Problemáticas WBTS

# Escaneo red IP

## Problemática

Se pretende escanear una red IP vía ARP. ARP es un protocolo que nos permite descubrir la dirección MAC de un dispositivo a través de su dirección IP siempre y cuando dicho dispositivo se encuentre en nuestra misma red.

El principal problema es que existen dispositivos que para que no puedan ser rastreados en redes IP, no responden a las peticiones ARP para descubrir si dicho dispositivo está activo.

## Alternativas de solución

Aunque dichos dispositivos no reaccionen a las peticiones ARP, estos sí que pueden generar peticiones ARP con dirección destino broadcast a nivel de enlace.

Los paquetes ARP con destino broadcast sí se pueden capturar e inspeccionar. A través de este escaneo pasivo sí sería posible conocer sí un determinado equipo está activo en nuestra misma red IP.

El escaneo ARP se haría de dos formas:

* Escaneo ARP activo: se pretende lanzar un conjunto de ARP requests para toda la red y registrar los dispositivos que estén activos.
* Escaneo ARP pasivo: trataría de escuchar el tráfico de tipo ARP y broadcast de nivel 2 y registrar los dispositivos que estén activos.

Otra forma de escanear una red IP sería vía DHCP. Se pretende escuchar el tráfico a nivel dos que sea tipo DHCP y registrar los dispositivos que quieran tener asignada un dirección IP.

# Trazabilidad de usuarios

## Problemática

Durante el escaneo de dispositivos Bluetooth y de una red IP nos interesa conocer la dirección MAC de dicho dispositivo ya que lo identifica unívocamente a él.

Esto puede dar a entender que se está registrando a un dispositivo de forma poco anónima porque se puede conocer la dirección real y localización en la que se ha encontrado un determinado dispositivo.

## Alternativas de solución

Sí bien la dirección MAC de un dispositivo lo identifica únicamente a él, se propone que solamente se registre un hash de dicha dirección MAC del cual no se pueda revertir el cambio (computacionalmente exigente).

De esta forma tenemos una secuencia de bytes que identifican que un dispositivo ha estado activo durante el escaneo pero no se puede conocer el dispositivo en concreto que ha estado activo.