REPORT TECNICO

Analisi del Protocollo DNS con Wireshark

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: *18/02/2026*

Oggetto: Osservazione del traffico di rete e analisi delle query e risposte DNS

1. Introduzione

Il presente report documenta l'attività di analisi del traffico di rete volta all'osservazione del processo di risoluzione dei nomi di dominio tramite il protocollo DNS (**Domain Name System**).

L'attività è stata svolta utilizzando l'ambiente di virtualizzazione Kali Linux e gli strumenti di network sniffing. L'obiettivo principale dell'esercitazione è catturare ed esaminare i pacchetti generati tra un host client e un server DNS durante la risoluzione di un nome a dominio.

Per l'analisi dei pacchetti e dei datagrammi UDP, è stato impiegato lo strumento **Wireshark**. Nello specifico, l'analisi si concentra sulla struttura delle "Standard Query" e delle relative "Standard Query Response", verificando i dettagli del livello Applicazione e Trasporto.

2. Configurazione dell'ambiente di test e cattura del traffico

Per simulare e analizzare una richiesta di risoluzione nomi, è stato utilizzato il sistema operativo Kali Linux. Dalla console terminale, è stato utilizzato lo strumento '**nslookup**' per interrogare il server DNS predefinito riguardo il dominio "**www.cisco.com**".

Prima dell'esecuzione del comando, è stato avviato lo **sniffer Wireshark** in ascolto sull'interfaccia principale (eth0), al fine di intercettare l'intero scambio di pacchetti.

Il comando eseguito:

`nslookup www.cisco.com`

```
┌──(kali㉿kali)-[~]
└──(kali㉿kali)-[~]
└─$ nslookup www.cisco.com
Server:         10.0.2.3
Address:        10.0.2.3#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.ak
adns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net      canonical name = e2867.dsca.akamaie
dge.net.
Name:   e2867.dsca.akamaiedge.net
Address: 104.85.9.21
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d:a81::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d:a96::b33
```

Fig. 1 nslookup per interrogare il server DNS

Questa operazione ha innescato una richiesta DNS (Query) dal client verso il server DNS configurato e la conseguente ricezione dell'indirizzo IP associato.

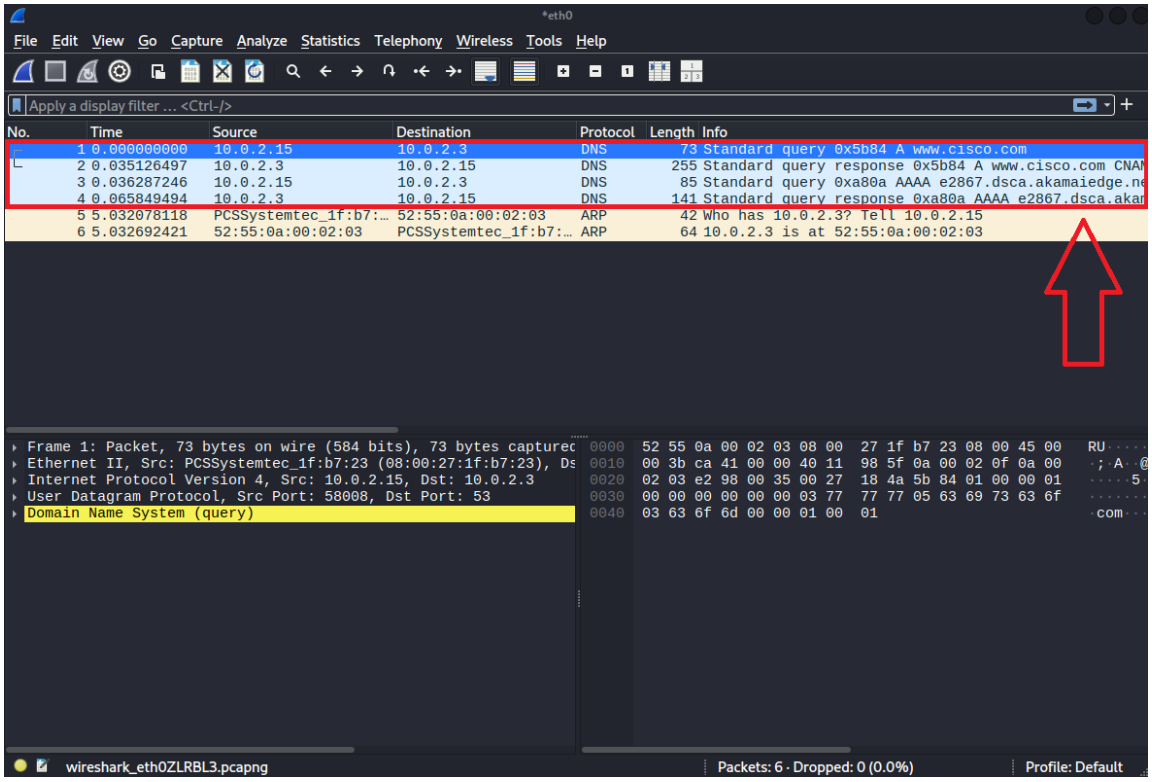

Fig. 2 cattura del traffico tramite sniffer Wireshark

3. Analisi del Traffico DNS

Approfondendo l'analisi al Livello di Trasporto, è stato verificato che la comunicazione DNS avviene tramite il protocollo UDP.

Questa scelta architetturale privilegia la velocità e la bassa latenza rispetto all'affidabilità garantita dal TCP, essendo la risoluzione dei nomi un'operazione che richiede risposte immediate.

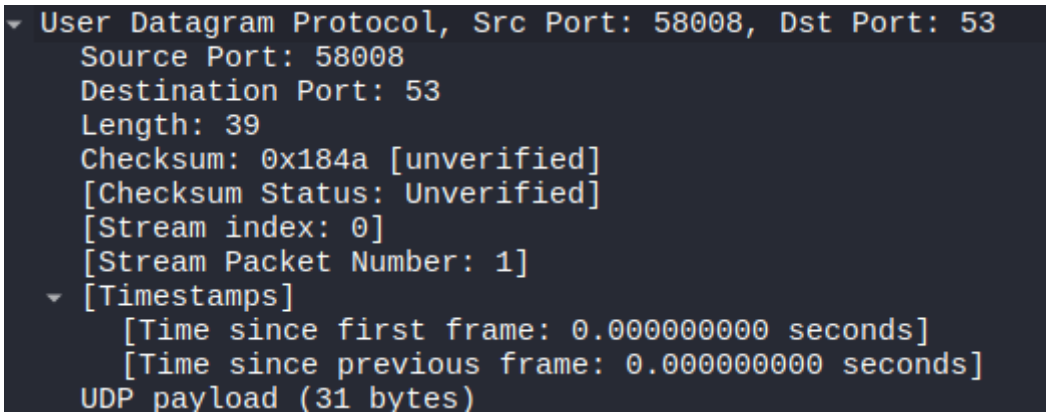

Fig. 3 User Datagram Protocol

Dallo screenshot si evidenziano le porte utilizzate per la sessione:

- **Destination Port**: 53. È la porta standard su cui il server DNS è in ascolto per ricevere le richieste.
- **Source Port**: 58008. È una porta effimera generata casualmente dal sistema operativo del client per gestire il ritorno della risposta.
- **Length**: Il payload UDP è di soli 39 bytes, confermando la leggerezza dell'header UDP rispetto a quello TCP.

3.1 Analisi della Richiesta (Query)

Isolando il traffico tramite il filtro '**udp.port == 53**', è stato identificato il primo pacchetto della sequenza: la Standard Query inviata dal client (**10.0.2.15**) al server DNS locale (**10.0.2.3**).

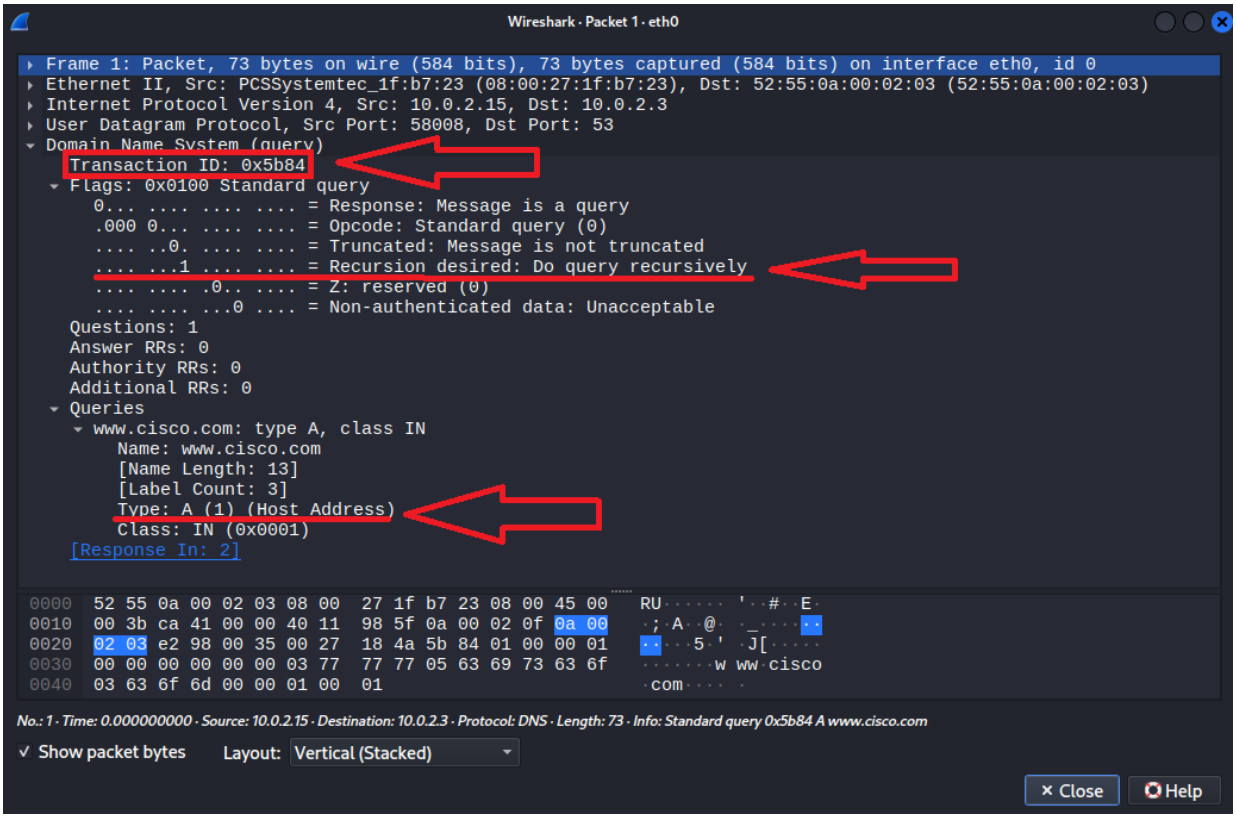

Fig. 4 Analisi della Query

Dall'analisi dei dettagli del pacchetto, si evidenziano i seguenti parametri nel livello Applicazione:

- **Transaction ID**: Un identificativo univoco utilizzato per correlare questa richiesta alla futura risposta.
- **Flags**: È stato osservato il flag "Recursion Desired" (RD) impostato a 1. Questo indica che il client richiede al server di risolvere completamente il nome, contattando se necessario altri server autoritativi.

- **Queries**: La sezione interroga specificamente il record di tipo "A" (Host Address) per il dominio "www.cisco.com", indicando la volontà di ottenere l'indirizzo IPv4 associato.

3.2 Analisi della Risposta (Response)

Il pacchetto successivo costituisce la risposta del server DNS.

L'associazione con la richiesta precedente è garantita dalla corrispondenza del **Transaction ID** (*0x5b84*).

Analizzando la sezione "**Answers**", si osserva che la risoluzione non è immediata, ma segue una catena di record **CNAME** (*Canonical Name*), tipica delle infrastrutture che utilizzano **Content Delivery Networks** (CDN) per il bilanciamento del carico.

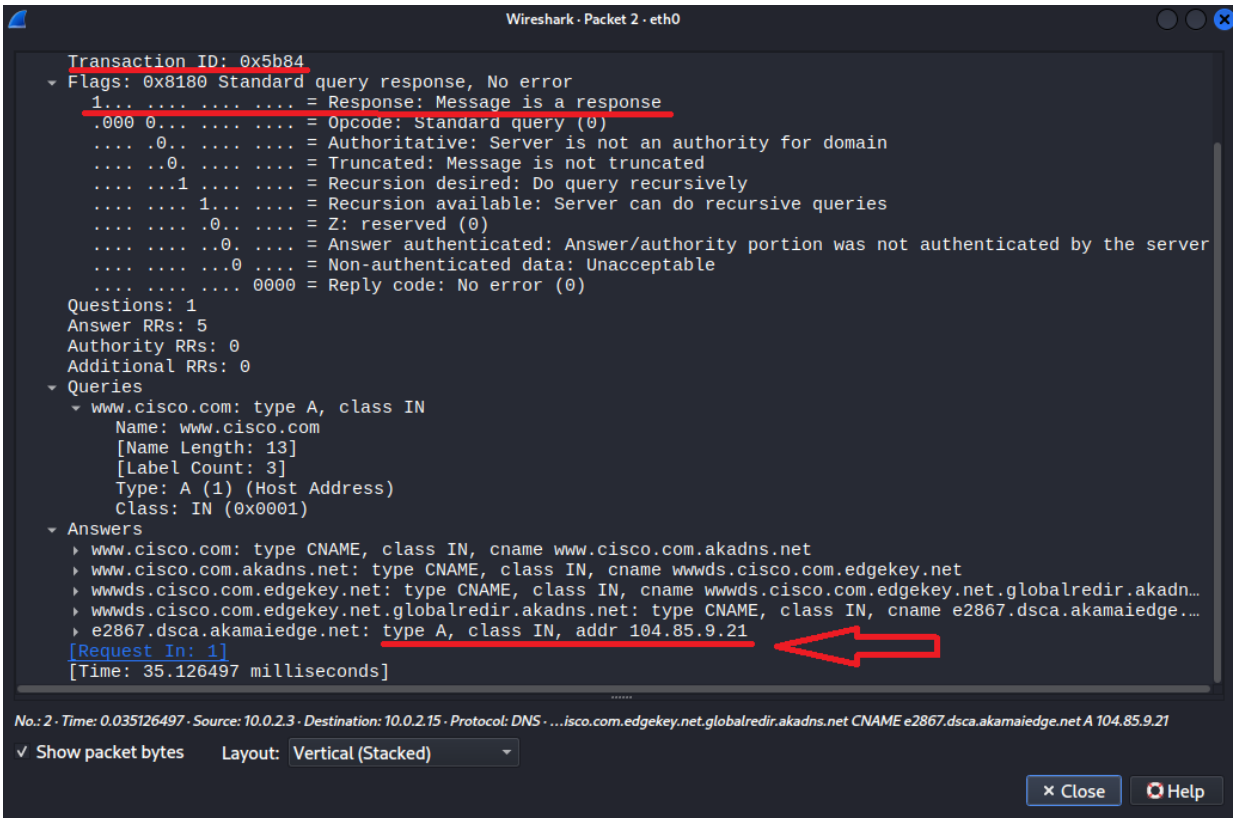

Fig. 5 Analisi della Response

La sequenza osservata è la seguente:

- www.cisco.com punta all'alias www.cisco.com.akadns.net.
- Quest'ultimo rimanda a ulteriori alias interni alla rete **Akamai**.
- Il processo termina con un record di tipo "A" che restituisce l'indirizzo IP pubblico finale (**104.85.9.21**), permettendo al client di stabilire la connessione.

3.3 Analisi del Traffico IPv6 (Pacchetti 3 e 4)

Oltre alla richiesta principale, abbiamo notato che il computer ha effettuato un secondo controllo simultaneo (Pacchetti 3 e 4).

Questa volta cercava un record di tipo "AAAA".

Mentre il record "A" visto prima serve a trovare l'indirizzo IP classico (**IPv4**), il record "AAAA" serve a trovare l'indirizzo di nuova generazione (**IPv6**).

- **Pacchetto 3** (Domanda): Il client chiede se il sito ha anche un indirizzo IPv6.
- **Pacchetto 4** (Risposta): Il server risponde di sì e fornisce questo indirizzo più lungo e complesso. Questo ci conferma che l'infrastruttura del sito è moderna e "parla" entrambi i linguaggi (sia il vecchio IPv4 che il nuovo IPv6).

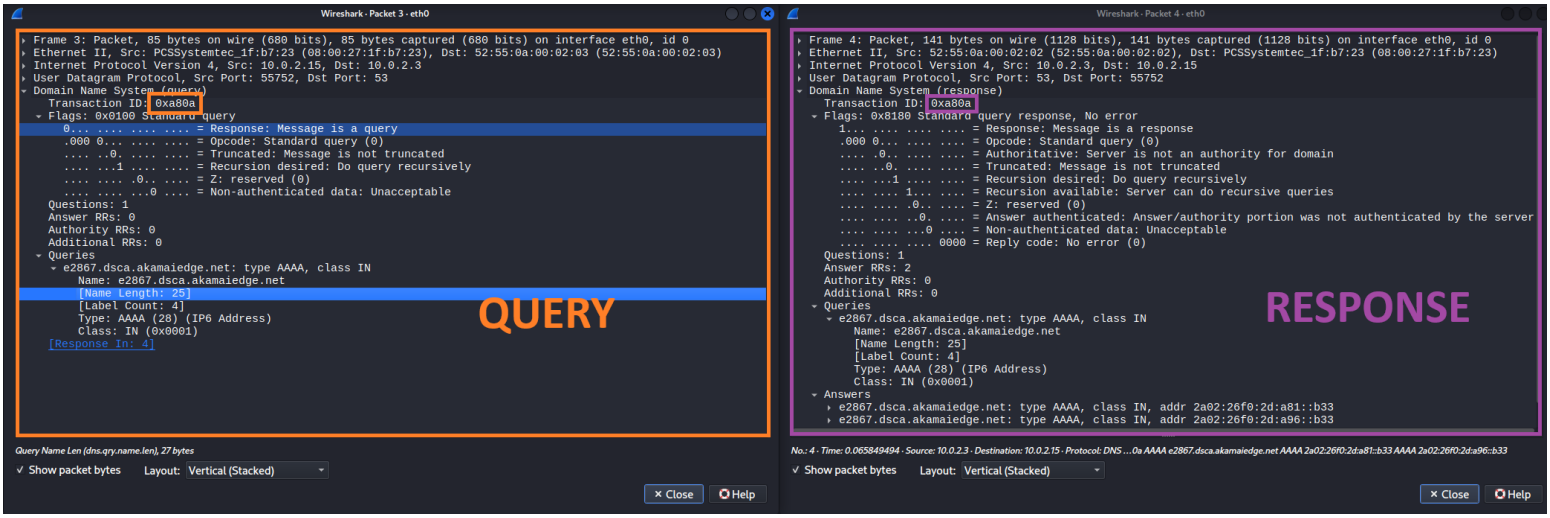

Fig. 6 Analisi del traffico IPv6

4. Conclusioni

L'attività di laboratorio ha permesso di osservare e analizzare nel dettaglio il funzionamento del protocollo DNS, confermando il suo ruolo critico nella traduzione dei nomi di dominio in indirizzi IP. L'utilizzo di Wireshark in ambiente Kali Linux ha reso possibile l'ispezione profonda dei pacchetti, evidenziando la struttura delle header, i flag di controllo e la logica delle risposte.

4.1 Risposte ai Quesiti di Analisi

Di seguito si riportano le risposte tecniche ai quesiti specifici posti dalla traccia di laboratorio:

- Quali sono gli indirizzi MAC di origine e destinazione? A quali interfacce di rete sono associati questi indirizzi MAC?

Risposta:

L'indirizzo MAC di origine: **08:00:27:1f:b7:23** è associato all'interfaccia di rete "eth0" della macchina virtuale Kali Linux

L'indirizzo MAC di destinazione: **52:55:0a:00:02:03** corrisponde all'interfaccia del Gateway predefinito della rete NAT, che agisce come server DNS per la risoluzione della richiesta.

- Quali sono gli indirizzi IP di origine e destinazione?

Risposta: L'indirizzo IP di origine è **10.0.2.15** (Client), mentre l'indirizzo IP di destinazione è **10.0.2.3** (Server DNS).

- Quali sono le porte di origine e destinazione? Qual è il numero di porta DNS predefinito?

Risposta: La porta di origine è una porta dinamica (effimera) allocata dal client, 58008. L porta di destinazione è la 53.

- Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione? Come si confrontano con gli indirizzi nei pacchetti di query DNS?

Risposta: Nel pacchetto di risposta, i ruoli si invertono speculari alla query:

1. IP Sorgente: 10.0.2.3 (Server) -> IP Destinazione: 10.0.2.15 (Client).
2. Porta Sorgente: 53 -> Porta Destinazione: 58008.

- Il server DNS può fare query ricorsive?

Risposta: Sì. L'analisi dei flag nel pacchetto di risposta (in particolare il flag "RA - Recursion Available") conferma che il server è configurato per supportare ed eseguire query ricorsive.

- Come si confrontano i risultati con quelli di nslookup?

Risposta: I risultati coincidono. Le sezioni "Answers" e "CNAME" visibili nel payload del pacchetto Wireshark corrispondono esattamente all'output testuale fornito dal comando 'nslookup', confermando la correttezza della cattura.

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

Risposta: Un attaccante all'interno della rete locale potrebbe utilizzare Wireshark in modalità promiscua per:

1. Effettuare ricognizione (**Reconnaissance**) mappando gli indirizzi IP e i servizi attivi.
2. Intercettare traffico non cifrato per sottrarre credenziali o informazioni sensibili (**Sniffing**).