Antikörper

Wireless Intrusion Detection Systems

Simulación

Josu Barrientos Bahamonde

Trabajo de Fin de Grado

Índice

Introducción

En este documento se mostrarán las simulaciones de los módulos principales del Wireless Intrusion Detection System (WIDS), junto a una breve explicación del funcionamiento de cada uno de los módulos y cada una de las fases del funcionamiento de estos.

NOTA: La explicación completa del funcionamiento del sistema, junto a un análisis del código usado para el desarrollo del software, serán incluidos en el documento del Trabajo de Fin de Grado

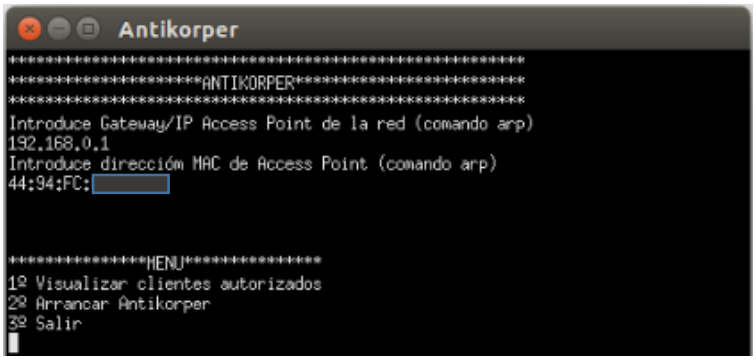
---

Simulación

Módulo de Filtrado Principal

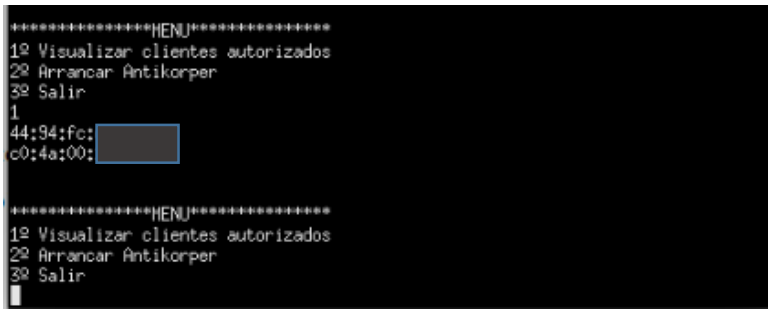
Este módulo será el encargado de monitorizar el tráfico dentro de la red a proteger. El trafico recibido será filtrado, por un lado, en base a un MAC filtering de los clientes autorizados previamente incluidos en los ficheros de configuración de sistema. Por otro lado, será tratado mediante un filtro de trafico ARP, mediante el cual, obtendrá la información necesaria para detectar un ataque ARP Poisoning, evitando así los ataques que derivan de este.

- Arranque del módulo



Nada más arrancar el módulo de filtrado, se pedirá al usuario la información básica de la red que desea proteger. Estos datos serán la dirección IP del Gateway de la red y la dirección MAC del punto de acceso. Tras eso, mostrara un menú con la opción de visualizar los clientes de la red que ha autorizado el usuario y el botón de arranque del sistema.

- Visualización

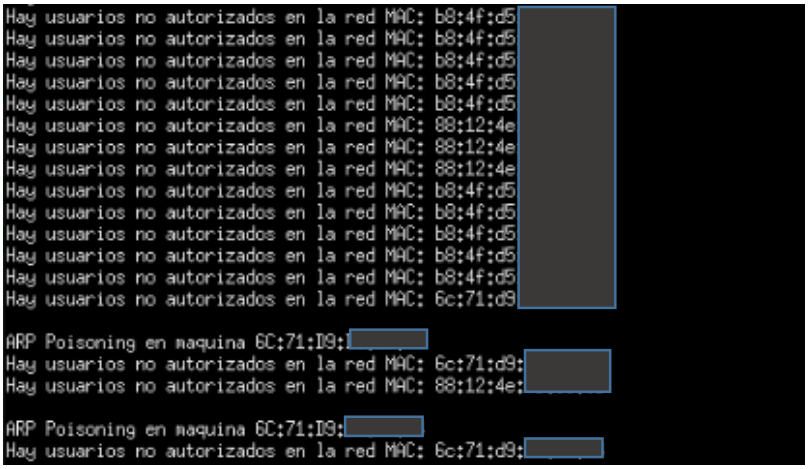


Pulsando la opción 1, cargara del fichero de clientes autorizados un listado de estos.

- Selección de interfaces de monitorización

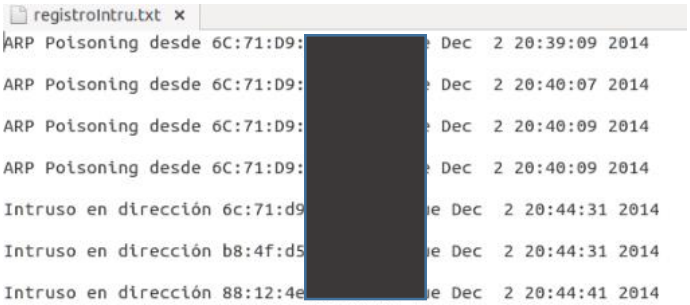
Al seleccionar la opción 2, se listaran por pantalla los interfaces disponibles en el equipo sobre el que corre el sistema. Una vez elegido el interfaz, se deberá introducir el nombre con el que muestra el interfaz.

- Información en vivo



Mientras el software realiza los análisis correspondientes, informara al usuario de los clientes no autorizados detectados en la red y de los ataques ARP Poisoning llevados a cabo, junto a la dirección física del intruso o del atacante.

- Ficheros de registro



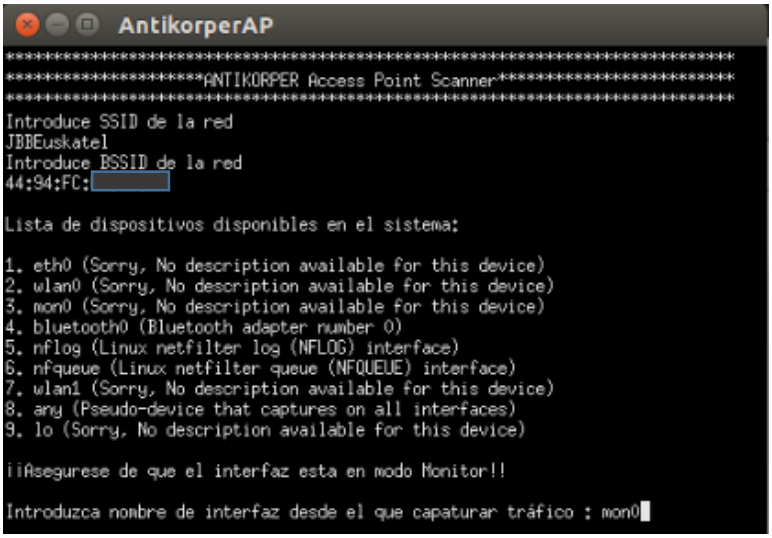
El software creara un fichero de registro en que las entradas tendrán la siguiente estructura:

[Tipo de ataque] [Dirección Física] [Fecha/Hora de ataque]

Módulo de escaneo de Puntos de Acceso/Access Point

Este módulo será el encargado de escanear el entorno de la red que se desea proteger, para así mantener un registro de los Access Point (AP) cercanos y monitorizar el tráfico en busca de ataques de tipo Rogue AP. Solo serán necesario procesar las Beacon frame pertenecientes al IEEE 802.11.

- Arranque de módulo



De la misma manera que el módulo de filtrado, este pedirá los siguientes datos básicos:

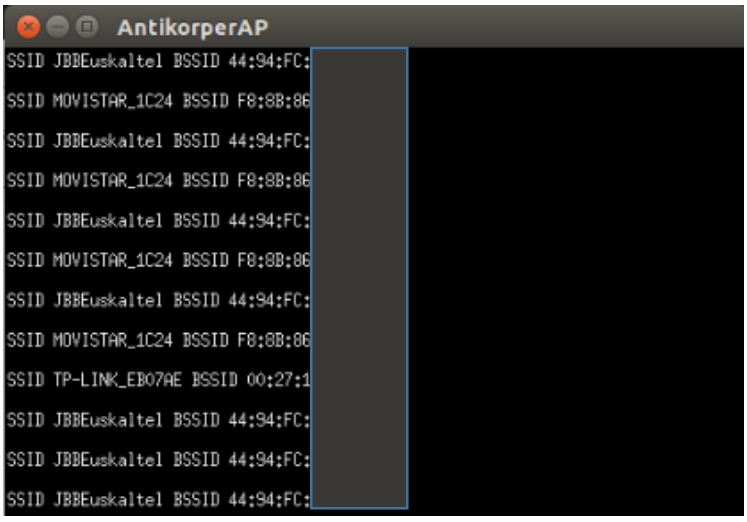
- SSID (**S**ervice **S**et **ID**entifier): Nombre de la red a proteger.
- BSSID (***B**asic **S**ervice **S**et **Id**entifier*): Direction MAC del Access Point.

Tras esto, listara los interfaces disponibles en el equipo para la selección por parte del usuario.

NOTA: Necesario configurar previamente el interfaz escogido en modo Monitor

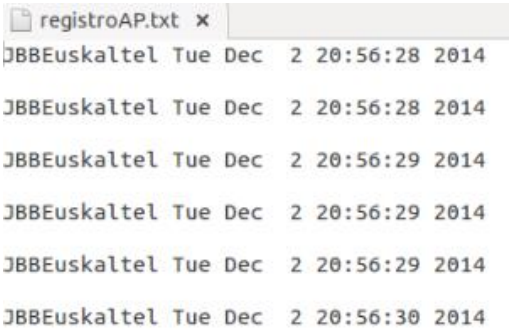
---

- Información en vivo



El sistema mostrara extraerá la información básica de los Beacon frames recibidos, entre esta información se encuentra el SSID y el BSSID de cada frame, los cuales visualizara por pantalla.

- Ficheros de registro



El software creara un fichero de registro que contendrá, en caso de que se haya detectado un Rogue AP, la SSID de este junto la fecha y hora a la que ha sido visto.

NOTA: El fichero ha sido creado de manera manual debido a falta de infraestructura

---