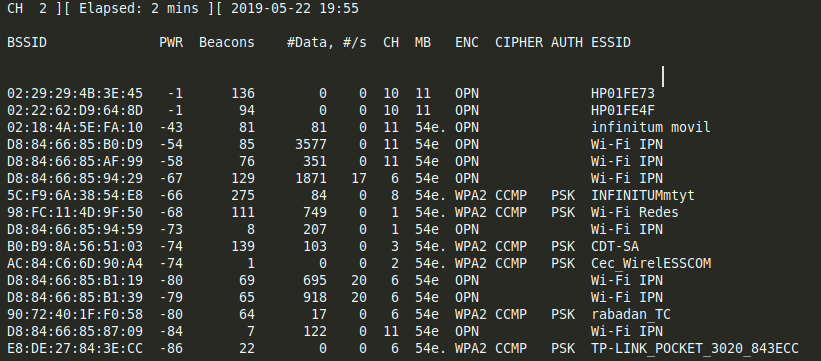
sudo airmon-ng start wlp3s0

Para este ejemplo el nombre de nuestra interface de red Wi-Fi se llama wlp3s0, usualmente se llama wlan0, pero eso ya varia de cada computador. Para verificar el nombre de su interfaz basta con utilizar el comando **ifconfig** en la terminal de comandos.

Una vez habilitado podemos verificar utilizando el comando **ifconfig** nos aparecerá de la siguiente manera “wlp3s0mon” y con ello podemos utilizar la instrucción:

sudo airodump-ng wlp3s0mon

y nos mostrará en la ventana algo similar a esto:



El cual nos muestra:

* **BSSID:** Direcciones Mac del punto de acceso.
* **PwR:** Nivel de señal (Depende de la tarjeta de red).
* **Beacons:** Número de paquetes de anuncios enviados por el AP.
* **#Data:** Número de paquetes de datos capturados.
* **#/s:** El número de paquetes de datos por segundo.
* **CH:** Número de canal de la red wireless.
* **MB:** Velocidad máxima soportada por el AP.
* **ENC:** Algoritmo de cifrado en uso.
* **CIPHER:** Tipo de cifrado que utiliza la red.
* **AUTH:** El protocolo de autenticación utilizado.
* **ESSID:** Nombre de la red wireless

Como se puede ver se pueden obtener una gran cantidad de datos de redes wifi con esta herramienta, además nos permite filtrar y ordenar por medio de argumentos y opciones en el comando.

Normalmente en un entorno pequeño suele haber un número importante de puntos de acceso Wi-Fi, por lo que la tabla que muestra el comando sobrepasa el tamaño de la consola y la información se corta. Por lo que recomendamos guardar el resultado del ejercicio en un archivo con formato CSV, para poder dar un mejor tratamiento a la información

airodump-ng -w nombreDelArchivo --output-format csv wlp3s0mon

# 

# **Zenmap**

Esta suite de herramientas ya se encuentra instalada dentro del sistema operativo Kali Linux. Pero en caso de que se requiera instalar en otro sistema operativo Unix se hará de la siguiente manera.

Primero hay que instalar la herramienta nmap para poder usar los comandos en caso de que se quiera realizar la terminal y es con el siguiente comando

sudo apt-get install nmap

Para la versión gráfica podemos ir al centro de software de Ubuntu y ahí se encuentra la aplicación, basta con seleccionar instalar y para abrirlo con permisos root utilizaremos en la terminal el siguiente comando:

sudo zenmap

# **Access Point**

Es un dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que enlaza dispositivos móviles o tarjetas de red inalámbricas. Son dispositivos que son configurados en redes de tipo inalámbricas que son intermediarios entre una computadora y una red (Internet o local). Facilitan conectar varias máquinas cliente sin la necesidad de un cable (mayor portabilidad del equipo) y que estas posean una conexión sin limitar tanto su ancho de banda.

Con los datos obtenidos con airodump, podemos verificar la dirección MAC de los access point y con esto podemos buscar el fabricante y posible modelo del punto de acceso. En nuestro caso pudimos averiguar que la red **Wi-Fi IPN** está constituido por AP Extreme Mobility, con el modelo más posible AP3917. Mientras que la red **Wi-Fi ESCOM** la constituyen AP AeroHive con el posible modelo AP1130.

Con esto también podemos saber cuales son las características que tienen los Access Point y poder ser más precisos en nuestras medición e interpretaciones para calcular la zona de disponibilidad y la capacidad de cada punto de acceso.

## 

## **Extreme Mobility AP3917**

Este tipo de access point son utilizados para la red llamada “Wifi IPN” [7]

## 

## 

## **AeroHive AP1130**

Este tipo de access point son utilizados para la red llamada “Wifi Escom” así como para sus similares. [8]



**Características:**

* Especificaciones de radio — 802.11a
  + 5.150–5.950 GHz de frecuencia de funcionamiento.
  + Modulación de multiplexación por división de frecuencia ortogonal (OFDM)
  + Tarifas (Mbps): 54, 48, 36, 24, 18, 12, 9, 6 con reducción automática.
* Especificaciones de radio — 802.11b
  + Frecuencia de operación 2.4-2.5 GHz
  + Modulación de secuencia directa de espectro expandido (DSSS)
  + Tarifas (Mbps): 11, 5.5, 2, 1 w / auto fallback
* Especificaciones de radio — 802.11n
  + Frecuencia de operación de 2.4–2.5 GHz y 5.150–5.950 GHz
  + Modulación 802.11n
  + Tarifas (Mbps): MCS0 - MCS15 (6.5MBps - 300Mbps)
* Especificaciones de radio - 802.11ac
  + 5.150–5.950 GHz de frecuencia de funcionamiento
  + Modulación 802.11ac (256-QAM)
  + Tarifas (Mbps): MCS0 – MCS9 (6.5Mbps - 867 Mbps), NSS = 1-2.
* Montaje
  + Montado en la pared
  + Montado en el poste: correa para poste de 1-2.75 pulgadas incluida con el AP
* Antenas
  + 4 conexiones de antena tipo jack N para antenas externas
  + Antenas vendidas como accesorio

# **Análisis de los datos**

Como se mencionó anteriormente se tomaron muestras en varios puntos del edificio. Se realizó un vaciado de datos varios documentos en excel y se procedió a depurar la información. Ya que solo nos interesan las redes de acceso abierto y las redes de la escuela, se filtró los datos para poder tener solo estas redes a vista y que fuera más fácil su procesado.

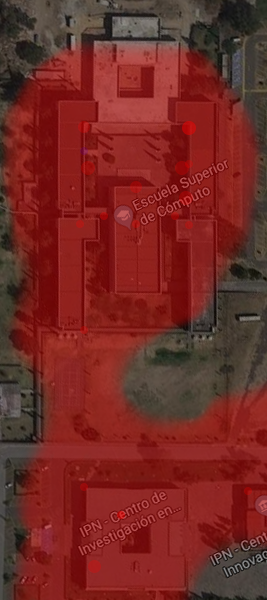
Una vez con el enfoque en los datos correctos, se continuó a revisar las similitudes de las señales en los diferentes puntos medidos, se tomaron las MACs de los datos, se empataron con las distintas muestras. y con los datos de velocidad, paquetes y poder, se realizó una triangulación de la señal para poder aproximar la posición del punto de emisión (Access Point).

Esto se hizo por cada una de las MAC que aparecían en los datos. Esto nos permite generar un mapeado del edificio con las posibles localizaciones, como se muestra en la siguiente imagen.



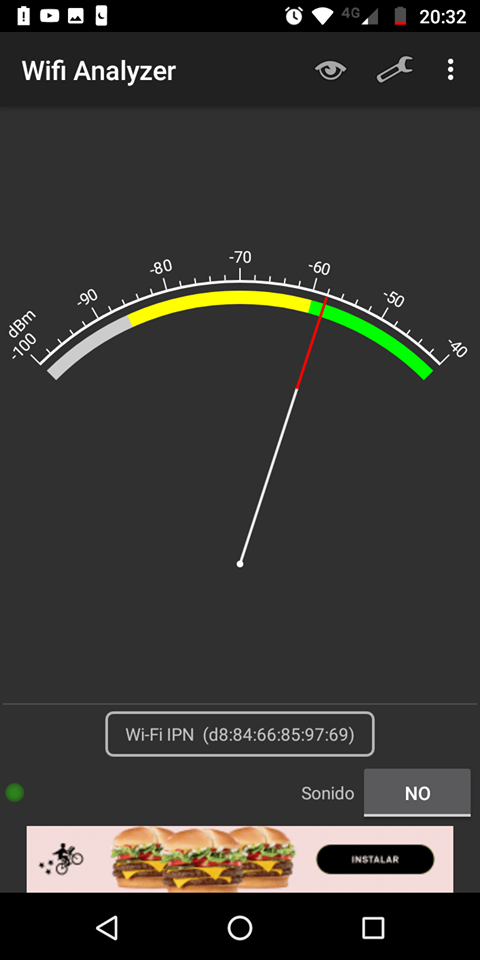
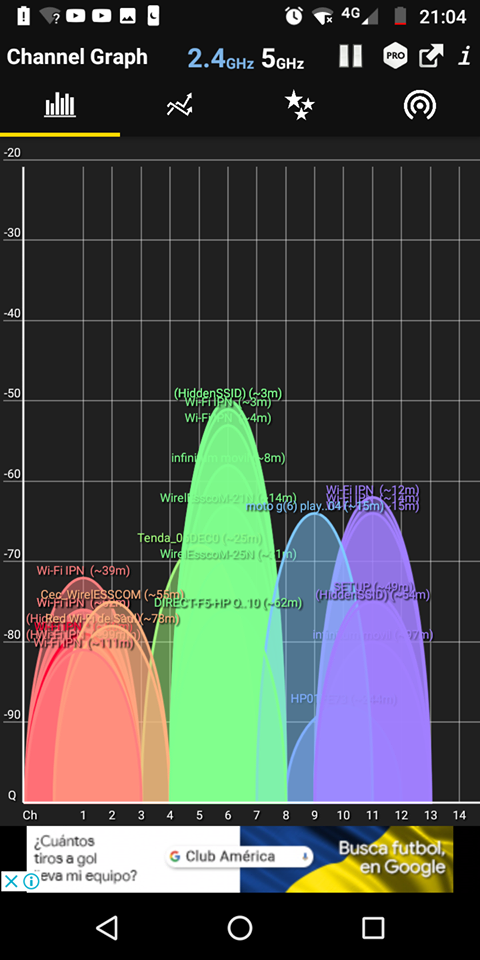
Los puntos que vemos en las imágenes no reflejan la posición real, sino más bien su posible ubicación, algunos de los cuales sí corresponderá a la realidad, mientras otros requerirán de ajustes. Cual sea el caso, con esto ya podemos darnos una idea bastante buena de la cobertura y la capacidad de la red.

Con los datos de las especificaciones de los Access Points y otras datos medidos se pudo realizar un mapa de la cobertura de la red inalámbrica, la cual es bastante precisa a la que podemos notar en la actualidad.



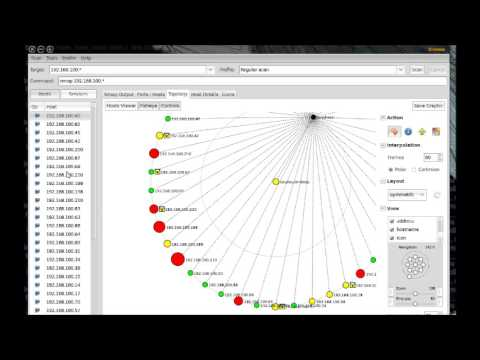
Con este mapa podemos notar que la mayoría de las instalaciones están cubiertas. Aunque la señal tambien dependera de la antena del dispositivo cliente, pudiendo obtener una zona con mayor área.

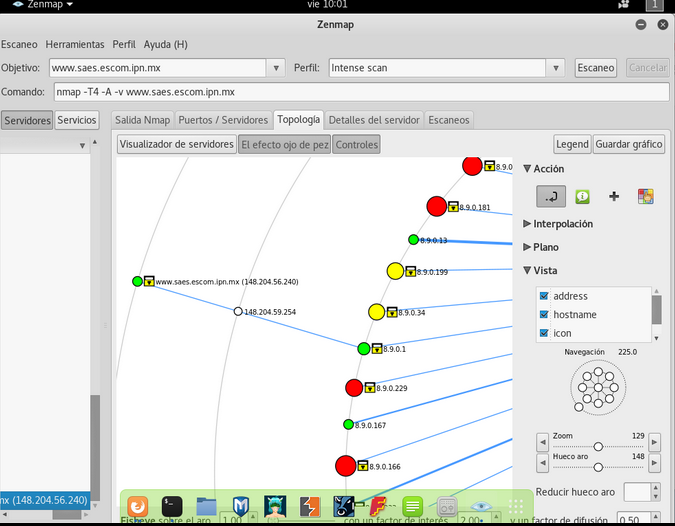
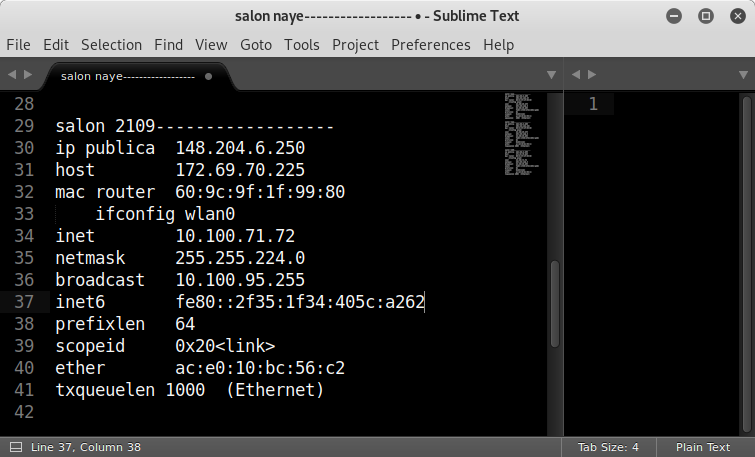
Comprobando con un dispositivo android pudimos notar como la información resultante era bastante precisa. Se bordeo a pie la zona para hacer esta comprobación.



## **Servicios en Red**

Después de ver el área, se escaneó la red para ver cuántos clientes había en el momento, para esto se utilizó la herramienta Zenmap. En el momento del escaneo había 82 usuarios conectados a la red, 4 servidores HTTP, 3 FTP. Se tiene en suposición que estos servicios, eran por parte de los alumno, ya que tener un servicio de estos en una red inalámbrica es ineficiente.



****

# **Conclusiones**

Con todos estos análisis se pudo reflejar la capacidad y calidad de la red Wi-Fi. Se pudo notar que la cobertura es buena, la señal es potente y la capacidad es la adecuada. Sin embargo, aún quedan zonas donde la señal es baja, además de que en el proceso de medición pudimos notar que había antenas que no estaban operando o que les faltaba mantenimiento, ya que producen una señal débil aun estando cerca de los puntos de acceso. También nos percatamos que había antenas apagadas y había algunas otras que prendian y apagaban de forma intermitente, causando que los clientes conectados a ese Access Point tengan que migrar y pierdan la coneccion y tiempo.

Son estos pequeños detalles aunado al limitado ancho de banda de la red que se pueden percibir una calidad media en la red de internet inalámbrica. Si diera mantenimiento y el ancho de banda de ajustara a la demanda, el servicio tendría fallos mínimos

# **Referencias**

**[1].** https://es.wikipedia.org/wiki/Aircrack-ng

**[2].** http://www.escom.ipn.mx/htmls/conocenos/organigramaDirectorio.php

**[3].** https://www.aircrack-ng.org/doku.php?id=airodump-ng

**[4].**https://www.extremenetworks.com/product/ap3917/?fbclid=IwAR16AFFPocF\_ffdZabvGHNXiqKtRPTYP3XL29a8sGqQg-KgkQZFfeuWvLJI#

**[5].**https://www.aerohive.com/products/access-points/

**[6].**https://es.wikipedia.org/wiki/Punto\_de\_acceso\_inal%C3%A1mbrico

**[7].**https://www.extremenetworks.com/product/ap3917/?fbclid=IwAR3x6cewbRxOc-d-NrqfZbKw-9SHlFmvps-ncTlfj-DijzjcTDVs8sh\_jf8

**[8]**.https://www.aerohive.com/wp-content/uploads/Aerohive\_Datasheet\_AP1130.pdf?fbclid=IwAR1Q-lKzr8olecqvAede4GAGDYD6n8bMKo2\_ONvenUsnvwnuZ-1ri0JYLGQ

Misión

Empresa de Servicio dedicada a satisfacer las necesidades de Mantenimiento que el cliente requiera, elevando el rendimiento en sus equipos de cómputo y mejorado los sistemas de información, a través del diagnóstico y supervisión de nuestro personal.

Visión

Ser reconocida como una empresa a nivel regional, brindando servicios de mantenimiento de computo y asistiendo personalmente en un corto lapso de tiempo satisfacer las necesidades del cliente y una supervisión constante de sus equipos.