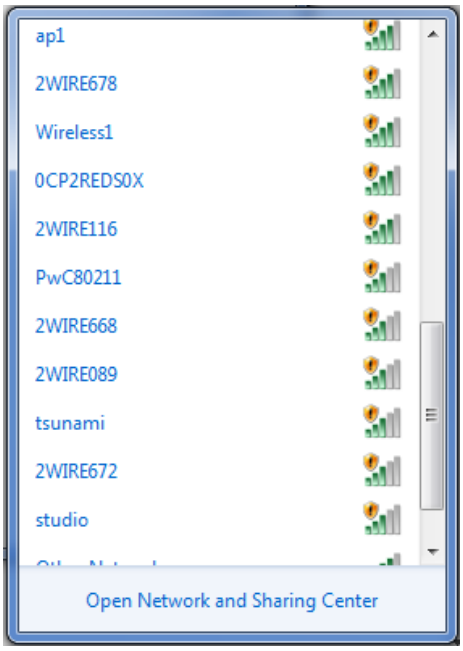
FuzzAP: una herramienta para ofuscar redes inalámbricas

Publicado por Vicente Motos on miércoles, 28 de mayo de 2014 Etiquetas: fortificación , herramientas , python , wireless



FuzzAP es un script en Python que puede generar un montón de puntos de acceso (APs) falsos para "ocultar" redes inalámbricas. Es similar a otras herramientas como FakeAP o AirRaid pero no es tan dependiente de los drivers de hardware. En lugar de crear APs falsos reconfigurando las tarjetas de red inalámbricas lo que hace es utilizar directamente las tarjetas que soportan inyección de paquetes. Esto mejora la velocidad (no es necesario resetear el dispositivo de red) y permite utilizar un mayor número de modelos de tarjetas y drivers: rtl8187, ath5k, ath9k, la mayoría de ralink, etc... y en definitiva cualquier dispositivo que pueda funcionar en modo monitor vía airmon-ng.

La lista SSID utilizada fue obtenida de https://wigle.net/gps/gps/Stat y la lista de OUI de fabricantes fue parseada de http://standards.ieee.org/develop/regauth/oui/oui.txt (netgear, cisco, linksys, d-link, atheros, ralink, apple).

Requiere python 2.7, Scapy 2.2.0 y, como comentamos, tarjetas de red inalámbricas con drivers que soporten inyeccción de paquetes.

Para utilizarlo previamente hay que activar el modo monitor con airmon-ng (suite aircrack-ng):

```
airmon-ng start [interface]
```

FuzzAP.py requiere dos argumentos: el primero el interfaz a usar y el segundo el número de puntos de acceso falsos a generar:

```
python fuzzap.py [interface] [number of APs]
```

Proyecto GitHub: https://github.com/lostincynicism/FuzzAP