

S11 – L3

Analisi del Traffico DNS con Wireshark (Kali Linux)

Introduzione

In questo esercizio ho **analizzato il traffico DNS generato da una macchina Kali Linux utilizzando Wireshark**. L’obiettivo è stato osservare e comprendere il **processo di risoluzione dei nomi di dominio**, esaminando nel dettaglio una query e la relativa risposta a livello dei protocolli Ethernet, IPv4, UDP e DNS. Attraverso il confronto con il comando **nslookup**, ho verificato la coerenza dei dati intercettati, approfondendo anche le implicazioni di sicurezza legate all’analisi del traffico di rete.

PARTE 1 — CATTURA DEL TRAFFICO

1.1 Avvio Wireshark e cattura

Passaggi operativi

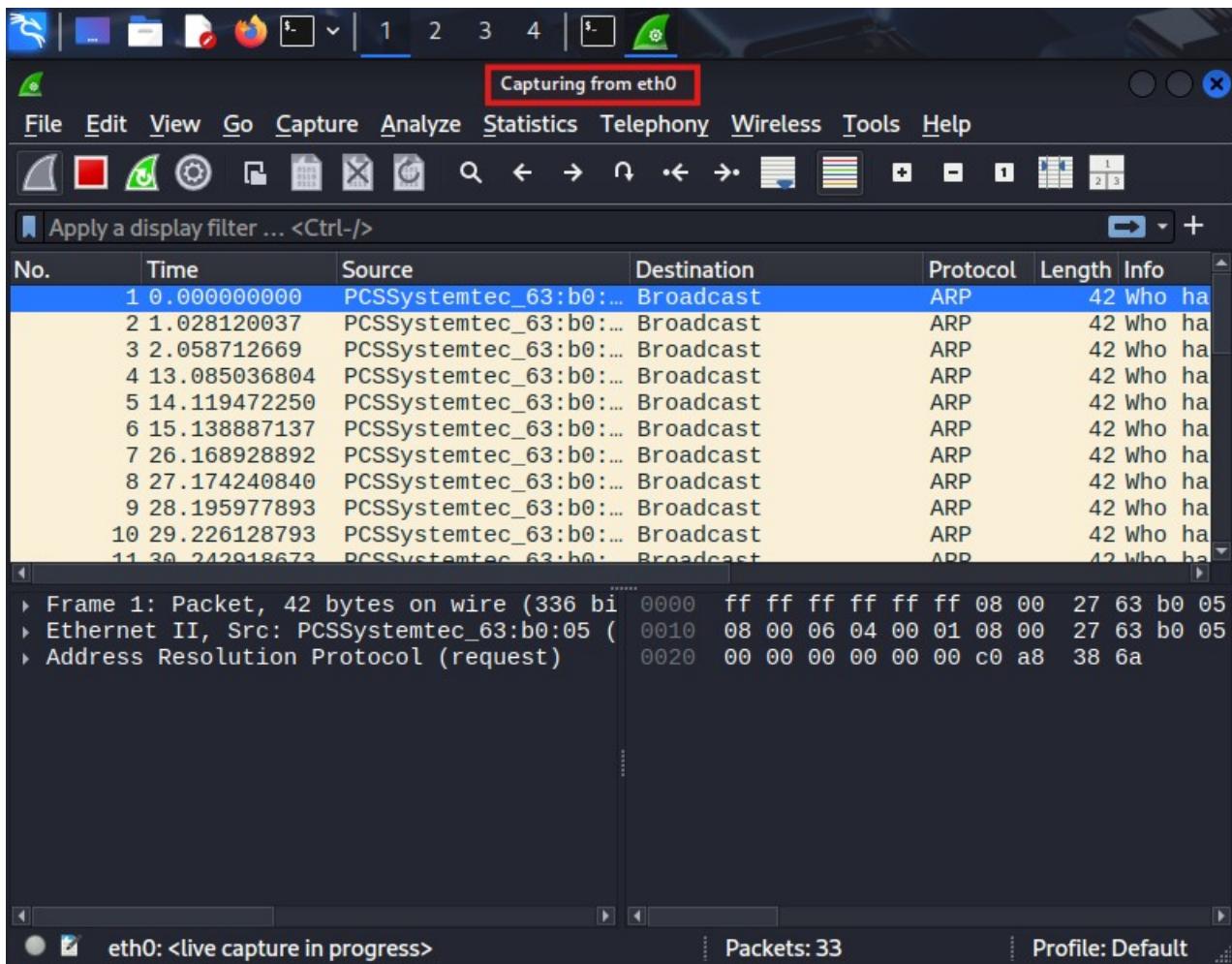
- Avvio Wireshark su Kali (**sudo wireshark**).
- Seleziono l’interfaccia attiva (**eth0/wlan0**).
- Avvio la cattura.
- Apro terminale e digito:

```
nslookup  
www.cisco.com  
exit
```

- Interrompo la cattura.

The screenshot shows a terminal session on a Kali Linux system. The user runs 'nslookup' to resolve 'www.cisco.com', which returns a non-authoritative answer with the canonical name 'www.cisco.com.akadns.net.'. Simultaneously, Wireshark is capturing traffic on the interface 'eth0'. The capture starts at 08:56:04.092209 and includes three DNS messages: a request from Wireshark to the local host, a response from the local host, and a file save operation for the captured traffic.

```
(kali㉿kali)-[~] $ sudo wireshark
** (wireshark:14751) 08:56:04.092209 [Capture MESSAGE] -- Capture Start ...
** (wireshark:14751) 08:56:04.136829 [Capture MESSAGE] -- Capture started
** (wireshark:14751) 08:56:04.136867 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0PSX0K3.pcap"
png"
File System Non-authoritative answer:
www.cisco.com canonical name = www.cisco.com.akadns.net.
```



Output:

Avvio di Wireshark su Kali Linux con selezione dell'interfaccia di rete attiva e cattura dei pacchetti in corso.

```
kali@kali: ~
Session Actions Edit View Help

[(kali㉿kali)-[~]
$ nsLookup
> www.cisco.com
[2209 [Capture MESSAGE] — Capture Start ...
Server: 8.8.8.8 [Capture MESSAGE] — Capture started
Address: 8.8.8.8#53 [Capture MESSAGE] — File: "/tmp/wireshark_eth0P5X0K3.pcap

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: 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
> exit
```

Output:

Esecuzione del comando nslookup per generare traffico DNS e verificare la risoluzione del dominio www.cisco.com.

PARTE 2 — ANALISI DELLA QUERY DNS

2.1 Filtro DNS

Applico filtro:

udp.port == 53

Seleziono il pacchetto:

Standard query A www.cisco.com

No.	Time	Source	Destination	Protocol	Length	Info
105	269.455562924	10.0.2.15	192.168.56.1	DNS	65	Standard query 0xe2b8 A clear
106	269.456456510	10.0.2.2	10.0.2.15	ICMP	93	Destination unreachable (Port unreachable)
107	269.456966750	10.0.2.15	192.168.56.1	DNS	65	Standard query 0xe2b8 A clear
108	269.457490574	10.0.2.2	10.0.2.15	ICMP	93	Destination unreachable (Port unreachable)
109	269.457704316	10.0.2.15	192.168.56.1	DNS	65	Standard query 0xe2b8 A clear
110	269.458400648	10.0.2.2	10.0.2.15	ICMP	93	Destination unreachable (Port unreachable)
111	269.458689923	10.0.2.15	8.8.8.8	DNS	65	Standard query 0xe2b8 A clear
112	269.575750141	8.8.8.8	10.0.2.15	DNS	140	Standard query response 0xe2b8 No such name A clear
113	354.794922934	10.0.2.15	8.8.8.8	DNS	73	Standard query 0xffffb6 A www.cisco.com
114	354.846289858	8.8.8.8	10.0.2.15	DNS	255	Standard query response 0xffffb6 A www.cisco.com CNAME
115	354.847930750	10.0.2.15	8.8.8.8	DNS	85	Standard query 0xf091 AAAA e2867.dsca.akamaiedge.net
116	354.8655801070	8.8.8.8	10.0.2.15	DNS	141	Standard query response 0xf091 AAAA e2867.dsca.akamaiedge.net

Output 1:

Applicazione del filtro **udp.port == 53** per isolare esclusivamente il traffico DNS.

Output 2:

Selezione del pacchetto DNS di tipo query relativo alla richiesta del dominio www.cisco.com.

I protocolli sono presenti nel frame sono:

Ethernet II, IPv4, UDP e DNS (Query).

2.2 Analisi Ethernet II

Domanda:

Quali sono gli indirizzi MAC di origine e destinazione?

Risposta:

Il MAC di origine è quello della macchina Kali (interfaccia eth0).

Il MAC di destinazione è quello del gateway della rete NAT.

Domanda:

A quali interfacce di rete sono associati questi indirizzi MAC?

Risposta:

Il MAC di origine è associato all'interfaccia di rete di Kali (eth0).

Il MAC di destinazione è associato all'interfaccia del router/gateway virtuale della rete.

2.3 Analisi IPv4

Espando “Internet Protocol Version 4

Domanda:

Quali sono gli indirizzi IP di origine e destinazione?

Risposta:

L'IP di origine è quello assegnato alla macchina Kali.

L'IP di destinazione è quello del server DNS configurato (es. 8.8.8.8 o il gateway).

Domanda:

A quali interfacce di rete sono associati questi indirizzi IP?

Risposta:

L'IP di origine è associato all'interfaccia di rete di Kali (eth0).

L'IP di destinazione è associato all'interfaccia del server DNS o del gateway che riceve la richiesta.

2.4 Analisi UDP

Domanda:

Quali sono le porte di origine e destinazione?

Risposta:

La porta di origine è una porta effimera assegnata dinamicamente al client (Kali).

La porta di destinazione è la porta 53 del server DNS.

Domanda:

Qual è il numero di porta DNS predefinito?

Risposta:

Il numero di porta DNS predefinito è **53 (UDP)**.

2.5 Confronto con il sistema

Comandi:

```
ip a  
ip link
```

Output:

Verifica degli indirizzi IP e MAC locali tramite comandi di sistema per confronto con i dati osservati in Wireshark.

Domanda:

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

Risposta:

Gli indirizzi IP e MAC visualizzati in Wireshark coincidono con quelli mostrati dai comandi di sistema (ip a / ip link). Questo conferma che il traffico DNS analizzato è stato effettivamente generato dalla macchina Kali e instradato verso il gateway/server DNS corretto.

Gli indirizzi MAC/IP corrispondono?

Sì, coincidono con quelli del sistema operativo.

2.6 Analisi DNS (Query)

Output:

Analisi del pacchetto DNS con verifica del flag Recursion Desired e del record di tipo A richiesto.

Domanda:

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

Risposta:

Nella risposta DNS, il MAC e l'IP di origine appartengono al server DNS, mentre quelli di destinazione appartengono alla macchina Kali.

La porta di origine è 53 e la porta di destinazione è la porta effimera usata nella query.

Domanda:

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

Risposta:

Rispetto alla query DNS, gli indirizzi MAC, IP e le porte risultano invertiti, come previsto in una comunicazione client-server.

Domanda:

Il server DNS può fare query ricorsive?

Risposta:

Sì, il server DNS supporta la ricorsione (flag Recursion Available = 1).

PARTE 3 — ANALISI DELLA RISPOSTA DNS

Output 1:

Selezione del pacchetto DNS di risposta proveniente dal server DNS.

Output 2:

Analisi della risposta DNS con inversione di indirizzi IP e porte rispetto alla query, tipica della comunicazione client-server.

Output 3:

Verifica del flag Recursion Available e analisi dei record DNS restituiti dal server.

Domanda:

Come si confrontano i risultati con quelli di nslookup?

Risposta::

I risultati osservati in Wireshark coincidono con quelli restituiti da **nslookup**. Gli indirizzi IP (record A) e gli eventuali CNAME visualizzati nella sezione **Answers** della risposta DNS corrispondono agli stessi valori mostrati dal comando **nslookup**, confermando la corretta risoluzione del dominio e la coerenza tra analisi del traffico e risultato applicativo.

PARTE 4 — RIFLESSIONE

Domanda:

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

Risposta:

Rimuovendo il filtro DNS è possibile osservare tutto il traffico di rete, come ARP, TCP/HTTPS, ICMP e altre comunicazioni tra dispositivi. Questo permette di identificare host presenti in rete, gateway, servizi attivi, pattern di traffico e possibili anomalie, offrendo una visione più completa della topologia e del funzionamento della rete.

Domanda:

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

Risposta:

Un attaccante può utilizzare Wireshark per effettuare attività di ricognizione, identificare dispositivi e servizi attivi, analizzare query DNS e intercettare traffico non cifrato. Può inoltre individuare informazioni sensibili trasmesse in chiaro e raccogliere dati utili per attacchi successivi, come spoofing o poisoning, compromettendo così la sicurezza della rete.

Conclusione finale:

L'esercizio ha consentito di **analizzare** in modo approfondito **il funzionamento del protocollo DNS a livello Ethernet, IPv4, UDP e DNS**, verificando la risoluzione del dominio, la ricorsione e la coerenza **tra Wireshark e nslookup**, comprendendo anche le implicazioni di sicurezza legate all'analisi del traffico.