

## Pratica Cisco Ops 3

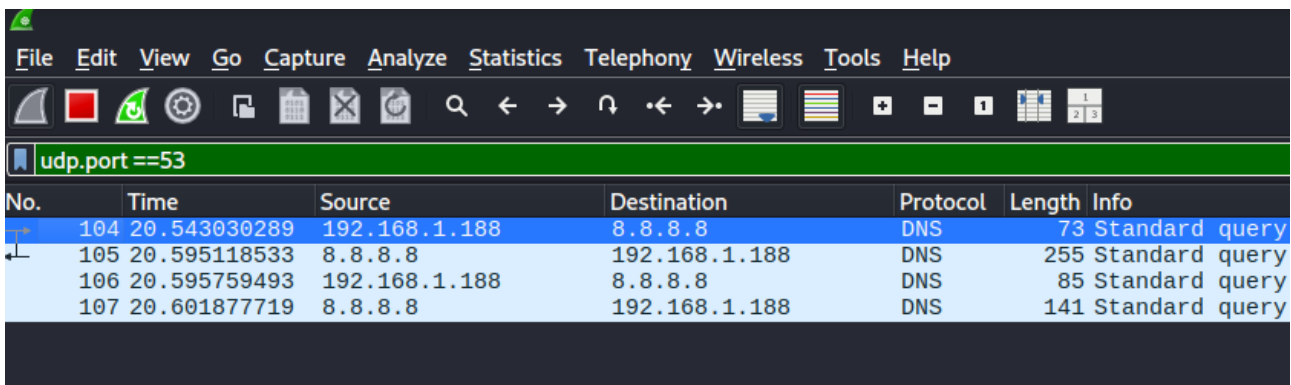
Nella pratica di oggi utilizzeremo Wireshark sulla nostra Kali e risponderemo alle domande.

Una volta aggiornati i pacchetti sul nostro terminale Kali, apriamo wireshark e mettiamolo in ascolto. Subito dopo nel nostro terminale usiamo il comando **nslookup** ove si aprirà una modalità interattiva, dove andremo a digitare [www.cisco.com](http://www.cisco.com) – noteremo che il nostro wireshark avrà catturato dei pacchetti.

```
(kali@kali)-[~]
$ nslookup
> www.cisco.com
Server:      8.8.8.8
Address:     8.8.8.8#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: 23.49.196.116
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:8d00:c9e::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:8d00:cb6::b33
>
```

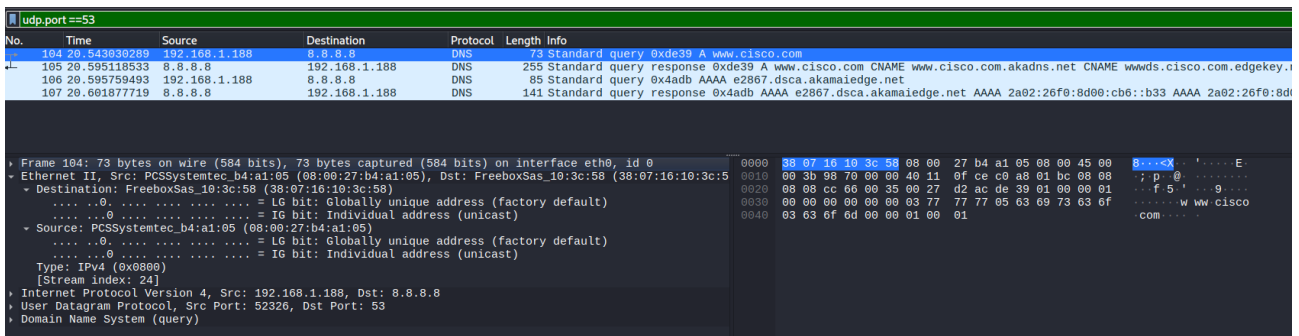
Digitiamo exit nella nostra console e concentriamoci ora su wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
104	20.543030289	192.168.1.188	8.8.8.8	DNS	73	Standard query
105	20.595118533	8.8.8.8	192.168.1.188	DNS	255	Standard query response
106	20.595759493	192.168.1.188	8.8.8.8	DNS	85	Standard query
107	20.601877719	8.8.8.8	192.168.1.188	DNS	141	Standard query response

Come richiesto dall'esercizio digitiamo nel **filtro** **udp.port == 53**, filtro che serve per visualizzare solo il traffico DNS che usa il protocollo UDP sulla porta 53, che è la porta standard per le richieste DNS.

Andiamo adesso a rispondere alle prime domande, basandoci sull'analisi dello screenshot sottostante.



The screenshot shows the packet details pane for packet 104, a DNS Standard query. The packet is captured on interface eth0, id 0. The Ethernet II header shows the source as PCSSystemtec\_b4:a1:05 and the destination as FreeboxSas\_10:3c:58. The IP header shows the source as 192.168.1.188 and the destination as 8.8.8.8. The UDP header shows the source port as 52326 and the destination port as 53. The DNS header shows the transaction ID as 0x4dbb and the query type as A. The query is for the domain www.cisco.com.

Domande:

- Quali sono gli indirizzi MAC di origine e destinazione?

**R:** Il MAC di origine si trova sia nel primo rigo su "PCSSystemtec\_b4: 08:00:27:b4:a1:05" – e lo ritroviamo di nuovo più in basso sotto source, dove ci viene ripetuto.

Il MAC di destinazione invece lo troviamo 'Destination: FreeboxSas\_10: 38:07:16:10:3c:58'

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

**R:** 08:00:27:b4:a1:05 (il MAC source) è un indirizzo VirtualBox o interfaccia di rete locale in questo caso del nostro dispositivo Kali Linux.

Prefisso 08:00:27 è noto come MAC address di Oracle/VirtualBox.

38:07:16:10:3c:58 (Destination MAC) è associato a Freebox, un router (tipico ISP francese).

È la gateway/router sulla mia rete locale.

Espandiamo adesso il Protocol Version 4.

```
164 20.54369280 192.168.1.188 8.8.8.8 DNS 73 Standard query 0xde39 A www.cisco.com
165 20.595118533 8.8.8.8 192.168.1.188 DNS 253 Standard query response 0xde39 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edg
166 20.595759493 192.168.1.188 8.8.8.8 DNS 85 Standard query 0x4adb AAAA e2867.dsca.akamaiedge.net
167 20.601877719 8.8.8.8 192.168.1.188 DNS 141 Standard query response 0x4adb AAAA e2867.dsca.akamaiedge.net AAAA 2a02:26f0:8d00:cb6::b33 AAAA 2a02:26

Frame 164: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05), Dst: FreeboxSas_10:3c:58 (38:07:16:10:3c:58)
Internet Protocol Version 4, Src: 192.168.1.188, Dst: 8.8.8.8
0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 59
Identification: 0x0870 (39024)
000: ... = Flags: 0x0
... 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x0fce [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.188
Destination Address: 8.8.8.8
[Stream index: 20]
User Datagram Protocol, Src Port: 52326, Dst Port: 53
Domain Name System (query)
```

Domande:

- Quali sono gli indirizzi IP di origine e destinazione?

**R:** IP di origine: 192.168.1.188 – l'ip della nostra Kali, che troviamo nel primissimo rigo evidenziato in arancione "Internet Protocol Version 4, Src (che sta per source), Dst (che sta per destination) infatti l'IP di destinazione è 8.8.8.8

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

**R:** l'ip 192.168.1.188 È l'indirizzo IP privato associato all'interfaccia di rete della mia macchina virtuale Kali Linux. Lo verifichiamo con un **ip a** da terminal che ci restituirà questo risultato:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.188/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
```

Invece per quanto riguarda l'indirizzo di destinazione 8.8.8.8 Server DNS pubblico (Google).

Espandere User Datagram Protocol (UDP). Osservare le porte di origine e destinazione.

- Quali sono le porte di origine e destinazione?

**R:** Src Port (porta d'origine): 48521 – Dst Port (porta di destinazione): 53

```
User Datagram Protocol, Src Port: 48521, Dst Port: 53
Source Port: 48521
Destination Port: 53
Length: 39
Checksum: 0xc49e [unverified]
[Checksum Status: Unverified]
[Stream index: 21]
[Stream Packet Number: 1]
```

- Qual è il numero di porta DNS predefinito?

**R:** Il numero di porta DNS predefinito è: 53.  
Ovvero il destination port - La porta 53 è stata designata dall'IANA (Internet Assigned Numbers Authority) come porta ufficiale per il DNS.

Determinare l'indirizzo IP e MAC del PC.

```
Frame 65: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05), Dst: FreeboxSas_10:3c:58 (38:07:16:10:3c:58)
  Destination: FreeboxSas_10:3c:58 (38:07:16:10:3c:58)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 25]
Internet Protocol Version 4, Src: 192.168.1.188, Dst: 1.1.1.1
  User Datagram Protocol, Src Port: 48521, Dst Port: 53
  Domain Name System (query)

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.188 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:b4:a1:05 txqueuelen 1000 (Ethernet)
    RX packets 7074 bytes 1825372 (1.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 454 bytes 133552 (130.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 680 (680.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 680 (680.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
0000 38 07 16 10 3c 58 08 00 27 b4 a1 05 08 00 45 00 8...<X...E
0010 00 3b b3 fb 00 00 40 11 02 51 c0 a8 01 bc 01 01 :...@...Q...
0020 01 01 bd 89 00 35 00 27 c4 9e 3a 83 01 00 00 01 :...5...T:...
0030 00 00 00 00 00 00 03 77 77 05 63 69 73 63 6f :...wwww.cisco
0040 83 63 6f 6d 00 00 01 00 01 :...com...
```

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

**R:** Sia gli indirizzi IP che i MAC di sorgente corrispondono perfettamente.

Esplorare il Traffico delle Risposte DNS

```
Frame 68: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface eth0, id 0
Ethernet II, Src: FreeboxSas_10:3c:58 (38:07:16:10:3c:58), Dst: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05)
  Destination: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: FreeboxSas_10:3c:58 (38:07:16:10:3c:58)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 25]
Internet Protocol Version 4, Src: 1.1.1.1, Dst: 192.168.1.188
  User Datagram Protocol, Src Port: 53, Dst Port: 48521
    Source Port: 53
    Destination Port: 48521
    Length: 221
    Checksum: 0xdc54 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 21]
    [Stream Packet Number: 2]
    [Timestamps]
    UDP payload (213 bytes)
  Domain Name System (response)
```

```
0000 08 00 27 b4 a1 05 38 07 16 10 3c 58 08 00 45 00 8...<X...E
0010 00 f1 04 e8 40 00 39 11 77 ae 01 01 01 01 c0 a8 :...@...W...
0020 01 bc 00 35 bd 89 00 dd dc 54 3a 83 81 80 00 01 :...5...T:...
0030 00 05 00 00 00 00 03 77 77 05 63 69 73 63 6f :...wwww.cisco
0040 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 00 01 00 :...com...
0050 00 0e 01 00 1a 83 77 77 77 05 63 69 73 63 6f 63 :...wwww.cisco
0060 63 6f 6d 06 61 6b 61 64 6e 73 03 6e 65 74 00 c0 :...com.akad.ns.net
0070 2b 00 05 00 01 00 00 01 1d 00 1a 85 77 77 77 64 :...+...www
0080 73 85 03 09 73 63 6f 63 63 6f 6d 07 65 64 67 65 :...svcisco.com.edge
0090 8b 85 79 c0 40 c0 51 00 05 00 01 00 00 54 51 00 :...key-l-q...TQ
00a0 2a 85 77 77 77 64 73 85 63 69 73 63 6f 63 6f 63 :...wwwds.cisco.co
00b0 6d 07 65 64 67 65 6b 65 79 03 6e 65 74 0b 67 6c :...m.edgekey.net.gl
00c0 6f 62 61 6c 72 65 64 69 72 c0 39 c0 77 00 05 00 :...obalredi.r9.w...
00d0 01 00 00 0e 01 00 18 05 65 32 38 36 37 04 64 73 :...e2867.ds
00e0 63 61 8a 61 6b 61 6d 61 69 65 64 67 65 c0 40 c0 :...ca.akamaiedge@
00f0 ad 00 01 00 01 00 00 00 05 00 04 17 31 c4 74 :...1.t
```

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

**R:**

**Ethernet II:**

- MAC di Sorgente (Src MAC): FreeboxSas\_10:3c:58 (38:07:16:10:3c:58)
- MAC di Destinazione (Dst MAC): PCSSystemtec\_b4:a1:05 (08:00:27:b4:a1:05)

**Internet Protocol Version 4:**

- IP di Sorgente (Src IP): 1.1.1.1
- IP di Destinazione (Dst IP): 192.168.1.188

**User Datagram Protocol:**

- Porta di Sorgente (Src Port): 53
- Porta di Destinazione (Dst Port): 48521

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

- R:** Come previsto per una comunicazione client-server (in questo caso, client DNS che interroga un server DNS e riceve una risposta), gli indirizzi e le porte di sorgente e destinazione si sono invertiti tra la query e la risposta.

**Indirizzi MAC:**

- Query: Client MAC (08:00:27:b4:a1:05) -> Router MAC (38:07:16:10:3c:58)

- **Risposta:** Router MAC (38:87:16:10:3c:58) -> Client MAC (08:00:27:b4:a1:05)
- **Osservazione:** Gli indirizzi MAC di sorgente e destinazione si sono invertiti. Questo è il comportamento normale: il router che ha ricevuto la query dal client ora invia la risposta al client.

## 2. Indirizzi IP:

- **Query:** Client IP (192.168.1.188) -> DNS Server IP (1.1.1.1)
- **Risposta:** DNS Server IP (1.1.1.1) -> Client IP (192.168.1.188)
- **Osservazione:** Gli indirizzi IP di sorgente e destinazione si sono invertiti. Il server DNS (1.1.1.1) risponde direttamente al client che ha inviato la query (192.168.1.188).

## 3. Numeri di Porta:

- **Query:** Client Port (48521) -> DNS Standard Port (53)
- **Risposta:** DNS Standard Port (53) -> Client Port (48521)
- **Osservazione:** Le porte di sorgente e destinazione si sono invertite. La risposta proviene dalla porta DNS standard (53) e viene inviata alla porta effimera (48521) che il client aveva usato per inviare la query. Questo permette al client di associare la risposta alla richiesta originale.

In sintesi, i pacchetti di query e risposta DNS mostrano un perfetto scambio di ruoli tra sorgente e destinazione per tutti i livelli (MAC, IP, Porte), confermando che il pacchetto attuale è la risposta alla query precedente.

## • Il server DNS può fare query ricorsive?

**R:** Sì, un server DNS può fare query ricorsive. I server DNS ricorsivi (come 1.1.1.1 o 8.8.8.8) sono progettati per cercare l'indirizzo IP per conto del client, interrogando altri server DNS finché non trovano la risposta.

Osservare i record CNAME e A nei dettagli delle Risposte (Answers).

```

▼ 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
    Name: www.cisco.com.akadns.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 285 (4 minutes, 45 seconds)
    Data length: 26
    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 23.49.196.116

```

## • Come si confrontano i risultati con quelli di nslookup?

**R:** I risultati sono coerenti. Sia la traccia Wireshark che nslookup mostrano la stessa catena di CNAME (alias) che termina con un record A (indirizzo IPv4) per e2867.dsca.akamaiedge.net, risolvendo a 23.49.196.116.

```

▼ 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
    Name: www.cisco.com.akadns.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 285 (4 minutes, 45 seconds)
    Data length: 26
    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 23.49.196.116

```

## Riflessione

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

**R:**

*Rimuovendo il filtro da Wireshark, puoi imparare quanto segue sulla rete:*

1. **Traffico Broadcast e Multicast:** Si osservano pacchetti broadcast (es. ARP) e multicast (es. SSDP per M-SEARCH HTTP/1.1), indicando attività di scoperta di rete e servizi da parte di vari dispositivi sulla LAN.
2. **Protocolli Diversi:** Oltre a DNS/UDP/TCP/IP, sono visibili altri protocolli come ICMPv6 (Neighbor Solicitation per IPv6) e ARP (Address Resolution Protocol per IPv4).
3. **Comunicazione IPv6:** Sono presenti pacchetti IPv6 (es. ICMPv6 Neighbor Solicitation e indirizzi fe80:: o fdb0::), suggerendo che la rete supporta sia IPv4 che IPv6.
4. **Dispositivi Connessi:** Si possono identificare altri dispositivi sulla rete locale che comunicano (es. 192.168.1.193, 192.168.1.54, 192.168.1.49, ecc.) e si possono osservare i loro indirizzi MAC.
5. **Attività di Rete Generale:** Vengono mostrati una varietà di pacchetti UDP generici verso 255.255.255.255 (broadcast) e altre comunicazioni locali, fornendo una panoramica dell'attività di fondo sulla rete.
6. **Errore o Problema di Rete:** Se ci fossero problemi, si potrebbero notare pacchetti di errore, ritrasmissioni o altri indicatori di malfunzionamento (sebbene non evidenti in questa porzione specifica dello screenshot).

*In sintesi, senza filtri, Wireshark rivela un quadro molto più completo e dettagliato di tutta l'attività di rete, inclusi protocolli di livello inferiore e comunicazioni tra vari dispositivi presenti sulla LAN.*

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

**R:**

Un attaccante può usare Wireshark per:

1. **Intercettare Dati Sensibili:** Catturare e leggere informazioni non crittografate come password, nomi utente e file trasmessi sulla rete.
  2. **Mappare la Rete:** Scoprire la topologia della rete, gli indirizzi IP dei dispositivi, i sistemi operativi in uso e i servizi attivi, identificando così potenziali punti deboli.
  3. **Rivelare Vulnerabilità:** Trovare protocolli obsoleti o configurazioni di rete errate che possono essere sfruttate per attacchi.
  4. **Pianificare Attacchi Mirati:** Comprendere il normale traffico di rete per lanciare attacchi più efficaci o per far passare traffico malevolo inosservato.
-