Analisi del Traffico DNS mediante Wireshark

Introduzione

Il presente report documenta l'analisi del traffico di rete associato a una richiesta di risoluzione di nomi DNS (Domain Name System). L'obiettivo primario è stato osservare e interpretare i pacchetti scambiati tra un host client e un server DNS durante la risoluzione del nome a dominio www.cisco.com. L'analisi è stata condotta utilizzando il software Wireshark su un sistema operativo ParrotOS, concentrandosi sui protocolli a vari livelli dello stack ISO/OSI (Ethernet, IP, UDP) e sul protocollo applicativo DNS.

Acquisizione del Traffico DNS

Sul sistema operativo ParrotOS, è stato avviato lo strumento di analisi di rete Wireshark. È stata selezionata l'interfaccia di rete attiva, identificata come **enp0s3**. Per generare il traffico di interesse, è stata eseguita una query DNS specifica per il nome a dominio www.cisco.com attraverso un'utility da riga di comando (nslookup). Immediatamente dopo l'esecuzione della query, il processo di cattura su Wireshark è stato interrotto.

```
┌──[user@parrot]─[~]
└─$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.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net      canonical name = e2867.dsca.akamaiedge.net.
Name:   e2867.dsca.akamaiedge.net
Address: 23.32.112.103
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:8d00:c9e::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:8d00:ca9::b33
```

Esplorare il Traffico di Query DNS

udp.port == 53

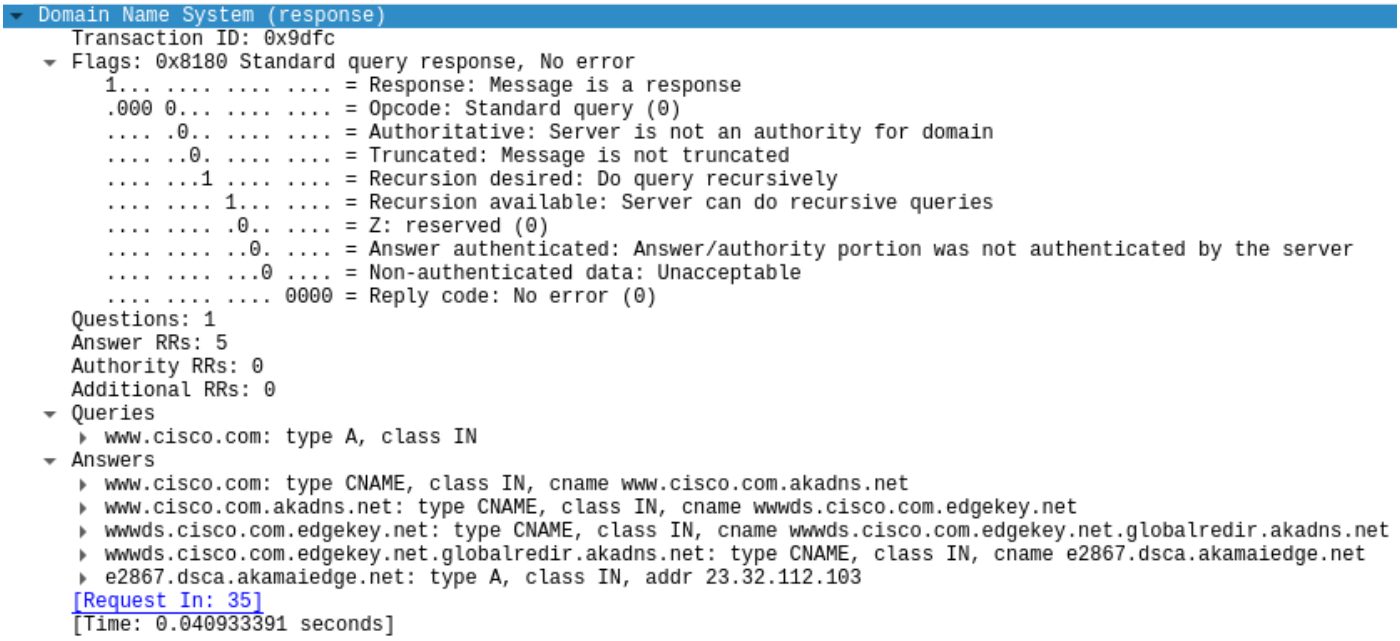
No.	Time	Source	Destination	Protocol	Length	Info
35	13.817530721	10.0.2.15	10.0.2.3	DNS	73	Standard query 0x9dfc A www.cisco.com
36	13.858464112	10.0.2.3	10.0.2.15	DNS	255	Standard query response 0x9dfc A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME ww
37	13.858913976	10.0.2.15	10.0.2.3	DNS	85	Standard query 0xdf32 AAAA e2867.dsca.akamaiedge.net
38	13.893366019	10.0.2.3	10.0.2.15	DNS	141	Standard query response 0xdf32 AAAA e2867.dsca.akamaiedge.net AAAA 2a02:26f0:8d00:c9e::b33 AAAA 2a02:26f0:8d00:ca9::b33

Passando all'analisi, l'attenzione si è rivolta al Frame 35, identificato da Wireshark come la richiesta DNS inviata dall'host locale ("Standard query" per "A www.cisco.com"). L'header Ethernet indicava l'indirizzo **MAC** dell'host (**08:00:27:c0:c9:68**) come sorgente e quello del gateway locale (**52:55:0a:00:02:03**) come destinazione. L'header IP confermava l'indirizzo IP dell'host **(10.0.2.15**) come sorgente e l'**IP** del server **DNS** interrogato (**10.0.2.3**) come destinazione. È stata verificata la coerenza di questi indirizzi sorgente (MAC e IP) con la configurazione effettiva dell'interfaccia **enp0s3** dell'host tramite il comando **ip a**, confermando l'origine del pacchetto.

```
enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
 link/ether 08:00:27:c0:c9:68 brd ff:ff:ff:ff:ff:ff
 inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
```

Esplorare il Traffico di Risposta DNS

Successivamente, è stato analizzato il Frame 36, che rappresentava la risposta del server DNS alla query precedente. Come previsto in una comunicazione client-server, gli indirizzi MAC, IP e le porte UDP di origine e destinazione erano invertiti rispetto alla query: la risposta proveniva dal server DNS (10.0.2.3, porta 53) ed era diretta all'host (10.0.2.15, porta 58202). I flag indicavano una risposta avvenuta con successo e confermavano la capacità del server di gestire richieste ricorsive, pur specificando di non essere il server autoritativo per il dominio cisco.com.



I risultati ottenuti da Wireshark, sono perfettamente coerenti con l'output che si ottiene da un semplice comando nslookup www.cisco.com.