Defensa contra l'"ARP Spoofing"

L'enverinament ARP és conseqüència del propi disseny del protocol, així que l'únic mètode per evitar-ho realment és, de forma preventiva, fent fixes les entrades a la taula ARP de les potencials víctimes (especialment aquella referent a la porta d'enllaç, que és la que se sol falsificar). Això s'aconsegueix executant aquesta comanda en cadascuna d'elles (on se suposa que la IP i MAC indicades és la de la seva porta d'enllaç): *sudo ip neigh add 192.168.12.10 lladdr 00:ab:cd:ef:12:10*

> NOTA: Cal tenir en compte, però, que per protegir-nos completament, la porta d'enllaç també hauria de tenir una taula ARP amb l'associació fixa de totes les IPs de les màquines de la xarxa. Aquest fet, que ja de per sí és complicat degut a la variabilitat del parc informàtic que hi podria haver en la LAN en qüestió, es torna impossible si aquestes màquines adquireixen la seva adreça IP via DHCP (és a dir, dinàmicament)
> NOTA: Si volem eliminar una entrada fixa, caldrà executar una comanda com *sudo ip neigh del 192.168.12.10 dev eth0*
> NOTA: Una solució molt més radical que la indicada seria restringir tot el tràfic d'entrada a una màquina potencialment víctima per a què només s'acceptés el provinent de la porta d'enllaç (identificada per la seva MAC real). Això es pot aconseguir amb una regla de tallafocs com aquesta: *sudo nft add rule filter input iif eth0 ether saddr != 00:ab:cd:ef:12:10* Això provocaria, no obstant, que aquesta màquina només pogués accedir a Internet però no es pogués comunicar amb cap altra màquina de la seva xarxa.

Si no implementem el mètode anterior per evitar els atacs "ARP Spoofing" (a la pràctica pot ser poc realista), encara podem tenir la possibilitat, si més no, de detectar-los. La manera més eficient i "professional" de detectar aquests tipus d'atacs (i molts d'altres!) és utilitzar algun dels anomenat **NIDS** ("Network Intruder Detection System"), els quals són programes molt complets que es dediquen a detectar diferents tipus de comportaments "estranys" (és a dir, possiblement sospitosos) a la xarxa a partir de determinades regles predefinides que comparen amb les característiques dels fluxes dels paquets detectats i dels paquets individuals en sí). Concretament, en aquest cas s'emprarien per detectar respostes ARP no associades a cap petició prèvia (és a dir, paquets "gratuitous ARP", freqüentment símptoma d'un atac "ARP-Spoofing).

> NOTA: Aquesta funcionalitat NIDS (o part d'ella) es pot implementar directament dins dels routers. En el cas dels productes Cisco, per exemple, la possibilitat de detectar atacs "ARP Spoofing" es gestiona mitjançant una funcionalitat anomenada "DAI" ("Dynamic ARP Inspection"). Aquesta funcionalitat consisteix bàsicament en no reenviar paquets "gratuitous ARP" (és a dir, respostes ARP sense cap petició ARP prèvia reconeguda) a altres ports del router sota la mateixa VLAN (a més de registrar l'incident)
> NOTA: Els sistemes NIDS els estudiarem en un altre moment però podem mencionar com a exemples més representatius (n'hi ha molts més) els següents:
>
> **Suricata** (https://suricata-ids.org)
> **Snort** (https://www.snort.org)
> **Zeek** (https://zeek.org)

Si a la nostra infraestructura no podem disposar, no obstant, de cap solució NIDS, encara podem implementar altres solucions no tan sofisticades. Per exemple, el **Wireshark** sol ser capaç de detectar peticions ARP que obtinguin dues respostes diferents (amb la mateixa IP però MACs diferents) amb el missatge "*duplicate use of 192.168.1.11 detect!*"; (si no fos així sempre es pot buscar al tràfic de tipus ARP "a mà" -recordeu que filtres útils són, per exemple, *arp.opcode==1* per mostrar només les peticions o *arp.opcode==2* per mostrar només les respostes-) respostes que no es corresponguin a cap petició prèvia, etc.

També cal saber que es poden utilitzar eines especialitzades en detectar (i si pot ser, contrarestar) atacs "ARP Spoofing" específicament. Aquestes eines solen dedicar-se a observar canvis en l'associació MAC<->IP dels hosts de la xarxa (principalment de la porta d'enllaç), notificant-los en el cas de que es produïssin (a través de missatges de log, enviament de correus, etc). Algunes d'aquestes eines són **ArpOn** (http://arpon.sourceforge.net) , la més completa; **ArpWatch** (https://ee.lbl.gov) , molt antiga però funciona o **Addrwatch** (https://github.com/fln/addrwatch) , versió més moderna de l'anterior.