S11L3

-Quali sono gli indirizzi MAC di origine e destinazione?

Origine: **08:00:27:d1:f8:5d**

Destinazione: **52:55:c0:a8:32:01**

-A quali interfacce di rete sono associati questi indirizzi MAC?

Origine: **eth0**

Destinazione: interfaccia di rete del default gateway (router).

-Quali sono gli indirizzi IP di origine e destinazione?

IP d'origine: **192.168.50.10**

IP di destinazione: **1.1.1.1**

-A quali interfacce di rete sono associati questi indirizzi IP?

Origine: **eth0**

Destinazione: interfaccia di rete del server DNS pubblico.

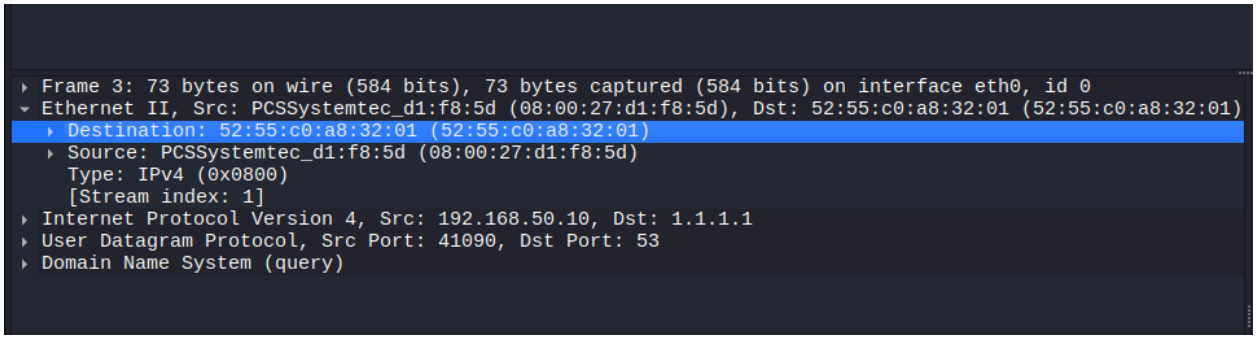
-Quali sono le porte di origine e destinazione?

Porta di destinazione: **53**

Porta d'origine: **41090**

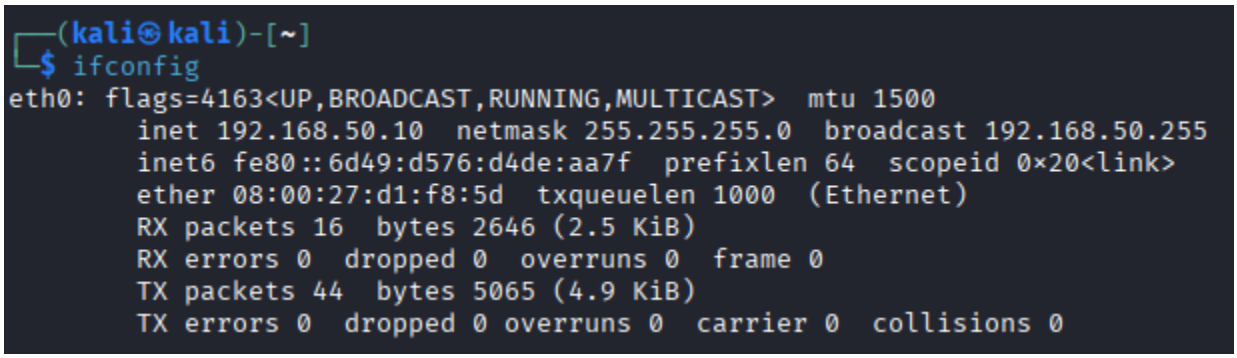
-Qual è il numero di porta DNS predefinito?

La porta 53 è la porta standard predefinita per il protocollo DNS.



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

L'osservazione è che gli indirizzi MAC e IP di origine nel pacchetto di query DNS su **Wireshark** corrispondono esattamente agli indirizzi configurati sull'interfaccia di rete locale verificati tramite **terminale**.



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

Mac d'origine: **52:55:c0:a8:32:01**

IP d'origine: **1.1.1.1**

Porta d'origine: **53**

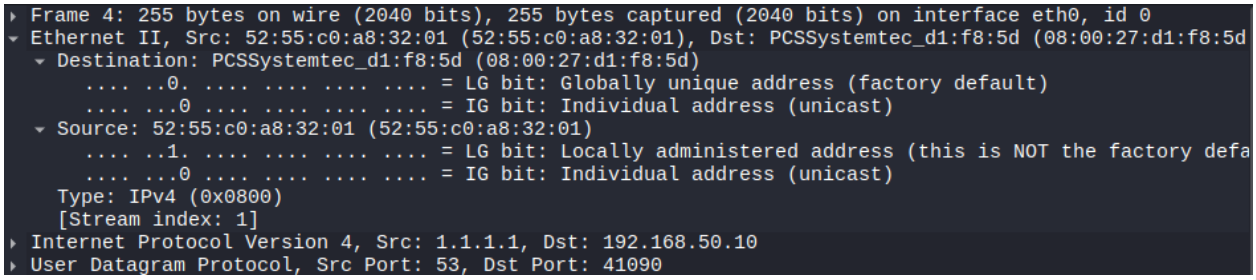
Destinazione: **08:00:27:d1:f8:5d**

IP di destinazione: **192.168.50.10**

Porta di destinazione: **41090**

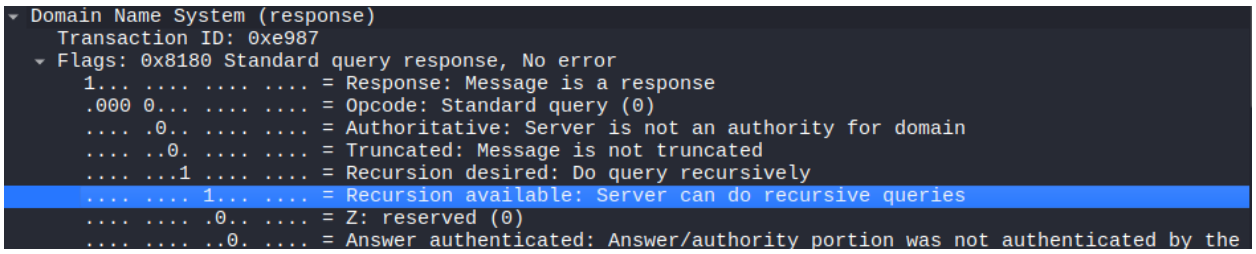
-Come si confrontano con gli indirizzi nei pacchetti di query DNS?

Gli indirizzi e le porte sono **invertiti** (o speculari) rispetto alla query, l"indirizzo IP e la porta che erano **sorgente** nella richiesta sono diventati **destinazione** nella risposta, e viceversa.



-Il server DNS può fare query ricorsive?

Sì.

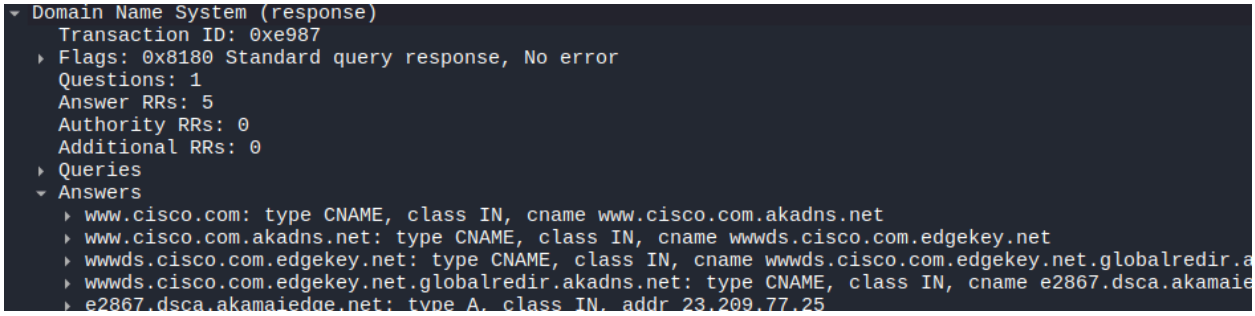


-Come si confrontano i risultati con quelli di nslookup?

I risultati osservati in Wireshark nella sezione **Answers** del pacchetto di risposta corrispondono esattamente all'output testuale fornito dal comando **nslookup**.

```
└─$ nslookup
> www.cisco.com
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
www.cisco.com   canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net        canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net     canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net      canonical name = e2867.dsca.akamaiedge.net.
Name:   e2867.dsca.akamaiedge.net
Address: 23.209.77.25
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:df:19d::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:df:1b1::b33
> exit
```



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

Rimuovendo il filtro, è possibile osservare tutto il traffico di 'background' della rete locale, e non solo le richieste DNS.

Si vedono i pacchetti ARP che i dispositivi usano per annunciare la loro presenza, rivelando gli indirizzi IP e MAC degli altri host nella rete locale.

Quali altri servizi sono attivi e il livello di **'rumore'** della rete, si nota quanto traffico di *broadcast* viene generato, utile per diagnosticare problemi di congestione o configurazioni errate.

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

Un attaccante può utilizzare Wireshark principalmente per due scopi dannosi:

-Sniffing di dati sensibili: poiché Wireshark cattura i dettagli completi dei pacchetti, se il traffico catturato non è crittografato (ad esempio protocolli come HTTP, Telnet, FTP o le query DNS appena analizzate), un attaccante può leggere il contenuto dei messaggi in chiaro. Questo include potenzialmente password, nomi utente, cookie di sessione, email e il contenuto delle pagine web visitate.

-Ricognizione e mappatura della rete (Reconnaissance): anche se il traffico è crittografato (come HTTPS), l'attaccante può comunque analizzare le intestazioni (header) dei pacchetti, come abbiamo fatto in questo laboratorio.

Questo permette di scoprire:

- Gli **indirizzi IP** in uso e la struttura della subnet.
- Gli **indirizzi MAC**, che rivelano il produttore dei dispositivi (es. Apple, Dell, Cisco), aiutando a identificare bersagli specifici o vulnerabili.
- Le abitudini dell'utente tramite l'analisi del **traffico DNS** (quali siti vengono visitati e con che frequenza), violando la privacy della vittima."