Atac "DHCP Starvation"

L'objectiu de l'atac "ARP Spoofing" és, en definitiva, fer-se passar per la porta d'enllaç de la víctima per tal que tot el tràfic dirigit a Internet travessi l'ordinador de l'atacant (i aquest pugui, doncs, inspeccionar-lo i/o manipular-lo com consideri). Però existeixen altres mètodes per aconseguir el mateix objectiu de fer-se passar per la porta d'enllaç de la víctima, i un d'aquests altres mètodes és l'atac anomenat "DHCP Starvation".

Aquest atac consisteix en realitzar els següents passos des de la màquina atacant:

1) Demanar una adreça IP al servidor DHCP legítim de la xarxa local
2) Canviar-se l'adreça MAC i tornar a demanar una altra adreça IP al mateix servidor DHCP. Aquest servidor considerarà que la petició prové d'un altre client perquè la MAC d'origen és diferent, així que li donarà una nova IP.
3) Repetir el pas anterior fins que la "borsa" d'adreces IP oferides pel servidor d'esgoti
4) Un cop ja el servidor DHCP legítim estigui "fora d'ús" (en un clar exemple d'atac "DoS"), ja no tindrem "competència" per posar en marxa llavors un servidor DHCP propi que ofereixi dades malicioses a les noves víctimes "en exclusiva" (per això se sol anomenar "Rogue DHCP Server"), com per exemple, i sobre tot, una porta d'enllaç (i/o uns servidors DNS) que estiguin sota el control de l'atacant A partir d'aquí, ja tindríem el mateix escenari que vam veure amb l'atac "ARP Spoofing"

NOTA: Es podria implementar directament el pas 4) però llavors la probabilitat d'èxit seria petita perquè recordeu que els servidors DHCP competeixen per oferir als clients els seus prèstecs, així que és probable que mantenint el servidor DHCP legítim en marxa molts clients no arribessin a "caure en la xarxa" del nostre servidor DHCP maliciós.

Existeixen comandes que específicament realitzen aquest atac, com per exemple **DHCPig** (https://github.com/kamorin/DHCPig) o bé mòduls concrets d'aplicacions més grans que inclouen suites d'atacs diferents, com per exemple el mòdul "**dhcp_exhaustion**" del framework Metasploit, que estudiarem aviat (https://digi.ninja/metasploit/dns_dhcp.php) o l'eina **Yersinia** (https://github.com/tomac/yersinia) , entre altres. També es poden trobar codis desenvolupats "ad-hoc" amb la llibreria especialitzada **Scapy** (https://scapy.net)

Una forma d'evitar aquest atac és configurar els "switchos" de la xarxa local amb una funcionalitat, que fins i tot els de gama baixa incorporen anomenada "DHCP Snooping". Aquesta funcionalitat consisteix en garantir que només els servidors DHCP legítims puguin proporcionar informació de configuració a la xarxa; per aconseguir això, a la configuració del "switch" es marquen com a "segurs" els ports on esta/n connectat/s el servidor/s legítim/s, de manera que qualsevol dispositiu que intenti unir-se a la xarxa a través d'un altre port es considerarà insegur. D'aquesta manera, si en algun d'aquests dispositius connectats a un port "insegur" s'executés un servidor DHCP, quan algun paquet DHCP dels que només pot enviar un servidor (DHCPOFFER, DHCPACK, DHCPMAK...) arribés al port "insegur", el switch bloquejaria el seu reenviament i, per tant, els clients no rebrien cap informació maliciosa.

NOTA: És cert que un servidor DHCP no autoritzat podrà seguir rebent paquets DHCPDISCOVER (és a dir, les sol·licituds dels clients), ja que són de tipus "broadcast", i també podrà seguir enviant paquets DHCPOFFER (la resposta a la sol·licitud), però aquesta no arribarà a cap client perquè s'haurà detectat que el paquet no prové d'un servidor de confiança