LAN Sniffing con Ettercap

In questa rubrica non ci siamo occupati molto dei problemi di sicurezza delle reti locali, le LAN, un po' perché sono fin troppo discussi ed un po' perché rendere ragionevolmente sicura una LAN aziendale è quasi impossibile. In una LAN più che in altri punti del networking, vi è uno scontro diretto tra sicurezza e fruibilità e per ragioni note a tutti è quasi sempre la sicurezza a venire tralasciata. Uno degli argomenti che vengono proposti spesso come scusa per ignorare i problemi di sicurezza delle LAN è che con l'avvento degli switch solo il traffico destinato ad un particolare elaboratore viene instradato sul cavo connesso a quell'elaboratore, mentre precedentemente con gli hub, tutto il traffico presente in rete veniva instradato a tutti gli elaboratori. Questa affermazione è vera in condizioni di traffico normali, ma è facilmente aggirabile, al punto che vi sono anche tool automatici per farlo. In questo articolo utilizzeremo Ettercap, tra l'altro un prodotto italiano, per dare un esempio di come sia semplice sovvertire una switched LAN nella quale non si siano prese adeguate misure di sicurezza.

Arp Spoofing

La principale tecnica per attacchi in switched ethernet LAN è l'Arp Spoofing. Per comprenderlo dobbiamo ricordare alcuni dettagli del protocollo ethernet. I pacchetti IP sono incapsulati in frame ethernet ed inviati dalla scheda di rete sui cavi. Ogni frame ethernet è inviata ad un indirizzo, detto MAC address, di un'altra scheda ethernet sulla stessa LAN. Uno switch si ricorda i MAC address delle schede di rete connesse ad ognuna delle sue porte ed invia solo i pacchetti destinati ad ognuna di esse attraverso la relativa porta. E' necessario perciò associare agli indirizzi IP delle macchine sulla rete locale i MAC address delle relative schede di rete. Ogni elaboratore mantiene una tabella detta *Arp Table* con la relativa traduzione. Di norma quando si accende una macchina questa tavola è vuota, quando poi un elaboratore deve contattare un'altra macchina di cui conosce il numero IP ma non il MAC address, invia a tutte le macchine sulla LAN una *arp-request* (in broadcast) per il numero IP che conosce. La macchina che ha tale numero IP risponde con il proprio MAC address. Per velocizzare il riempimento delle tavole Arp, spesso all'avvio un elaboratore invia a tutte le macchine un *unsolicited-arp* con il quale informa tutte le macchine del proprio numero IP e MAC address. Un elaboratore che riceve una informazione Arp per un indirizzo IP per il quale ha già il MAC address nella tavola Arp, sostituisce il vecchio MAC con il nuovo a meno che l'amministratore non abbia specificatamente marcato il MAC address nella tavola come immutabile. Questo comportamento del protocollo Arp permette in condizioni *normali* di sostituire schede ethernet, cambiare indirizzi IP ecc. senza doversi curare di quello che

succede a livello ethernet. Da questo punto di vista possiamo dire che la LAN ethernet a livello 2 della pila ISO/OSI si auto-configura.

Questa semplicità può essere però sfruttata per un semplice attacco man-in-the-middle.

L'attacco

Supponiamo di avere due macchine che si devono parlare, *host* 192.168.12.66 e *GateWay* 192.168.12.254, e l'attaccante *attack* 192.168.12.193. L'attaccante utilizza ad esempio dei *unsolicited arp* per cambiare le tavole Arp delle due macchine sotto attacco mettendo in queste il proprio indirizzo MAC al posto di quello del relativo corrispondente. In tabella 1 riportiamo la situazione prima dell'attacco su tre macchine con SO Linux prese come esempio.[1] Utilizzando ettercap su 192.168.12.193, l'attacco è molto semplice, basta dare il comando

```
ettercap -a 192.168.12.66 192.168.12.254
```

l'opzione -a indica di effettuare un attacco di *sniffing* basato sulla manipolazione delle tavole Arp delle due macchine indicate nella linea di comando. Dopo aver dato questo comando, le tavole Arp su *host* e *GateWay* sono modificate come riportato in Tabella 2. Il significato di queste tabelle è molto semplice, sia *host* che *GateWay* associano all'indirizzo IP dell'altro il MAC address di *attack* e perciò inviano ad *attack* tutti i pacchetti destinati all'altro. In condizioni normali, quando *attack* riceve dei pacchetti a livello ethernet per un numero IP non proprio, li scarta. Invece in un attacco *mitm*, quando *attack* riceve i pacchetti in transito tra *host* e *GateWay*, ne fa una copia, li modifica se vuole, e poi li invia al legittimo destinatario che non si accorge di nulla. Ettercap rende tutto questo procedimento semplice da implementare con il solo comando indicato, ma questo tipo di attacchi è ben noto e facilmente implementabile in molti altri modi e con molti altri tool.

Per verificare il successo dell'attacco, ci colleghiamo ad *host* e scarichiamo una pagina web tramite *GateWay*. In realtà il traffico passa attraverso *attack,* ed infatti le figure 1, 2, e 3 mostrano cosa viene registrato da Ettercap su *attack:* tutto il traffico!

Contromisure

Possiamo ora provare a prendere delle contromisure. Ad esempio su *GateWay* blocchiamo la tavola Arp in modo che *attack* non possa cambiarla dando il comando:

```
arp -s 192.168.12.66 00:00:B4:C7:14:7B
```

in questo modo assegnamo staticamente al numero IP 192.168.12.66 il MAC address 00:00:B4:C7:14:7B ed Arp non può più cambiare questa assegnazione. Nella tabella 3 è riportata la nuova Arp Table su *GateWay*, il flag M indica che la relativa riga non può essere modificata dinamicamente ma solo dall'amministratore del sistema manualmente. Provando ancora a scaricare

1 Nulla cambia, a parte il formato dell'output nelle tabelle, su altri SO.

una pagina web su *host*, dalle figure 4 e 5 si nota come Ettercap rileva solo il traffico da *host* verso *GateWay* ma correttamente non vede il traffico da *GateWay* verso *host*.

Questo esempio ci indica quali possibili azioni possiamo adottare per proteggerci da questi tipi di attacchi. Fondamentalmente bisogna bloccare le righe di interesse delle tavole Arp. Questo si può fare, a secondo del caso, a livello del singolo host, o dei server, dei gateway, ed anche sugli switch; si può inoltre dividere il traffico sulla LAN introducendo le VLAN ecc. Il problema principale è quello della gestione degli indirizzi MAC: distribuire e tenere aggiornate su tutte o parte delle macchine tavole Arp parziali o complete è un grande lavoro che non si sposa per nulla con le odierne richieste di dinamicità, dai portatili alle W-LAN, delle reti aziendali.

Andrea Pasquinucci
Libero Professionista in Sicurezza Informatica
pasquinucci@ucci.it

Riferimenti Bibliografici

[1] Ethernet RFC-894, ARP RFC-826
[2] http://ettercap.sourceforge.net/

```
host# ifconfig
eth0 Link encap:Ethernet  HWaddr 00:00:B4:C7:14:7B
 inet addr:192.168.12.66   Bcast:192.168.12.255  Mask:255.255.255.0

host# arp -n
Address         HWtype  Hwaddress           Flags   Mask  Iface
192.168.12.254  ether   00:06:7B:02:6A:39   C             eth0
192.168.12.193  ether   00:50:BA:5D:C2:0F   C             eth0

----------

GW# ifconfig
eth0 Link encap:Ethernet  HWaddr 00:06:7B:02:6A:39
 inet addr:192.168.12.254 Bcast:192.168.12.255  Mask:255.255.255.0

GW# arp -n
Address        HWtype  HWaddress           Flags   Mask   Iface
192.168.12.66  ether   00:00:B4:C7:14:7B   C              eth0
192.168.12.193 ether   00:50:BA:5D:C2:0F   C              eth0

----------

attack# ifconfig
eth0 Link encap:Ethernet  HWaddr 00:50:BA:5D:C2:0F
inet addr:192.168.12.193  Bcast:192.168.12.255  Mask:255.255.255.0

attack# arp -n
Address        HWtype  HWaddress           Flags  Mask  Iface
192.168.12.66  ether   00:00:B4:C7:14:7B   C            eth0
192.168.12.254 ether   00:06:7B:02:6A:39   C            eth0
```

Tabella 1. Indirizzi IP, Mac Address e Arp Table prima dell'attacco

```
host# arp -n
Address         HWtype  Hwaddress           Flags   Mask  Iface
192.168.12.254  ether   00:50:BA:5D:C2:0F   C             eth0
192.168.12.193  ether   00:50:BA:5D:C2:0F   C             eth0

GW# arp -n
Address        HWtype  HWaddress           Flags   Mask   Iface
192.168.12.66  ether   00:50:BA:5D:C2:0F   C              eth0
192.168.12.193 ether   00:50:BA:5D:C2:0F   C              eth0
```

Tabella 2. Le Arp Table durante l'attacco

```
GW# arp -n
Address        HWtype  HWaddress           Flags   Mask   Iface
192.168.12.66  ether   00:00:B4:C7:14:7B   CM             eth0
192.168.12.193 ether   00:50:BA:5D:C2:0F   C              eth0
```

Tabella 3. La Arp Table di *GW* con il MAC di 192.168.12.66 bloccato

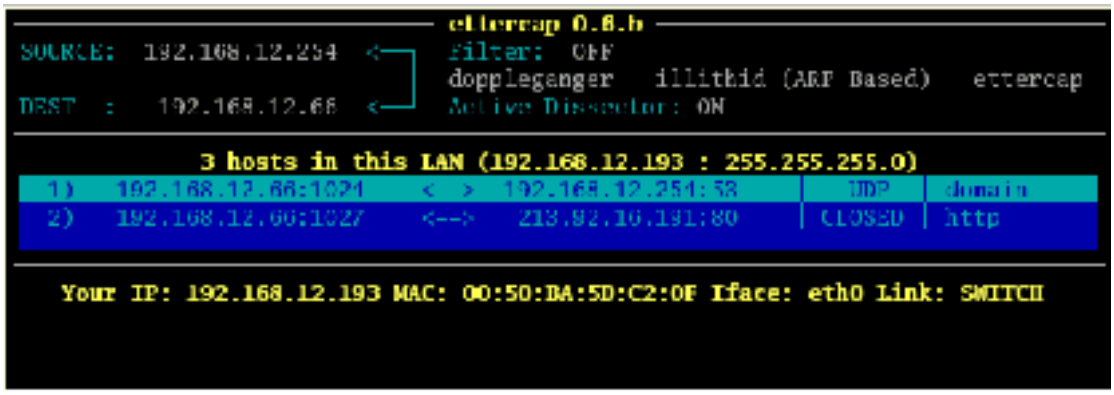

Figura 1. Le due connessioni (DNS e HTTP) per la richiesta di una pagina web

Figura 2. I dati intercettati per la connessione DNS

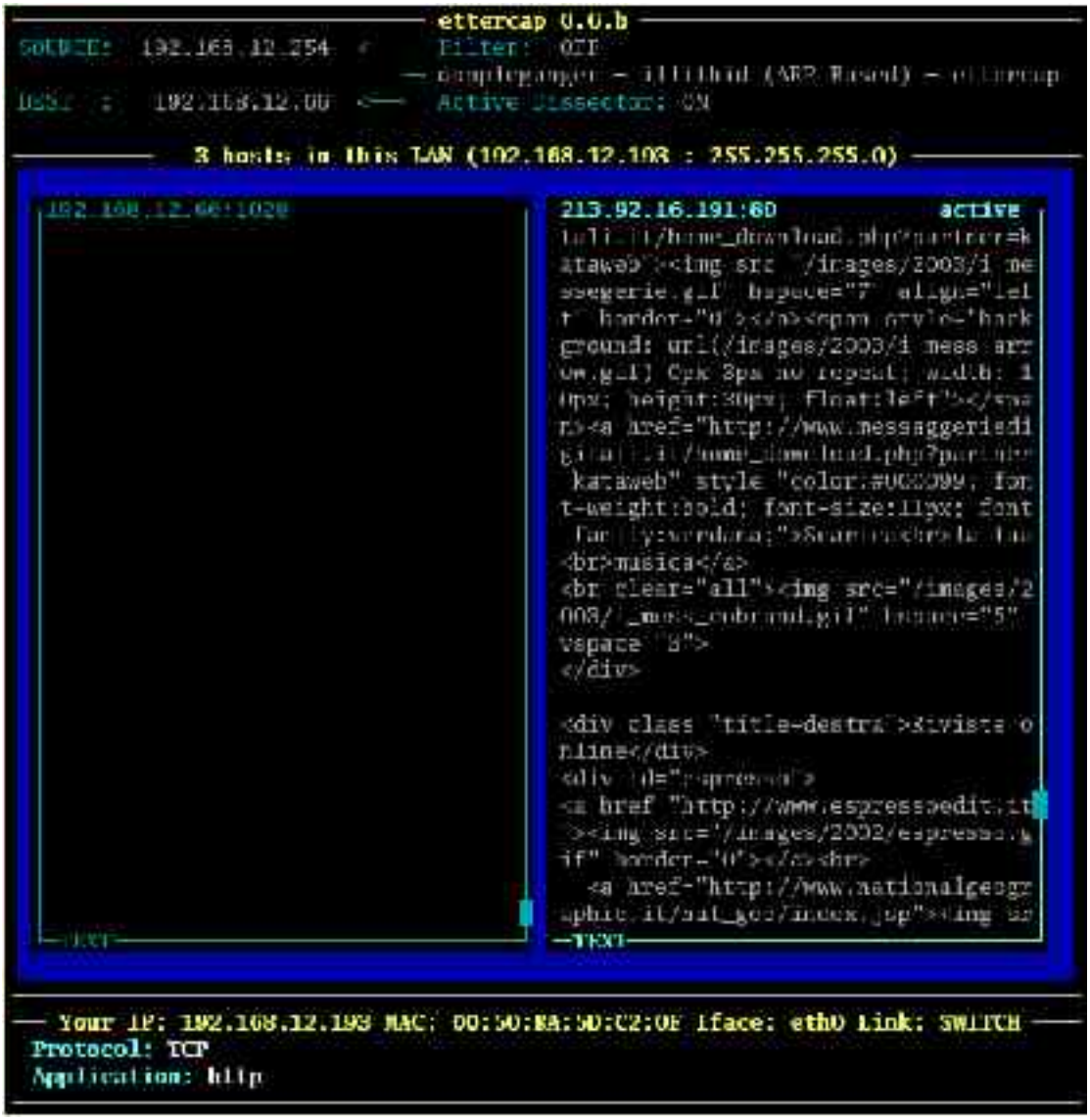

Figura 3. I dati intercettati per la connessione HTTP

Figura 4. La nuova richiesta di *host* rimane nello stato CLOSING poiché *attack* non vede i pacchetti di ritorno che chiudono del tutto la connessione

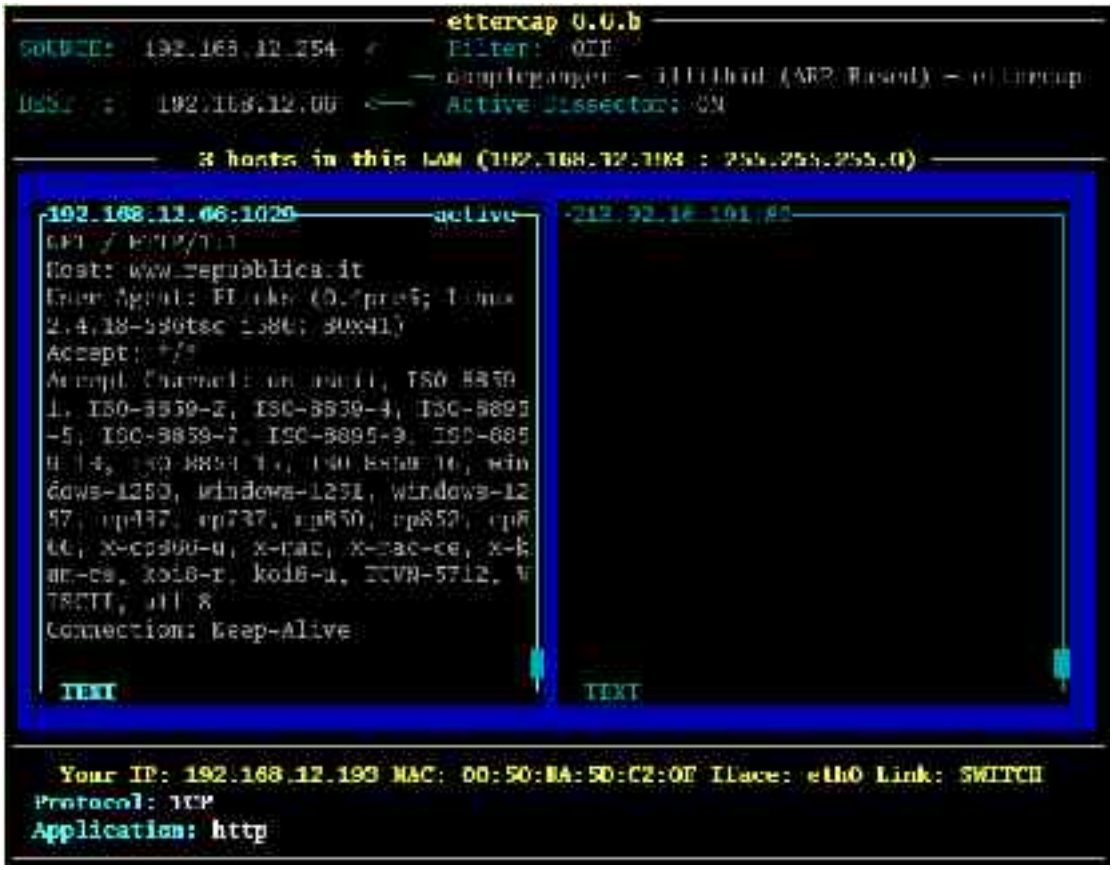

Figura 5. Ettercap rileva solo la richiesta da *host* ma non i pacchetti di ritorno con i dati della pagina web