
S11L3

UNIT 3

Marco Falchi

Quali sono gli indirizzi MAC di origine e destinazione?

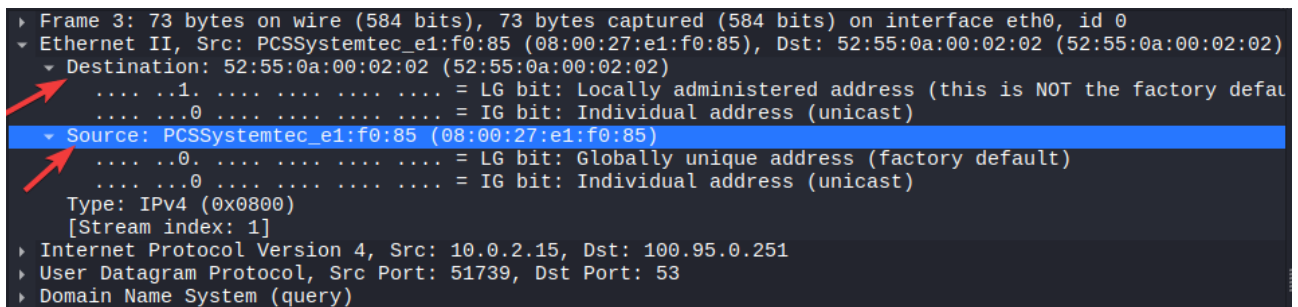
Origine: PCSSystemtec_e1:f0:85 (08:00:27:e1:f0:85)

Destinazione: 52:55:0a:00:02:02 (52:55:0a:00:02:02)

A quali interfacce di rete sono associati questi indirizzi MAC?

L'indirizzo MAC di origine (Source): 08:00:27:e1:f0:85. È associato a un'interfaccia di rete chiamata PCSSystemtec_e1:f0:85.

Indirizzo MAC di destinazione (Destination): 52:55:0a:00:02:02. È associato a un'interfaccia di rete senza un nome specifico mostrato, identificata unicamente dal proprio indirizzo MAC.



```
▶ Frame 3: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
▼ Ethernet II, Src: PCSSystemtec_e1:f0:85 (08:00:27:e1:f0:85), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
  ▼ Destination: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: PCSSystemtec_e1:f0:85 (08:00:27:e1:f0:85)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 1]
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 100.95.0.251
▶ User Datagram Protocol, Src Port: 51739, Dst Port: 53
▶ Domain Name System (query)
```

Quali sono gli indirizzi IP di origine e destinazione?

Source Address (Indirizzo di origine): 10.0.2.15

Destination Address (Indirizzo di destinazione): 100.95.0.251

A quali interfacce di rete sono associati questi indirizzi IP?

Gli indirizzi MAC sono associati all'interfaccia di rete usata per catturare i pacchetti quindi di conseguenza sono associati all'interfaccia di rete eth0

L'indirizzo di origine 10.0.2.15 appartiene all'interfaccia di rete eth0, da cui è stato catturato il pacchetto.

L'indirizzo di destinazione 100.95.0.251 è associato all'interfaccia di rete che riceve il pacchetto, che in questo caso funge da server DNS.

```
▼ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 100.95.0.251
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 59
  Identification: 0x9e71 (40561)
  ▶ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x6ad8 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.2.15
  Destination Address: 100.95.0.251
  [Stream index: 0]
```

```
Frame 3: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
```

Quali sono le porte di origine e destinazione?

Porta di origine (Source Port): 52303

Porta di destinazione (Destination Port): 53

Qual è il numero di porta DNS predefinito?

Il numero di porta DNS predefinito è 53.

```
▼ User Datagram Protocol, Src Port: 52303, Dst Port: 53
  Source Port: 52303
  Destination Port: 53
  Length: 39
  Checksum: 0x71a1 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Stream Packet Number: 1]
  ▶ [Timestamps]
  UDP payload (31 bytes)
```

Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?

Gli indirizzi sia MAC che IP sono perfettamente uguali sia dal prompt che dalle analisi wireshark

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fd17:625c:f037:2:62e6:20c6:b2f4:db5c prefixlen 64 scopeid 0x0<global>
    inet6 fe80::1e1:a956:34a5:a0d7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e1:f0:85 txqueuelen 1000 (Ethernet)
    RX packets 17 bytes 3947 (3.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 39 bytes 5134 (5.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?

Indirizzi e Porte

Indirizzi MAC:

Origine: 52:55:0a:00:02:02

Destinazione: 08:00:27:e1:f0:85

Indirizzi IP:

Origine: 100.95.0.251

Destinazione: 10.0.2.15

Numeri di porta:

Porta di origine: 53

Porta di destinazione: 52303

Come si confrontano con gli indirizzi nei pacchetti di query DNS?

La destinazione e origine si invertono

```
▼ Domain Name System (response)
  Transaction ID: 0x5a51
  ▼ Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... .0... .. = Authoritative: Server is not an authority for domain
    .... ..0... .. = Truncated: Message is not truncated
    .... ..1... .. = Recursion desired: Do query recursively
    .... ..1... .. = Recursion available: Server can do recursive queries
    .... ..0... .. = Z: reserved (0)
    .... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the
    .... ..0... .. = Non-authenticated data: Unacceptable
    .... ..0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 5
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
```

Il server DNS può fare query ricorsive?

Sì, il server DNS può fare query ricorsive

```
.... .. 1... .. = Recursion available: Server can do recursive queries
```

Come si confrontano i risultati con quelli di nslookup?

Nslookup ha informazioni meno dettagliate dando solamente l'ip associato al sito di riferimento, Wireshark contiene molte più informazioni permettendo di vedere il singolo pacchetto e molte informazioni di questo.

Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?

Togliendo i filtri su Wireshark, puoi ottenere una visione completa e non filtrata di tutto il traffico che transita sulla rete. Questa visione rimane però caotica a mio parere preferisco quindi utilizzare i filtri dopo aver avuto una visione generale.

Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?

Se la rete non utilizza protocolli sicuri come HTTPS, SSH o TLS, un attaccante può catturare il traffico e ispezionare i pacchetti per trovare informazioni sensibili in chiaro, come credenziali di accesso, password, cookie di sessione e dati personali dove catturando i cookie di sessione, un aggressore può dirottare la sessione di un utente e accedere a un servizio come se fosse l'utente stesso. Oppure, può condurre attacchi man-in-the-middle per reindirizzare tutto il traffico della vittima verso il suo computer e monitorarlo.

Inoltre, se l'attaccante si trova sulla stessa rete locale (LAN), può impostare la scheda di rete in **modalità promiscua** per "sniffare" tutti i pacchetti, non solo quelli a lui diretti. Questo gli consente di spiare il traffico di altri dispositivi sulla rete.

Analizzando il traffico, un attaccante può anche identificare i protocolli e le versioni dei servizi in esecuzione, esponendo potenziali vulnerabilità note che potrebbero essere sfruttate. Ad esempio, potrebbe scoprire un server obsoleto che usa un protocollo insicuro.