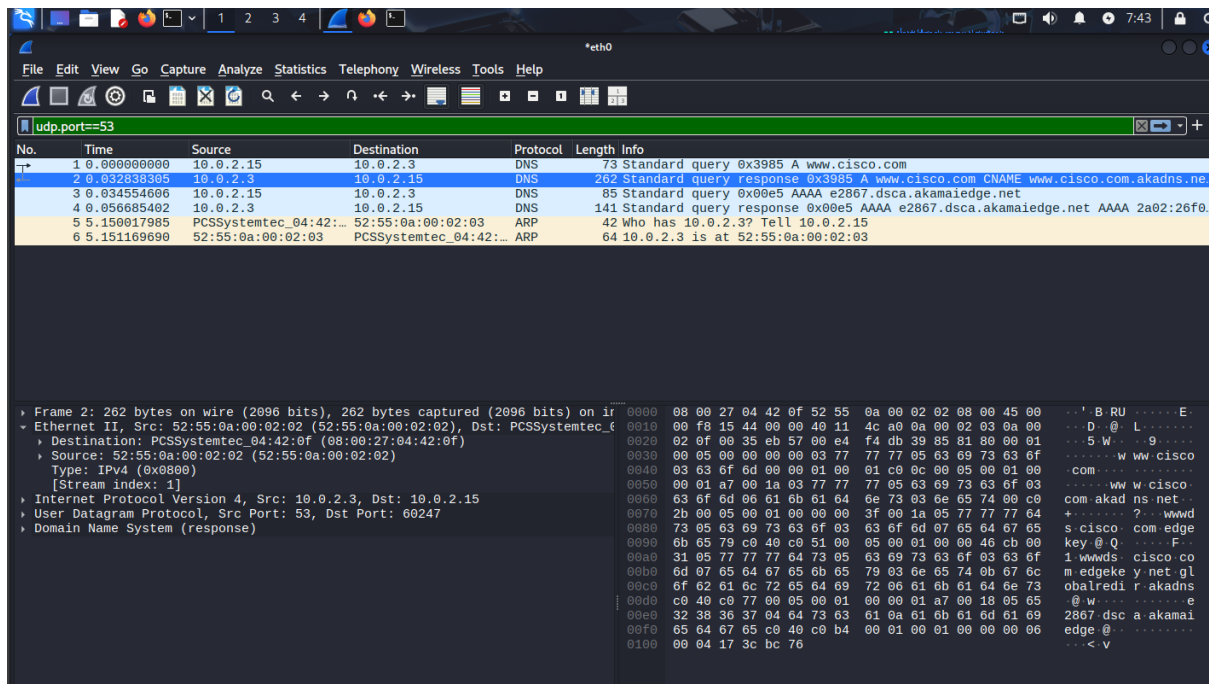


Quali sono gli indirizzi MAC di origine e destinazione?

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

Destinazione 08:00:27:04:42:0f



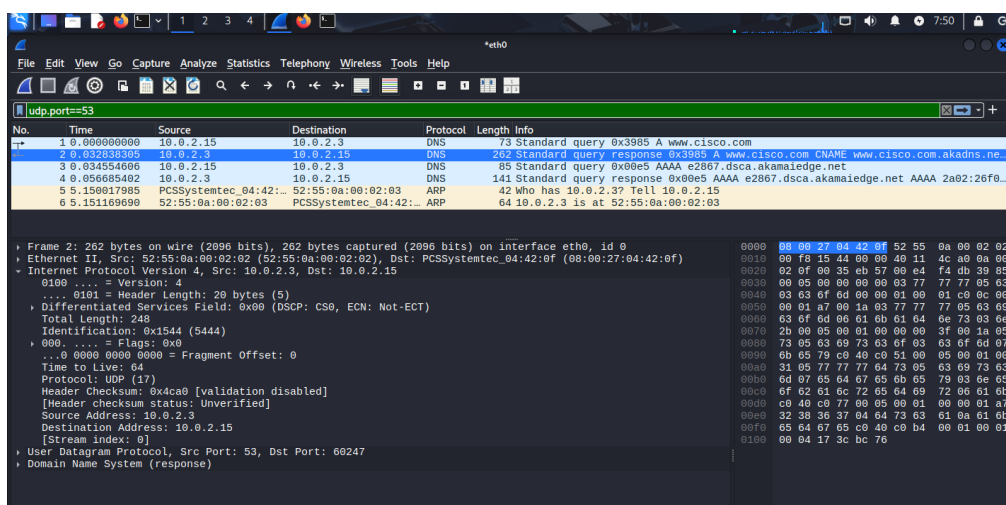
A quali interfacce di rete sono associati questi indirizzi MAC?

- 10.0.2.15 (MAC 08:00:27:04:42:0f) **macchina Kali o client**
- 10.0.2.3 (MAC 52:55:0a:00:02:02) è il **DNS resolver**

Quali sono gli indirizzi IP di origine e destinazione?

10.0.2.3.

10.0.2.15



A quali interfacce di rete sono associati questi indirizzi IP?

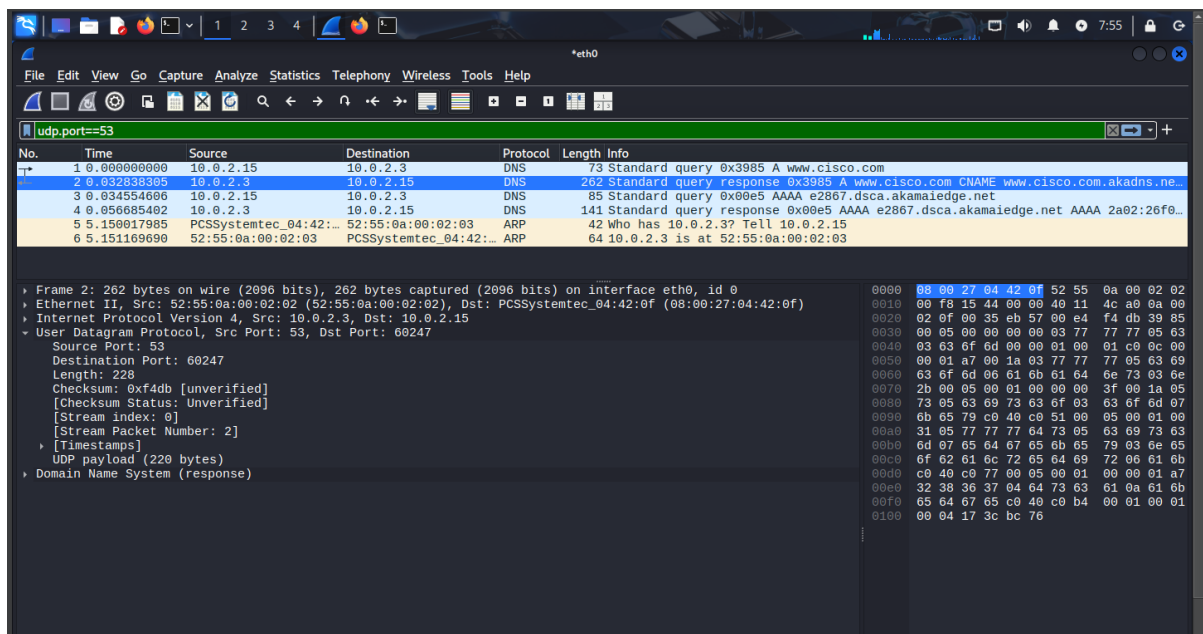
10.0.2.15 → 08:00:27:04:42:0f

- Questo MAC è mostrato come destinazione nei pacchetti in Wireshark.
- L'interfaccia in uso per la cattura è eth0, e il frame è stato ricevuto lì.
- Quindi eth0 è associata a 08:00:27:04:42:0f, cioè alla tua Kali.

10.0.2.3 → 52:55:0a:00:02:02

- Questo IP appare come sorgente nelle risposte DNS.
- Il MAC 52:55:0a:00:02:02 è tipico delle interfacce virtuali (QEMU/KVM o NAT di VirtualBox).
- Quindi 10.0.2.3 è il DNS gateway configurato dalla rete NAT della VM.

Quali sono le porte di origine e destinazione ? 53,60247



Qual è il numero di porta DNS predefinito? 53

Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC.

Qual è la tua osservazione?

Wireshark mostra che il frame è inviato a 08:00:27:04:42:0f, ma l'indirizzo MAC reale di Kali è 08:00:27:04:42:07.

Potrebbe essere un errore di cattura, un typo nello screenshot, o un tentativo di spoofing. Se il traffico è effettivamente ricevuto da Kali, potrebbe indicare:

Un errore nella scheda di rete virtuale (es. VirtualBox con MAC modificato).

Un problema di caching ARP.

Traffico DNS coerente:

Le query DNS partono da 10.0.2.15 (Kali) verso 10.0.2.3 (server DNS), e le risposte tornano correttamente.

```
(kali@kali)-[~]
$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 84395sec preferred_lft 84395sec
```

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

Sottolineati sotto in screenshot

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.3	DNS	73	Standard query 0x43e4 A www.cisco.com
2	0.032379378	10.0.2.3	10.0.2.15	DNS	262	Standard query response 0x43e4 A www.cisco.com
3	0.034166346	10.0.2.15	10.0.2.3	DNS	85	Standard query 0xcfc6 AAAA e2867.dsca.akamaiedge.net
4	0.056604454	10.0.2.3	10.0.2.15	DNS	141	Standard query response 0xcfc6 AAAA e2867.dsca.akamaiedge.net
5	5.107842483	PCSSystemtec_04:42:0f	52:55:0a:00:02:03	ARP	42	Who has 10.0.2.3? Tell 10.0.2.15
6	5.108896297	52:55:0a:00:02:03	PCSSystemtec_04:42:0f	ARP	64	10.0.2.3 is at 52:55:0a:00:02:03

Frame 2: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface eth0, id 0	0000
Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_04:42:0f (08:00:27:04:42:0f)	0010
Destination: PCSSystemtec_04:42:0f (08:00:27:04:42:0f)	0020
Source: 52:55:0a:00:02:02 (52:55:0a:00:02:02)	0030
Type: IPv4 (0x0800)	0040
[Stream index: 1]	0050
Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15	0060
User Datagram Protocol, Src Port: 53, Dst Port: 55055	0070
Domain Name System (response)	0080
	0090
	00a0
	00b0

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

Il server DNS può fare query ricorsive? Sì, lo vediamo in answers

```
Source: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
Type: IPv4 (0x0800)
[Stream index: 1]
Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 55055
Domain Name System (response)
Transaction ID: 0x43e4
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 5
Authority RRs: 0
Additional RRs: 0
Queries
  www.cisco.com: type A, class IN
Answers
  www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
  www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
  wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
  wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
  e2867.dsca.akamaiedge.net: type A, class IN, addr 23.60.188.118
[Request In: 1]
[Time: 0.032379378 seconds]
```

Come si confrontano i risultati con quelli di nslookup?

- Coerenza:
  - Sia Wireshark che `nslookup/dig` mostrano la stessa catena di CNAME e l'IP finale (23.60.180.118).
  - Entrambi indicano che il server DNS (10.0.2.3) ha eseguito una risoluzione ricorsiva.

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

Quando si rimuovono i filtri in Wireshark, otteniamo una visione completa del traffico di rete, rivelando dettagli nascosti che non emergono dalle sole query DNS. Ecco cosa si potrebbe imparare:

Identificazione dei dispositivi nella rete

Indirizzi MAC e IP:

ARP traffic

Altri servizi attivi oltre al DNS

Protocolli in uso

Server DHCP:

Comportamento anomalo o minacce

Scansioni di porte:

Broadcast/Multicast insoliti:

DNS sospetti:

Nella nostra cattura, notiamo:

1. DNS ricorsivo: Il server 10.0.2.3 risolve [www.cisco.com](http://www.cisco.com) passando per Akamai (akamaiedge.net).
2. ARP requests: Il dispositivo 10.0.2.15 (Kali) cerca 10.0.2.37, suggerendo che altri host sono presenti nella rete.
3. Tempi rapidi: La risposta DNS è veloce (0.032s), quindi il server locale è efficiente.

Se rimuoviamo il filtro, potremmo anche vedere:

- Chiamate NTP/SSH: Se Kali sta sincronizzando l'ora o ha sessioni attive.
- Traffico verso l'esterno: Se il gateway (10.0.2.1 o 10.0.2.3) inoltra traffico a Internet.

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

Sniffing del Traffico (Intercettazione Passiva)

ARP Spoofing/Poisoning (Intercettazione Attiva)

Analisi di Vulnerabilità

Ricostruzione di File Trasferiti

Attacchi a Protocolli Insicuri

Identificazione di Dispositivi IoT Vulnerabili

Wireshark è un'arma potente nelle mani di un attaccante: può essere usato per spiare, rubare dati e preparare attacchi mirati. La miglior difesa è crittografia, monitoraggio e hardening della rete.