Dificultando ataques ARP-Spoofing y ARP-Poisoned

abril 27, 2011 adastra Deja un comentario Go to comments

ESTABLECER TABLAS ARP ESTATICAS PARA PROTEGERSE DE ENVENENAMIENTO.

Como se ha podido ver anteriormente, una de las técnicas utilizadas para realizar un ataque MITM consiste en engañar al AP y al objetivo para que el trafico pase por medio de un host determinado (normalmente la maquina del atacante) para evitar (o al menos dificultar) este tipo de ataques, pueden emplearse tablas ARP estáticas con el fin de que no puedan ser envenenadas.

En distribuciones basadas en Linux se puede ejecutar el comando *arp -a* para ver las IP y direcciones MAC asociadas a las conexiones de red, si vemos alguna dirección MAC repetida, algo no va bien… posiblemente se es victima u objetivo de un ataque. Por este motivo es recomendable establecer tablas ARP estáticas de la siguiente forma:

arp -s 192.68.1.1 64:68:0c:45:71:88

Sin embargo de esta forma el cambio no se hace permanente, para hacerlo permanente:

>nano /etc/arp.conf

64:68:0c:45:71:88 192.68.1.1

00:0d:9d:82:cc:69 192.68.1.33

Posteriormente:

>nano /etc/network/interfaces

Al final del fichero:

post-up /usr/sbin/arp -f /etc/arp.conf

Con lo anterior se especifica que después de que la interfaz de red se encuentre levantada, se ejecute el comando arp con el fichero donde se ha establecido la MAC y su correspondiente IP (por ejemplo el AP al que nos conectamos habitualmente)