

REPORT DI LABORATORIO: ANALISI DEL TRAFFICO DNS CON WIRESHARK

Studente: Nicola Cassandra

Obiettivi: •Catturare il Traffico DNS

•Esplorare il Traffico delle Query DNS

•Esplorare il Traffico delle Risposte DNS

Tools: Wireshark

1. Obiettivo dell'Analisi

L'obiettivo di questo laboratorio è comprendere il funzionamento del protocollo **DNS (Domain Name System)** attraverso l'intercettazione e l'analisi dei pacchetti di rete. Utilizzando **Wireshark**, analizzeremo il processo di risoluzione dei nomi (Query) e la risposta del server (Response), esaminando i dettagli di encapsulamento dai livelli Ethernet fino al livello Applicativo.

2. Configurazione della Macchina Attaccante (Client)

Prima di analizzare il traffico, è fondamentale stabilire l'identità della nostra macchina nella rete locale per distinguere il traffico generato da noi rispetto a quello esterno.

Dall'analisi della configurazione di rete tramite terminale, abbiamo identificato i seguenti parametri per l'interfaccia **eth0**:

- **Indirizzo IP (Client):** 10.0.2.15
- **Indirizzo MAC (Client):** 08:00:27:1f:b7:23

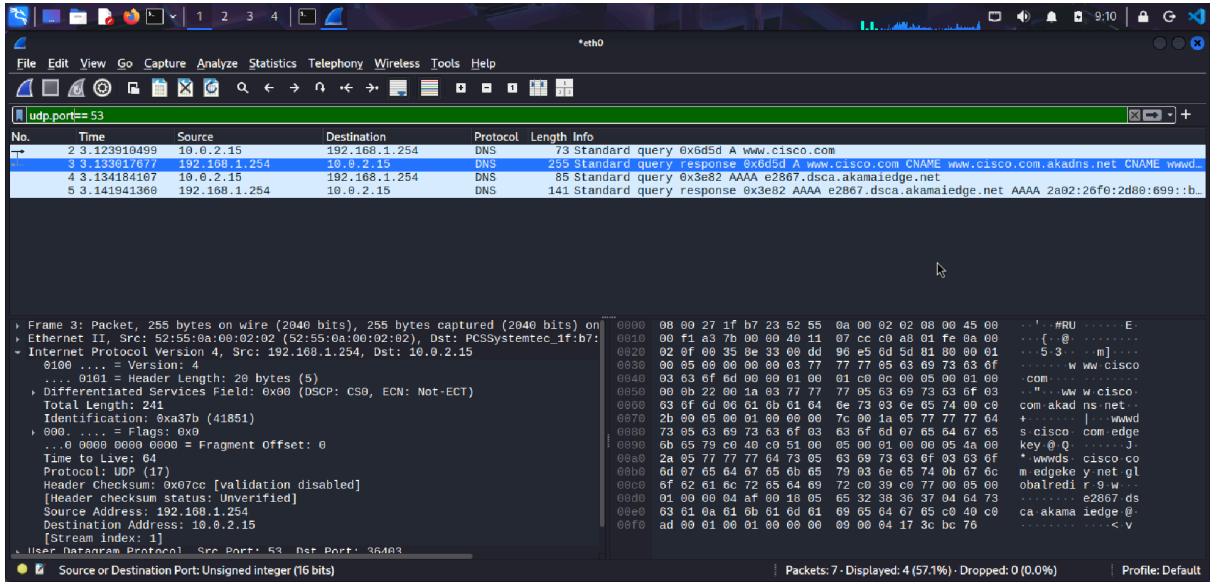
```
L$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:f069:7813:b8b4:c931 prefixlen 64 scopeid 0x0<global>
        inet6 fe80::371:21b6:2160:aff6 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:1f:b7:23 txqueuelen 1000 (Ethernet)
            RX packets 151701 bytes 221068637 (210.8 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 14380 bytes 877438 (856.8 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 10 bytes 580 (580.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 10 bytes 580 (580.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Descrizione: Screenshot del terminale con il comando `ifconfig` che mostra l'indirizzo IP e MAC dell'interfaccia eth0.

3. Cattura e Filtraggio del Traffico

Abbiamo avviato Wireshark e applicato un filtro specifico per isolare il traffico DNS. Il filtro utilizzato è `udp.port == 53`, poiché il DNS opera nativamente sulla porta 53 UDP per le query standard.



Descrizione: La finestra principale di Wireshark con il filtro applicato nella barra superiore e la lista dei pacchetti visibile.

4. Analisi del Pacchetto "DNS Query" (Richiesta)

Abbiamo selezionato il **Frame n. 2**, che rappresenta la richiesta inviata dal client per risolvere il dominio www.cisco.com.

4.1 Analisi Livello 2 (Data Link - Ethernet II)

Espandendo l'header Ethernet II, osserviamo i dettagli fisici della trasmissione.

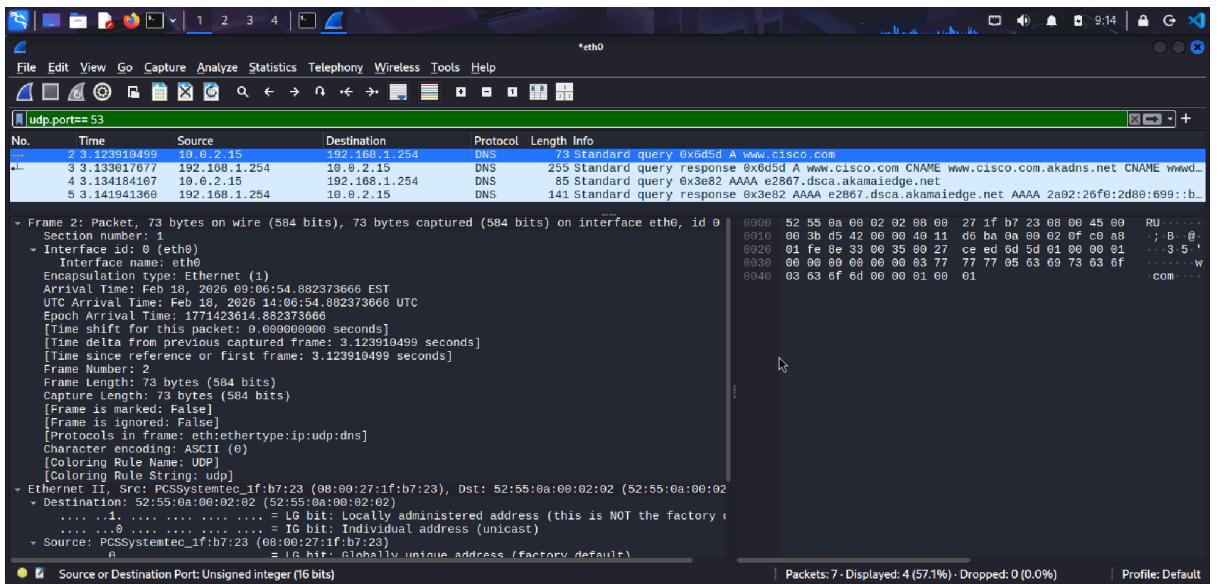
- **MAC Sorgente:** `08:00:27:1f:b7:23` (Corrisponde alla nostra macchina [PCSSystemtec...](#), verificato tramite [ifconfig](#)).
- **MAC Destinazione:** `52:55:0a:00:02:02` (Corrisponde al Gateway/Router che inoltrerà la richiesta).
- **Interfaccia di cattura:** Il pacchetto è stato catturato sull'interfaccia `eth0`.

```

Frame 2: Packet, 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface
Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: 52:55:0a:00:02:02
  Destination: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
  Source: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23)
  Type: IPv4 (0x0800)
    [Stream index: 0]
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 36403, Dst Port: 53
  Domain Name System (query)

```

Descrizione: Dettaglio del pannello "Packet Details" con il livello Ethernet II espanso, evidenziando Source e Destination MAC.



Descrizione: Dettaglio che mostra l'Interface id: 0 (eth0), confermando su quale scheda di rete fisica è avvenuta la cattura.

4.2 Analisi Livello 3 (Network - IPv4)

A livello IP, verifichiamo l'instradamento logico.

- **IP Sorgente:** 10.0.2.15 (Il nostro Client).
- **IP Destinazione:** 192.168.1.254 (Il Server DNS locale o il Gateway che fa da DNS forwarder).

No.	Time	Source	Destination	Protocol	Length	Info
2	3.123910499	10.0.2.15	192.168.1.254	DNS	73	Standard query 0x6d5d A www.cisco.com
3	3.133617677	192.168.1.254	10.0.2.15	DNS	255	Standard query response 0xd5d A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwd...
4	3.134184167	10.0.2.15	192.168.1.254	DNS	85	Standard query 0x3e82 AAAA e2867.dsca.akamaiedge.net
5	3.141941360	192.168.1.254	10.0.2.15	DNS	141	Standard query response 0x3e82 AAAA e2867.dsca.akamaiedge.net AAAA 2a02:26f0:2d80:699:b...

Descrizione: Focus sulla lista pacchetti o sui dettagli IP che mostrano chiaramente il flusso da 10.0.2.15 verso 192.168.1.254.

4.3 Analisi Livello 4 (Transport - UDP)

Il DNS utilizza UDP per la velocità e la leggerezza.

- **Porta Sorgente:** 36403 (Una porta alta dinamica/effimera assegnata dal sistema operativo al browser/client).
- **Porta Destinazione:** 53 (La porta standard riservata al servizio DNS).

```
▼ User Datagram Protocol, Src Port: 36403, Dst Port: 53
  Source Port: 36403
  Destination Port: 53
  Length: 39
  Checksum: 0xceed [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Stream Packet Number: 1]
  ▶ [Timestamps]
  UDP payload (31 bytes)
  ▶ Domain Name System (query)
```

Descrizione: Sezione "User Datagram Protocol" espansa che mostra Source Port: 36403 e Destination Port: 53.

4.4 Analisi Livello 7 (Application - DNS Query)

Analizzando il payload DNS, notiamo che il flag **Recursion Desired** è impostato a 1. Questo significa che il nostro client chiede al server DNS di farsi carico dell'intera ricerca (se non ha l'IP in cache, dovrà chiedere ai Root server, ai TLD server, ecc.) e di restituirci solo il risultato finale.

```
▼ Domain Name System (query)
  Transaction ID: 0x6d5d
  ▶ Flags: 0x0100 Standard query
    0... .... .... = Response: Message is a query
    .000 0.... .... = Opcode: Standard query (0)
    .... .0. .... = Truncated: Message is not truncated
    .... .1 .... .... = Recursion desired: Do query recursively
    .... .0... .... = Z: reserved (0)
    .... .... .0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▶ Queries
    ▶ www.cisco.com: type A, class IN
      [Response In: 3]
```

Descrizione: Sezione "Domain Name System (query)" espansa, con focus sui Flags dove si vede "Recursion desired: Do query recursively".

5. Analisi del Pacchetto "DNS Response" (Risposta)

Abbiamo selezionato il **Frame n. 3**, che rappresenta la risposta del server.

5.1 Confronto Indirizzi (IP e MAC)

In questo pacchetto, i ruoli si invertono speculabilmente rispetto alla query:

- **Sorgente:** IP 192.168.1.254 (Server) / MAC 52:55:0a:00:02:02.
- **Destinazione:** IP 10.0.2.15 (Client) / MAC 08:00:27:1f:b7:23.
- **Porte:** Sorgente 53 -> Destinazione 36403.

```

Frame 3: Packet, 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface eth0, interface
Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23)
  Destination: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23)
  Source: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
  Type: IPv4 (0x0800)
  [Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 10.0.2.15
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 241
  Identification: 0xa37b (41851)
  000. .... = Flags: 0x0
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x07cc [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.254
  Destination Address: 10.0.2.15
  [Stream index: 1]
User Datagram Protocol, Src Port: 53, Dst Port: 36403
  Domain Name System (response)

```

Descrizione: Dettaglio del pacchetto di risposta che mostra l'inversione degli indirizzi IP e MAC rispetto alla richiesta.

5.2 Analisi Application Layer (Flags & Answers)

Nel pacchetto di risposta, il server conferma di supportare la ricorsione (**Recursion available: Server can do recursive queries**).

```

Domain Name System (response)
  Transaction ID: 0x6d5d
  Flags: 0x8100 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
    .... 0.... .... = Recursion available: Server can do recursive queries
    .... 0.... .... = Z: reserved (0)
    .... 0.... .... = Answer authenticated: Answer/authority portion was not authenticated by 1
    .... 0.... .... = Non-authenticated data: Unacceptable
    .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 5
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.cisco.com: type A, class IN
  Answers
    [Request In: 2]

```

Descrizione: I Flags della risposta DNS che mostrano "Standard query response" e "Recursion available".

Nella sezione **Answers**, il server non restituisce immediatamente un IP, ma una catena di **CNAME** (Alias). www.cisco.com è un alias per www.cisco.com.akadns.net, che a sua volta rimanda ad altri alias Akamai (CDN), fino ad arrivare al record **A** finale con l'indirizzo IP 23.60.188.118 (o simile in base alla geolocalizzazione della CDN).

```
▼ 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: 2]
[Time: 9.107178 milliseconds]
```

Descrizione: La sezione "Answers" espansa che mostra la catena di CNAME e l'indirizzo IP finale (Record A).

6. Conclusioni e Riflessioni sulla Sicurezza

Dall'analisi effettuata con Wireshark emerge quanto segue:

1. **Visibilità Totale:** Wireshark, operando in "promiscuous mode", permette di vedere chiaramente chi sta parlando con chi. Se il protocollo non è cifrato (come il DNS standard sulla porta 53), tutto è visibile in chiaro.
2. **Implicazioni di Sicurezza:** Un attaccante sulla stessa rete locale (LAN) potrebbe utilizzare Wireshark per eseguire attacchi di tipo **Man-In-The-Middle (MITM)** o semplice **Sniffing**. Vedendo le query DNS, l'attaccante può conoscere esattamente quali siti web sta visitando la vittima, profilandone le abitudini o preparando attacchi di **DNS Spoofing** (rispondendo con un IP falso prima del server reale) per reindirizzare l'utente su siti di phishing.