

REPORT S11/L3

Cisco CyberOps 3

Traccia

Esplorazione del Traffico DNS

In questo laboratorio, completa i seguenti obiettivi:

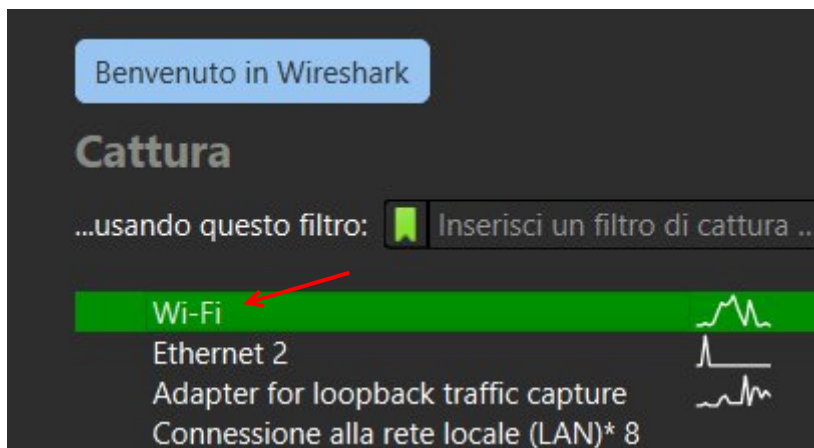
- Catturare il traffico DNS
- Esplorare il traffico delle query DNS
- Esplorare il traffico delle risposte DNS

Svolgimento

Wireshark è uno strumento di acquisizione e analisi di pacchetti open source. Consente di filtrare il traffico per la risoluzione dei problemi di rete, indagare sui problemi di sicurezza e analizzare i protocolli di rete. Poiché Wireshark ti consente di visualizzare i dettagli del pacchetto, può essere utilizzato come strumento di ricognizione per un utente malintenzionato.

Parte 1: Cattura il traffico DNS

Per catturare il traffico DNS con Wireshark avviamo il programma e selezioniamo un'interfaccia attiva con il traffico per l'acquisizione dei pacchetti.



Poi svuotiamo la cache dns tramite il comando **ipconfig /flushdns**

```
PS C:\Users\Alberto> ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.
PS C:\Users\Alberto> |
```

A questo punto avviamo la cattura dei pacchetti facendo doppio click sull'interfaccia scelta e contemporaneamente in una nuova finestra del terminale avviamo uno strumento utilizzato per interrogare server DNS (Domain Name System) e ottenere informazioni dettagliate riguardo ai nomi di dominio. Nel nostro caso questo strumento è **nslookup**, mentre il server (in questo caso sito) che prendiamo come esempio sarà **www.cisco.com**

```
PS C:\Users\Alberto> nslookup
Server predefinito:  UnKnown
Address:  2001:b07:aa7:e97a:7606:35ff:fe32:f3e0

> |
```

```
> www.cisco.com
Server:  UnKnown
Address:  2001:b07:aa7:e97a:7606:35ff:fe32:f3e0

Risposta da un server non autorevole:
Nome:      e2867.dsca.akamaiedge.net
Addresses: 2a02:26f0:8d00:ca9::b33
           2a02:26f0:8d00:c9e::b33
           23.209.77.25
Aliases:   www.cisco.com
           www.cisco.com.akadns.net
           wwwds.cisco.com.edgekey.net
           wwwds.cisco.com.edgekey.net.globalredir.akadns.net

>
```

I risultati che otteniamo così su Wireshark sono decine, pertanto applichiamo un filtro per concentrarci sui pacchetti di nostro interesse. Il filtro sarà: **udp.port == 53** e quelli che vediamo sono i pacchetti di nostro interesse.

udp.port == 53					
No.	Time	Source	Destination	Protocol	Length Info
112	22.110779	2001:b07:aa7:e97a:b...	2001:b07:aa7:e97a:7...	DNS	152 Standard query 0x0001 PTR 0.e.3.f.2.3.e.f.f.5.3.6.0.6.7.a.7.9.e.7.a.a.0.7.0.b.0.1.0.0.2.ip6.arpa
113	22.115547	2001:b07:aa7:e97a:7...	2001:b07:aa7:e97a:b...	DNS	152 Standard query response 0x0001 No such name PTR 0.e.3.f.2.3.e.f.f.5.3.6.0.6.7.a.7.9.e.7.a.a.0.7.0.b.0.1.0.0.2.ip6.arpa
252	74.379627	2001:b07:aa7:e97a:b...	2001:b07:aa7:e97a:7...	DNS	99 Standard query 0x0002 A www.cisco.com.nexxt
253	74.385081	2001:b07:aa7:e97a:7...	2001:b07:aa7:e97a:b...	DNS	99 Standard query response 0x0002 No such name A www.cisco.com.nexxt
254	74.385943	2001:b07:aa7:e97a:b...	2001:b07:aa7:e97a:7...	DNS	99 Standard query 0x0003 AAAA www.cisco.com.nexxt
255	74.389040	2001:b07:aa7:e97a:7...	2001:b07:aa7:e97a:b...	DNS	99 Standard query response 0x0003 No such name AAAA www.cisco.com.nexxt
256	74.389838	2001:b07:aa7:e97a:b...	2001:b07:aa7:e97a:7...	DNS	93 Standard query 0x0004 A www.cisco.com
257	74.403041	2001:b07:aa7:e97a:7...	2001:b07:aa7:e97a:b...	DNS	304 Standard query response 0x0004 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.com...
258	74.411358	2001:b07:aa7:e97a:b...	2001:b07:aa7:e97a:7...	DNS	93 Standard query 0x0005 AAAA www.cisco.com
259	74.421068	2001:b07:aa7:e97a:7...	2001:b07:aa7:e97a:b...	DNS	344 Standard query response 0x0005 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco...

Parte 1: Esplorare il traffico delle query DNS

Analizziamo ora in particolare il pacchetto che riporta la dicitura **Query standard** e **A www.cisco.com**

Offset	Length	Info
152	Standard query	0x0001 PTR 0.e.3.f.2.3.e.f.f.f.5
152	Standard query response	0x0001 No such name PTR
99	Standard query	0x0002 A www.cisco.com.nexxt
99	Standard query response	0x0002 No such name A w

Dal **Riquadro Dettaglio** in basso possiamo estrarre delle informazioni interessanti, soprattutto espandendo la voce **Ethernet II**.

```
▶ Frame 252: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{FEA70BE3-...}
▼ Ethernet II, Src: Intel_5b:c6:f6 (d4:f3:2d:5b:c6:f6), Dst: SernetTechno_32:f3:e0 (74:06:35:32:f3:e0)
  ▶ Destination: SernetTechno_32:f3:e0 (74:06:35:32:f3:e0)
  ▶ Source: Intel_5b:c6:f6 (d4:f3:2d:5b:c6:f6)
  Type: IPv6 (0x86dd)
  [Stream index: 0]
▶ Internet Protocol Version 6, Src: 2001:b07:aa7:e97a:b10a:9e27:5cce:57fd, Dst: 2001:b07:aa7:e97a:7606:35ff:fe32:f3e0
▶ User Datagram Protocol, Src Port: 52569, Dst Port: 53
▶ Domain Name System (query)
```

Nel nostro esempio, l'indirizzo MAC di origine è associato alla NIC sul PC e l'indirizzo MAC di destinazione è associato al gateway predefinito. Se è presente un server DNS locale, l'indirizzo MAC di destinazione sarebbe l'indirizzo MAC del server DNS locale.

Espandendo l'**Internet Protocol Version 6** possiamo estrarre gli indirizzi IP di origine e destinazione, che nel nostro caso sono indirizzi IPv6.

```
[Stream index: 0]
▼ Internet Protocol Version 6, Src: 2001:b07:aa7:e97a:b10a:9e27:5cce:57fd, Dst: 2001:b07:aa7:e97a:7606:35ff:fe32:f3e0
  0110 .... = Version: 6
  ▶ .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0001 1001 0101 0001 1001 = Flow Label: 0x19519
  Payload Length: 45
  Next Header: UDP (17)
  Hop Limit: 64
  ▶ Source Address: 2001:b07:aa7:e97a:b10a:9e27:5cce:57fd
  ▶ Destination Address: 2001:b07:aa7:e97a:7606:35ff:fe32:f3e0
  [Destination SLAAC MAC: SernetTechno_32:f3:e0 (74:06:35:32:f3:e0)]
  [Stream index: 6]
▶ User Datagram Protocol, Src Port: 52569, Dst Port: 53
```

Dallo **User Datagram Protocol** vediamo quali sono state le porte usate per questa comunicazione:

```
▼ User Datagram Protocol, Src Port: 52569, Dst Port: 53
  Source Port: 52569
  Destination Port: 53
  Length: 45
  Checksum: 0xe0a9 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 12]
  [Stream Packet Number: 1]
  ▶ [Timestamps]
  UDP payload (37 bytes)
```

Parte 3: Esplorare il traffico delle risposte DNS

Selezioniamo la risposta corrispondente che presenta **Standard query response** e **A** **www.cisco.com** nella colonna Informazioni.

Come ci potremmo aspettare adesso l'IP di origine, l'indirizzo MAC e il numero di porta nel pacchetto di query sono ora indirizzi di destinazione, mentre quello di destinazione, l'indirizzo MAC e il numero di porta nel pacchetto di query sono ora indirizzi di origine.

```
▶ Frame 252: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{FEA70BE3-
▶ Ethernet II, Src: Intel_5b:c6:f6 (d4:f3:2d:5b:c6:f6), Dst: SernetTechno_32:f3:e0 (74:06:35:32:f3:e0)
▶ Internet Protocol Version 6, Src: 2001:b07:aa7:e97a:b10a:9e27:5cce:57fd, Dst: 2001:b07:aa7:e97a:7606:35f
▶ User Datagram Protocol, Src Port: 52569, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0002
  ▼ 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.nexxt: type A, class IN
    [Response In: 253]
```