

6. Problemes del servei

6.1. Atacs al funcionament de DHCP i conflictes d'adreces IP

Com tot servei de xarxa, el servidor DHCP és susceptible de patir atacs mal intencionats. L'atac més fàcil i clàssic és el DoS o de denegació de servei. Consisteix a inundar de peticions un servidor per tal de saturar-lo i bloquejar-ne el funcionament. Un client pot realitzar innumerables peticions DHCP discovery fingint que són clients diferents (emmaskarant la seva MAC) amb la intenció d'esgotar les adreces IP disponibles del servidor o simplement amb la intenció de sobrecarregar-lo amb tantes peticions que no done a l'abast a atendre-les o que ho faci lentament.

Un altre tipus d'atac consisteix a falsejar la informació que s'envia al client (DHCP Spoofing). Recordem que el client fa una sol·licitud d'IP en forma de difusió (broadcast) i la seva petició pot ser atesa per un o més servidors DHCP. Un dels servidors DHCP pot ser un atacant que intentarà proporcionar informació de configuració falsa al client. Per exemple indicant un servidor DNS també maliciós. Aquest pot falsejar les identitats de les màquines de la xarxa i, quan el client s'adreça a la seva entitat bancària, el servidor DNS en realitat li ha proporcionat una IP d'una màquina que falseja la de l'entitat bancària. Perillós, veritat?

Per posar remei a la inseguretat en la comunicació client-servidor DHCP, el protocol permet utilitzar mecanismes d'autenticació i xifratge. Aquests mecanismes queden fora de l'abast d'aquesta explicació.

Esquema de funcionament del DHCP Spoofing:

