

Antikörper

Wireless Intrusion Detection Systems

Simulación

Josu Barrientos Bahamonde

Trabajo de Fin de Grado

Índice

Introducción	3
Simulación	4
Módulo de Filtrado Principal	4
Módulo de escaneo de Puntos de Acceso/Access Point	6

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.

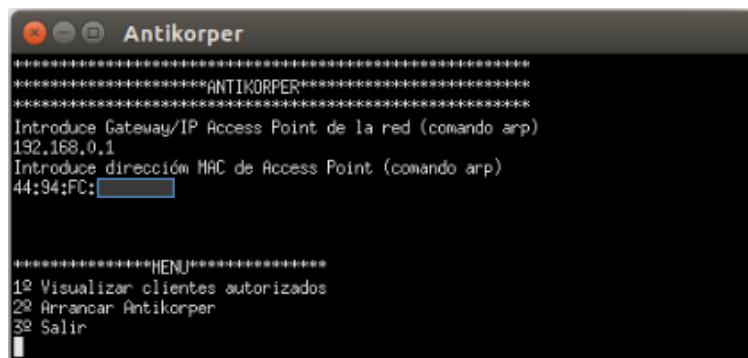
NOTA: La explicación completa del funcionamiento del sistema, junto a un análisis del código usado para el desarrollo del software, serán incluidos en el documento del Trabajo de Fin de Grado

Simulación

Módulo de Filtrado Principal

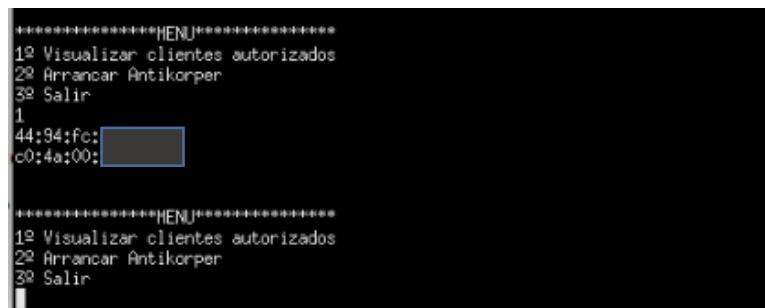
Este módulo será el encargado de monitorizar el tráfico dentro de la red a proteger. El tráfico recibido será filtrado, por un lado, en base a un MAC filtering de los clientes autorizados previamente incluidos en los ficheros de configuración de sistema. Por otro lado, será tratado mediante un filtro de tráfico 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

```
*****MENU*****
1º Visualizar clientes autorizados
2º Arrancar Antikörper
3º Salir
2

Lista de dispositivos disponibles en el sistema:

1. eth0 (Sorry, No description available for this device)
2. wlan0 (Sorry, No description available for this device)
3. mon0 (Sorry, No description available for this device)
4. tap0 (Sorry, No description available for this device)
5. bluetooth0 (Bluetooth adapter number 0)
6. nflog (Linux netfilter log (NFLOG) interface)
7. nfqueue (Linux netfilter queue (NFQUEUE) interface)
8. wlan1 (Sorry, No description available for this device)
9. mon1 (Sorry, No description available for this device)
10. any (Pseudo-device that captures on all interfaces)
11. lo (Sorry, No description available for this device)

Introduzca nombre de interfaz desde el que capturar tráfico : ■
```

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

```
Hay usuarios no autorizados en la red MAC: b8:4f:d5
Hay usuarios no autorizados en la red MAC: b8:4f:d5
Hay usuarios no autorizados en la red MAC: b8:4f:d5
Hay usuarios no autorizados en la red MAC: b8:4f:d5
Hay usuarios no autorizados en la red MAC: b8:4f:d5
Hay usuarios no autorizados en la red MAC: 88:12:4e
Hay usuarios no autorizados en la red MAC: 88:12:4e
Hay usuarios no autorizados en la red MAC: 88:12:4e
Hay usuarios no autorizados en la red MAC: b8:4f:d5
Hay usuarios no autorizados en la red MAC: b8:4f:d5
Hay usuarios no autorizados en la red MAC: b8:4f:d5
Hay usuarios no autorizados en la red MAC: b8:4f:d5
Hay usuarios no autorizados en la red MAC: 6c:71:d9

ARP Poisoning en maquina 6C:71:D9:■
Hay usuarios no autorizados en la red MAC: 6c:71:d9:■
Hay usuarios no autorizados en la red MAC: 88:12:4e:■

ARP Poisoning en maquina 6C:71:D9:■
Hay usuarios no autorizados en la red MAC: 6c:71:d9:■
```

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

```
registrointru.txt x
ARP Poisoning desde 6C:71:D9:■ Dec 2 20:39:09 2014
ARP Poisoning desde 6C:71:D9:■ Dec 2 20:40:07 2014
ARP Poisoning desde 6C:71:D9:■ Dec 2 20:40:09 2014
ARP Poisoning desde 6C:71:D9:■ Dec 2 20:40:09 2014
Intruso en dirección 6c:71:d9 Dec 2 20:44:31 2014
Intruso en dirección b8:4f:d5 Dec 2 20:44:31 2014
Intruso en dirección 88:12:4e Dec 2 20:44:41 2014
```

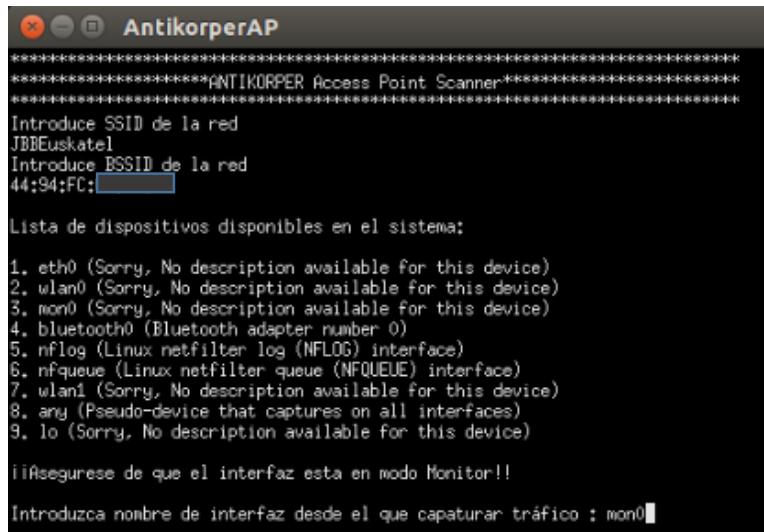
El software creara un fichero de registro en que las entradas tendrán la siguiente estructura:

[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



The screenshot shows a terminal window titled "AntikorperAP". It displays the following text:

```
*****ANTIKORPER Access Point Scanner*****
Introduce SSID de la red
JBBEuskalte1
Introduce BSSID de la red
44:94:FC:_____
```

Lista de dispositivos disponibles en el sistema:

1. eth0 (Sorry, No description available for this device)
2. wlan0 (Sorry, No description available for this device)
3. mon0 (Sorry, No description available for this device)
4. bluetooth0 (Bluetooth adapter number 0)
5. nflog (Linux netfilter log (NFLOG) interface)
6. nfqueue (Linux netfilter queue (NFQUEUE) interface)
7. wlan1 (Sorry, No description available for this device)
8. any (Pseudo-device that captures on all interfaces)
9. lo (Sorry, No description available for this device)

!!Asegurese de que el interfaz esta en modo Monitor!!

Introduzca nombre de interfaz desde el que capturar tráfico : mon0

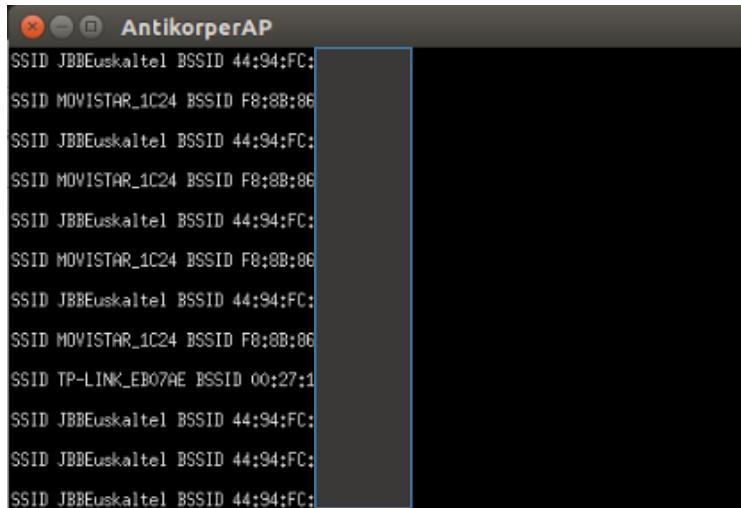
De la misma manera que el módulo de filtrado, este pedirá los siguientes datos básicos:

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

Tras esto, listará 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

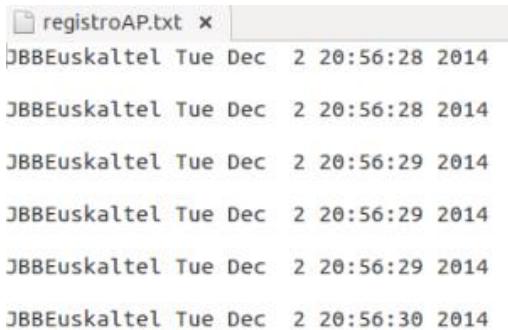


The screenshot shows a terminal window titled "AntikorperAP". It displays a list of nearby access points:

```
SSID JBBEuskalte1 BSSID 44:94:FC:  
SSID MOVISTAR_1C24 BSSID F8:8B:86  
SSID TP-LINK_EB07AE BSSID 00:27:1  
SSID JBBEuskalte1 BSSID 44:94:FC:  
SSID JBBEuskalte1 BSSID 44:94:FC:  
SSID JBBEuskalte1 BSSID 44:94:FC:
```

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



```
JBBEuskaltel Tue Dec 2 20:56:28 2014
JBBEuskaltel Tue Dec 2 20:56:28 2014
JBBEuskaltel Tue Dec 2 20:56:29 2014
JBBEuskaltel Tue Dec 2 20:56:29 2014
JBBEuskaltel Tue Dec 2 20:56:29 2014
JBBEuskaltel Tue Dec 2 20:56:30 2014
```

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
