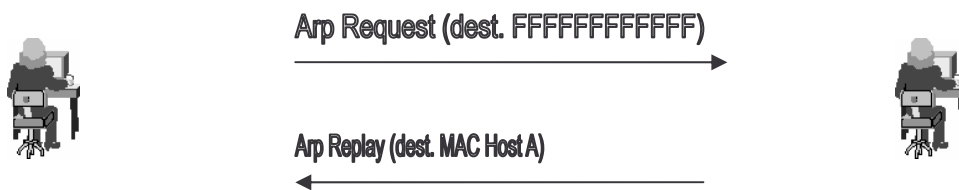


Arp Poison Routing (Man in the middle Attack) Copyright © 2005 Luca Sciortino

Quando l'host A nella rete vuole scambiare un pacchetto con l'host B deve conoscere il suo MAC Address per poter comunicare. L'host A chiederà il MAC Address dell'host B con una richiesta ARP di broadcast (ARP Request FFFFFFFF). Solo la macchina che avrà quello specifico IP Address risponderà a questa richiesta con un pacchetto di ARP Replay direttamente all'host A. A questo punto l'host A manderà un pacchetto IP con destinazione IP dell'host B usando il suo MAC Address come indirizzo di destinazione nel frame ethernet. Il pacchetto di ARP Request è inviato solo se l'host A non conosce il MAC Address dell'host B. Una volta che l'host A conoscerà il MAC Address dell'host B utilizzerà la tabella di cache dell'ARP.

Esempio (l'host A vuole colloquiare con l'host B)



- 1) Host A controlla se nella sua cache è presente un'associazione tra MAC B /IP B e se esiste usa quella.
- 2) Host A > Arp Request : Qual è il MAC Address associato all' IP B ?
- 3) Host B < Arp Replay : Il mio MAC Address è MAC B ed il mio IP è IP B.
- 4) Host A : Ok aggiorno la mia cache ARP e mando i pacchetti a IP B usando MAC B.

Lo switch di rete costruisce una propria tabella interna ed estrae il MAC Address dal frame ethernet per ogni pacchetto processato. Se non esiste una entry nella route table lo switch forwarderà il pacchetto su tutte le sue porte.

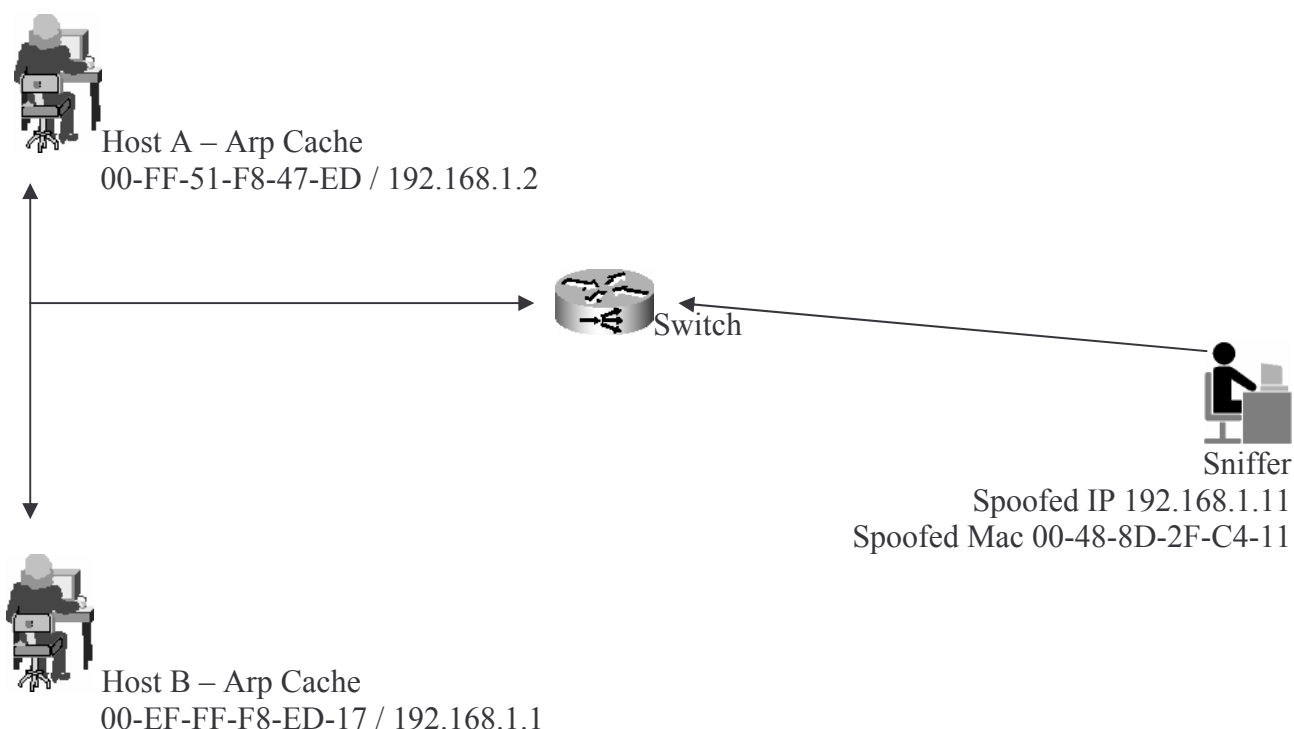
Switch Route Table

Port	Mac Address
5	00-FF-51-F8-47-ED
6	00-EF-FF-F8-ED-17

Di solito è impossibile visualizzare il traffico tra due host collegati ad uno switch proprio per la conformazione di cui sopra. Lo switch dirigerà il traffico dall'host A all'host B rispettando i MAC Address nella propria Switch Route Table.

Se nello switch non è effettivamente presente un port mirroring dove redirigere tutto il traffico un eventuale sniffer di rete potrà catturare solo il traffico unicast da e verso se stesso ed anche il traffico di broadcast / multicast traffic.

Come detto sopra, se non esiste una entry nella route table lo switch forwarderà il pacchetto su tutte le sue porte così, per un attaccante con una scheda in modalità promiscua non sarà difficile conoscere tutte le entry nello switch. Questo è un prerequisite essenziale per il funzionamento di un attacco di tipo Man in the middle.



Manipolando la cache dei due host (ARP Poisoning) è possibile cambiare la direzione del traffico tra di loro.

Il protocollo ARP è di tipo stateless non richiede nessun tipo di autenticazione, così inviando un semplice pacchetto di ARP-Replay ad entrambi gli host si forzerà l'update della loro ARP cache. Il pacchetto di poison dice all'host A che può trovare l'IP dell'host B al MAC ADDRESS 00-48-8D-2F-C4-11. Allo stesso modo un altro pacchetto di poison dice all'host B che può trovare l'IP dell'host A al MAC ADDRESS 00-48-8D-2F-C4-11. A questo punto delle cose il flusso della comunicazione tra l'host A e l'host B potranno essere intercettate da un terzo incomodo con a disposizione uno sniffer di rete bypassando tutti i controlli di sicurezza dello switch.

Il traffico tra l'host A e l'host B è stato appena redirezionato verso lo sniffer cui compito è quello di ruotare i tutti i pacchetti verso la vera destinazione ovviamente in entrambe le direzioni.

Se la macchina su cui gira lo sniffer non avrà attivato l'ip_forward entrambi gli host non riusciranno più a comunicare, si causerà in questo modo un attacco di tipo denial of service (DOS).

Se non esiste traffico tra i due host dopo un periodo di timeout l'ARP cache di entrambi sarà svuotata ed è per questo motivo che ad intervalli regolari si continuerà a posizionare pacchetti spoofati su entrambi gli host.

Alcune considerazioni da fare sono :

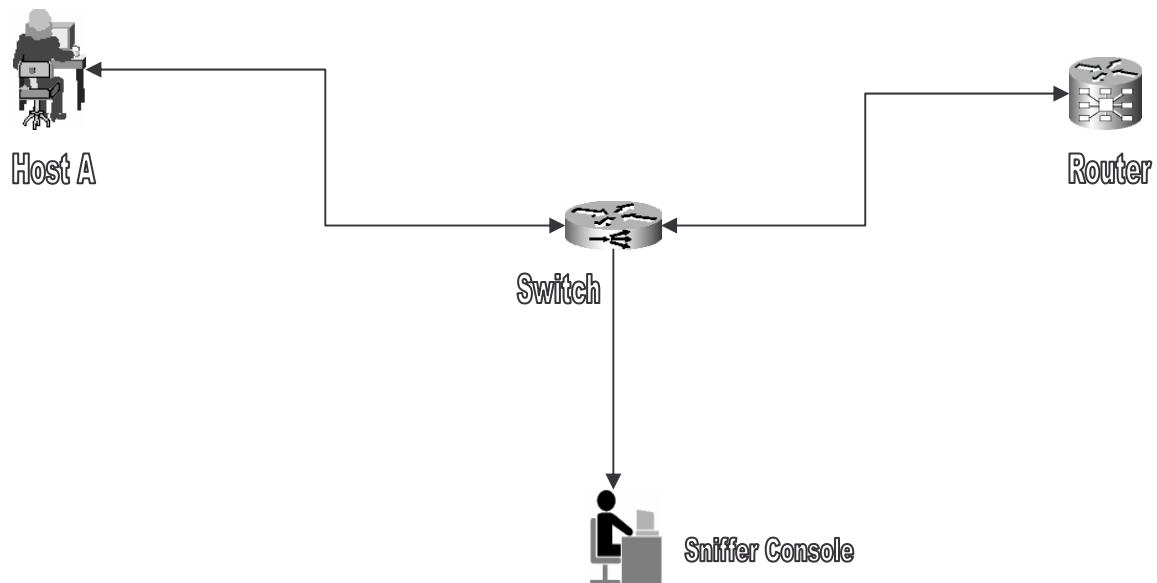
- 1) L'ARP Poisoning lavorerà solo all'interno del Broadcast Domain infatti è impossibile redirigere il traffico tra hosts su diverse subnets o VLAN.
- 2) Lo sniffer console deve essere in grado di ruotare i pacchetti alla destinazione corretta, in caso contrario si avrà un attacco di tipo DOS e gli hosts non saranno più in grado di comunicare.
- 3) Si otterrà un degrado delle prestazioni della rete in quanto buona parte del traffico passerà attraverso una scheda in modalità promiscua.

Guardiamo questa situazione e supponiamo ora che per raggiungere un host su una rete esterna l'host A invia i pacchetti generati al proprio default gateway (Router).

Il Router provvede a ruotare i pacchetti al prossimo hop fino a raggiungere la destinazione.

Quando il Router riceverà i pacchetti di ritorno provvederà a ruotarli sull'interfaccia corretta e finalmente sull'host A.

Consideriamo che momentaneamente ci siano 2 end point, uno in ingresso ed uno in uscita, lo Switch considererà il Router come un vero e proprio host sulla rete.



Come detto in precedenza non possiamo istruire un host di una LAN esterna a mandare i pacchetti sulla nostra sniffer console, tuttavia possiamo redirezionare tutto il traffico che passa tra l'host A ed il Router utilizzando l'ARP Poisoning.

In questa situazione dobbiamo fare alcune considerazioni :

- 1) La LAN esterna menzionata sopra potrebbe essere INTERNET così la sniffer console che ha il compito di riroutare i pacchetti non sarà di tipo host to host ma bensì host to all. Ci saranno dei grossi problemi di performance.
- 2) La sniffer console non è a conoscenza del gateway dell'host A e non sa se è veramente un router. I pacchetti che provengono dall'host A destinati alla sniffer console potrebbero contenere un indirizzo IP di destinazione nell' header IP differenti comunque dall'indirizzo IP del Router. Questo problema può essere risolto in 2 modi : Le tabelle di routing / Il broadcast.
- 3) Nella LAN ci potrebbero essere diversi percorsi ad esempio un host e 2 Routers.

Usando la tecnica del ARP Poison Routing è possibile manipolare il flusso del traffico IP tra gli host di una LAN.

Una volta ottenuto l'accesso alla macchina della subnet un intruso può utilizzare questa tipologia di attacco (Hijacking) per catturare password, effettuare attacchi DOS, fare il discovery della LAN ed impersonare ogni host nella rete.