Esercitazione di Laboratorio - NA01

Riccardo Persello

31 maggio 2021

Attivazione di Wirehark

Si verifica mendiante il comando `ifconfig` la configurazione di rete dell'host. Tra le molte interfacce indicate, si trova che quella attualmente in considerazione (scheda 802.11 a/b/g/n/ac/ax integrata nel computer portatile) corrisponde all'interfaccia `en0`.

```
riccardo@MBP-M1 ~ % ifconfig

...

en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether a0:78:17:83:57:03
    inet6 fe80::10b2:945:6846:62c4%en0 prefixlen 64 secured scopeid 0xc
    inet 172.20.10.7 netmask 0xfffffff0 broadcast 172.20.10.15
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active

...
...
...
~
```

L'indirizzo MAC dell'interfaccia è `A0:78:17:83:57:03`, mentre l'indirizzo IP corrisponde a `172.20.10.7`. Per trovare l'indirizzo del default gateway si ricorre ad un altro comando:

```
riccardo@MBP-M1 ~ % route get default

   route to: default
destination: default
       mask: default
    gateway: 172.20.10.1
```

```
  interface: en0
      flags: <UP,GATEWAY,DONE,STATIC,PRCLONING,GLOBAL>

...

~
```

Si scopre così che per `en0` il default gateway ha come indirizzo IP locale `172.20.10.1` (attualmente un telefono cellulare utilizzato come access point).

Analisi indirizzi MAC

Questa analisi è stata effettuata in precedenza, su una rete diversa da quella indicata nella prima parte di esercitazione. Si è scelto di usare una vecchia analisi in quanto il traffico singlecast sulla rete generata dal telefono cellulare come access point si è rivelato piuttosto scarno, essendo composto da soli due dispositivi.

Avviando una cattura con Wireshark (senza generare traffico di proposito) si notano comunque una moltitudine di pacchetti di vario tipo. Tutti i pacchetti riportano indirizzi MAC singlecast.

Si riportano in tabella alcuni dei protocolli ed i nomi dei produttori delle relative schede di rete rilevati in questa sessione (solo indirizzi singlecast, il produttore si riferisce alla scheda di rete di destinazione).

Protocollo	Costruttore scheda di rete e dettagli
UDP	Gemtek (access point)
IGMPv2	Gemtek (antenna FWA, default gateway)
MDNS	Sconosciuto (`F6:6B:E9`, probabilmente un indirizzo randomizzato)
MDNS	Texas Instruments (dispositivo IoT)
TCP	Rigol Technologies (oscilloscopio, probabilmente per LXI)
STUN	Apple, Inc. (tablet, STUN sfruttato da FaceTime, software VoIP)
TLSv1	Gemtek (antenna FWA, default gateway)

Si esegue il comando `ping` per forzare la trasmissione di pacchetti broadcast. Questo comporta la comparsa di vari pacchetti broadcast con protocollo ARP (Address Resolution Protocol) in Wireshark. L'indirizzo MAC dei pacchetti broadcast è `FF:FF:FF:FF:FF:FF`.

Imbustamento multiplo

Per la parte finale di questa esercitazione, si desidera ottenere una visione d'insieme di tutti gli imbustamenti effettuati per caricare una pagina web mentre si è connessi ad una rete 802.11ac. Non essendo momentaneamente possibile

ricorrere ad un collegamento Ethernet cablato, occorrerà utilizzare delle tecniche di sniffing per poter effettuare questa analisi su rete wireless.

Visto che attivare la modalità monitor su una scheda di rete wireless ne comporta la disconnessione dalla rete, si opererà nel modo seguente:

- Il computer con il software di cattura del traffico viene utilizzato come sniffer. Data la presenza di una sola scheda di rete wireless integrata, questo dispositivo sarà dedicato soltanto all'analisi del traffico, e non alla sua generazione.
- Un telefono cellulare è configurato come access point ("hotspot"). La rete generata è protetta da password, ma questa è conosciuta.
- Un altro dispositivo mobile (tablet) è connesso all'access point. Ad un certo punto si visiterà la home page di montessoro.it e si cercherà di catturarne la sua trasmissione mediante Wireshark. Se questo sarà opportunamente configurato, si potrà vedere l'imbustamento completo dei dati contenuti nella pagina.

(Si riporta la procedura di attivazione ed uso della monitor mode, in maniera simile a quanto indicato sul forum di e-learning).

Si è notato che effettuando una cattura del traffico 802.11 in *managed mode* si perdono molte informazioni sul protocollo 802.11. Nonostante non si sia in grado di analizzare gli header del protocollo 802.11ac, si vuole effettuare questa analisi avanzata in modo di avere un quadro generale degli imbustamenti effettuati.