MitM mitjançant l'atac "ARP Spoofing"

Introducció: què és MitM

El "Man-in-the-middle" (o MitM) és un atac LAN genèric on un sistema atacant vigila secretament la comunicació que es produeix entre dos extrems "posant-se al mig", mentre els extrems no se n'adonen de cap amenaça externa. Concretament, en un atac MitM, cada extrem és enganyat per l'atacant per tal de què pensi que està connectant-se a l'altre extrem i viceversa quan en realitat tots dos extrems s'estan connectant a l'atacant (el qual reenviarà el tràfic de la forma adient per a què, un cop processat/inspeccionat/manipulat, aquest tràfic arribi finalment al destí original i així ningú "noti res").

En un atac MitM l'atacant controla completament la connexió, de manera que a més d'interceptar la comunicació (i visualitzar/emmagatzemar de tota la informació que passa entre les màquines orígen i destí), fins i tot podria alterar els paquets transferits des d'una banda o des de l'altra. Així doncs, en resum: un atacant de MitM actua com un servidor intermediari (un "proxy") "invisible" entre dues parts on és capaç de robar o canviar qualsevol tipus de dades transferides entre elles sense ser descobert. Depenent del nivell en la pila TCP/IP on treballi i els protocols concrets implementats, en trobarem amb diferents tipus de "proxies invisibles" que serviran per aconseguir diferents objectius.

Els atacs MitM són un pas previ necessari a qualsevol altre atac més concret perquè, en una arquitectura LAN actual, totes les màquines estan connectats a un commutador a través del seu propi port ("boca"), el qual es troba aïllat de la resta. És a dir, un switch envia el trànsit destinat a una determinada màquina només a través de la boca corresponent (un cop ja té la taula MAC<->boca emplenada, procés que és molt ràpid) i cap més (de fet, per això es diuen "conmutadors"). Per tant, de manera predeterminada, un atacant no pot espiar el trànsit enviat a un altre host diferent a ell a no ser que primer realitzi un atac MitM per suplantar-lo.

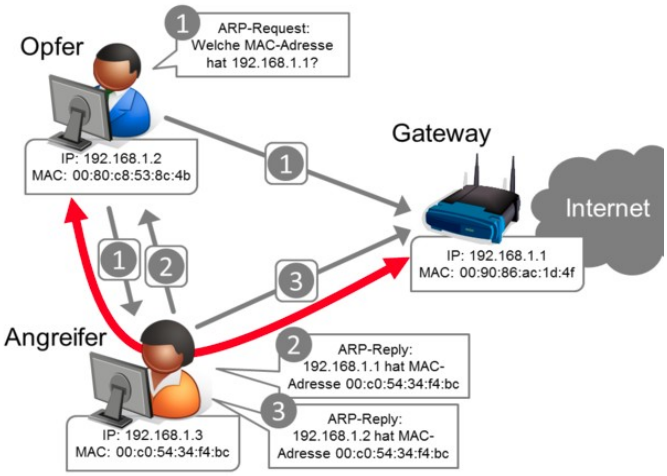
En aquest sentit, per poder espiar el trànsit dirigit a un determinat servidor provinent de múltiples clients de la LAN (i rebre, doncs, les sol·licituds dels clients, passar-les al servidor i reenviar les respostes del servidor als remitents originals) en teoria l'atacant hauria d'enganyar a tots els clients fent-los creure que el servidor és ell i enganyar el servidor fent que cregui que tots els clients són ell també. A la pràctica, com que la majoria de vegades el/s servidor/s més interessants a suplantar es troba/en a Internet, el que els atacants fan més sovint és posar-se entre els clients LAN i la seva porta d'enllaç (és a dir, fer creure als clients que l'atacant és la seva porta d'enllaç i fer creure a la porta d'enllaç que l'atacant són els diferents clients): d'aquesta manera, l'atacant podrà interceptar tot el trànsit de la LAN que es dirigeix a Internet (i el que prové d'allà).

NOTA: En aquest sentit, l'ús de "Rogue APs" en xarxes WiFi és un atac MitM bastant comú exclusiu d'aquests entorns

Tècnica "ARP Spoofing"

La tècnica més comuna usada per implementar un atac MitM en xarxes LAN és l'anomenada "ARP Spoofing" (o, a vegades, "ARP Poisoning"). Aquesta tècnica, a grans trets, consisteix en enverinar la catxé ARP d'un client de la xarxa LAN per fer-li creure que la direcció MAC de la seva porta d'enllaç és la direcció MAC de l'equip atacant, podent d'aquesta manera situar la màquina de l'atacant en mig de les comunicacions efectuades entre l'equip víctima i la porta d'enllaç legítima.

Per realitzar l'atac "ARP Spoofing", l'atacant tria una màquina client "objectiu" (també podrien ser totes les de la LAN) i li comença a enviar de forma periòdica paquets ARP de resposta falsa que contenen l'adreça MAC de l'atacant lligada a l'adreça IP de la porta d'enllaç legítima de la xarxa; paral·lelament, l'atacant també envia paquets ARP de resposta falsa a la porta d'enllaç legítima que contenen l'adreça MAC de l'atacant lligada a la IP del client atacat. D'aquesta manera s'estarà "enverinant" la catxé ARP d'ambdós extrems associant les IPs respectives a una MAC que no és la real de l'altre extrem sinó que és la de la màquina atacant. Com a conseqüència, quan qualsevol dels dos extrems envïin paquets a l'altre, aquests paquets es dirigiran a l'atacant. Per a què ningú noti res, un cop s'hagin processat de la forma necessària, l'atacant tindrà la feina extra de redirigir els paquets al seu destí legítim. Aquesta figura il·lustra el procés:



NOTA: Com es veu a la il.lustració anterior, l'atacant pot optar per inspeccionar (espiar) els paquets (alhora que reenvia el trànsit a la passarel·la predeterminada real per evitar el descobriment), i/o modificar les dades abans de reenviar-les o fins i tot llançar un atac de denegació del servei que provoqui que alguns (o tots) els paquets de la xarxa no puguin arribar al seu destí legítim (tallant a la pràctica la comunicació)

Tècnica "ARP Flooding"

Hi ha una altra tècnica anomenada "ARP Flooding" (o, a vegades, "MAC Flooding"), molt més agressiva que l'"ARP Spoofing", que consisteix en un enviament massiu de moltes respostes ARP aleatòries falses al switch. Aquest atac desborda la memòria interna (volàtil) on hi ha emmagatzemada la taula MAC<->boca (l'anomenada "**taula CAM**", de "Content-Addressable Memory"), la qual associa cada boca amb la direcció MAC de la màquina particular que s'hi troba connectada. Aquest desbordament fa, en alguns models de switch, que aquesta taula deixi de ser utilitzada, provocant que el switch ja no pugui saber quin client està endollat a cada port, fet que deixa el switch sense més remei que reenviar tots els paquets a totes les boques (com ho faria un "hub"). Això es coneix com a estat d'"obertura fallida" i, en aquest escenari, l'atacant podria interceptar totes les connexions LAN. Això també fa, de retruc, que el rendiment de la xarxa pateixi molt, cosa que podrien notar altres usuaris de la xarxa.

NOTA: Si el commutador no cau en estat d'"obertura fallida", l'única altra opció és que caigui en un estat de "tancada fallida" on totes les boques deixen de funcionar. En aquest cas, cap trànsit de xarxa no arribarà a cap host de la LAN i, per tant, estarem parlant d'un atac de denegació de servei ("DoS")

Una altra explicació del "ARP Flooding" més exhaustiva és la següent: és un atac consistent en l'enviament de múltiples trames falsificades a través d'una boca amb l'objectiu d'omplir la taula d'assignació de l'switch. Generalment un switch disposa d'una memòria interna anomenada CAM on assigna boques ("ports") a adreces MAC. Quan una trama arriba a un port, la CAM afegeix una entrada a la taula especificant la MAC de l'equip que va enviar la trama juntament amb el port en què es troba. D'aquesta manera, quan el switch rep una trama dirigida a aquest equip sabrà per quin port ha de enviar-la. En cas de desconèixer la destinació de la trama, bé perquè l'equip no ha arribat a generar trànsit o bé perquè l'entrada associada a aquest equip ha expirat, el switch copiarà la trama i l'enviarà per tots els ports de la mateixa VLAN excepte per aquell pel qual va ser rebuda. D'aquesta manera, tots els equips connectats al switch rebran aquesta trama i únicament l'equip corresponent (aquell la MAC del qual coincideixi amb la MAC destinació de la trama) contestarà; això permetrà al switch afegir una entrada al seu taula CAM amb la nova associació MAC/port. Gràcies a això, el switch no necessitarà inundar ("flood") tots els ports amb futurs paquets dirigits a aquest equip. Però, què passaria si s'envien centenars de trames falsificant la MAC origen de l'equip i omplint la taula CAM? En aquest cas, el seu comportament depèn de fabricant. Els switchos de baixa gamma no contenen taules CAM virtualitzades, és a dir, que si la taula disposa d'un nombre *n* màxim d'entrades per emmagatzemar les associacions MAC/port, i un equip aconsegueix omplir aquesta taula amb *n* entrades, la taula s'omplirà i totes les VLANs es veuran afectades. Amb taules CAM virtualitzades es mantindria un espai d'adreces independent per a cada VLAN (d'aquesta forma, només es veurien afectats els equips de la pròpia VLAN).

Eines

***Dsniff** (http://www.monkey.org/~dugsong/dsniff): Històrica suite de comandes especialitzades en atacs MitM, una de les quals, *arpspoof*, està específicament dissenyada per realitzar "ARP Spoofing" i una altra, *macof*, per realitzar "ARP Flooding". No obstant, la seva darrera actualització és de fa més de 15 anys

***Ettercap** (http://www.ettercap-project.org) : Històric programa, tant de terminal com gràfic, especialitzat en atacs MitM de varis tipus, incloent l'"ARP Spoofing". No obstant, la seva darrera actualització és de fa més de 10 anys.

***Bettercap** (https://www.bettercap.org): Programa millorat de l'anterior, més actual i complet

***Scapy** (https://scapy.net): Llibreria Python que permet desenvolupar scripts propis capaços de generar i interaccionar amb paquets de xarxa com ho desitgem. Concretament es pot utilitzar per implementar un atac d'"ARP Spoofing" sense massa dificultat.

***Nping** (https://nmap.org/nping) : Comanda que permet generar (i enviar) paquets "ad-hoc" amb les característiques desitjades. També es pot utilitzar per implementar un atac d'"ARP Spoofing" sense massa dificultat.