

Esplorazione del Traffico DNS

Obiettivi

Catturare il Traffico DNS.

Esplorare il Traffico delle Query DNS.

Esplorare il Traffico delle Risposte DNS.

Catturare il traffico DNS.

Per ottenere informazioni DNS si è utilizzato **nslookup**, un comando di rete utile per interrogare i server DNS.

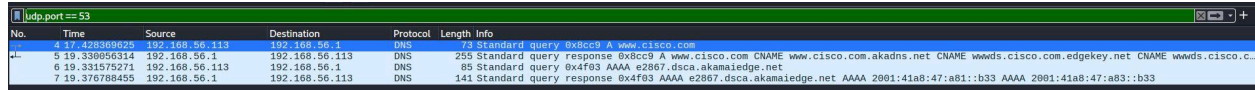
```
(kalivm@vboxkalivm)-[~]
$ nslookup
> www.cisco.com
Server:      192.168.56.1
Address:     192.168.56.1#53
Non-authoritative answer:
www.cisco.com canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net canonical 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: 104.85.9.21
Name:      e2867.dsca.akamaiedge.net
Address: 2001:41a8:47:a81::b33
Name:      e2867.dsca.akamaiedge.net
Address: 2001:41a8:47:a83::b33
>
```

Il comando è stato lanciato dopo aver aperto **Wireshark** con la Cache DNS pulita.

Una volta raccolti i pacchetti è stata interrotta la cattura di Wireshark, nel comando **nslookup** si è usciti con exit.

Esplorare il Traffico delle Query DNS.

Il filtro utilizzato per visualizzare i pacchetti DNS è stato **udp.port == 53**.



No.	Time	Source	Destination	Protocol	Length	Info
4	17.428369625	192.168.56.113	192.168.56.1	DNS	73	Standard query 0x8cc9 A www.cisco.com
5	19.33895314	192.168.56.1	192.168.56.113	DNS	255	Standard query response 0x8cc9 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.c...
6	19.331975271	192.168.56.113	192.168.56.1	DNS	85	Standard query 0x4f93 AAAA e2867.dsca.akamaiedge.net
7	19.376788455	192.168.56.1	192.168.56.113	DNS	141	Standard query response 0x4f93 AAAA e2867.dsca.akamaiedge.net AAAA 2001:41a8:47:a81::b33 AAAA 2001:41a8:47:a83::b33

Standard Query A.

E' una richiesta DNS per ottenere un record A.

Il record A restituisce l'indirizzo IPv4 di un dominio.

Sulla scheda **Ethernet II** è stato possibile vedere gli indirizzi MAC associati al pacchetto.

Quesiti.

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

1) Gli indirizzi MAC di origine è in questo caso:

08 : 00 : 27 : 1f : b0 : 09

Mentre di destinazione:

08 : 00 : 27 : 83 : 66 : 5a

```
▶ Frame 4: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
▶ Ethernet II, Src: PCSSystemtec_1f:b0:09 (08:00:27:1f:b0:09), Dst: PCSSystemtec_83:66:5a (08:00:27:83:66:5a)
  ▶ Destination: PCSSystemtec_83:66:5a (08:00:27:83:66:5a)
  ▶ Source: PCSSystemtec_1f:b0:09 (08:00:27:1f:b0:09)
  Type: IPv4 (0x0800)
  [Stream index: 2]
▶ Internet Protocol Version 4, Src: 192.168.56.113, Dst: 192.168.56.1
▶ User Datagram Protocol, Src Port: 45767, Dst Port: 53
▶ Domain Name System (query)
```

2) Gli indirizzi MAC in questione sono associati alla mia interfaccia di rete su VBox.

Su **Internet Protocol Version 4** è stato possibile visualizzare gli indirizzi **IPv4**.

Quesiti.

- 1) Quali sono gli indirizzi IP di origine e destinazione?**
- 2) A quali interfacce di rete sono associati questi indirizzi IP?**

```
Source Address: 192.168.56.113  
Destination Address: 192.168.56.1  
[Stream index: 0]
```

- 1) L'indirizzo IP di origine in questo caso è 192.168.56.113, mentre quello di destinazione è 192.168.56.1.
- 2) Gli indirizzi IP in questione sono associati alla mia interfaccia di rete.

Su **User Datagram Protocol** è possibile visualizzare i pacchetti UDP intercettati.

Quesiti.

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

```
▼ User Datagram Protocol, Src Port: 45767, Dst Port: 53  
  Source Port: 45767  
  Destination Port: 53  
  Length: 39  
  Checksum: 0xf1fb [unverified]  
  [Checksum Status: Unverified]  
  [Stream index: 0]  
  [Stream Packet Number: 1]  
  ▶ [Timestamps]  
  UDP payload (31 bytes)  
  Domain Name System (query)
```

- 1) La porta di origine è la 45767 mentre quella di destinazione la porta 53, la stessa che riporta al secondo quesito, legata al numero di porta predefinita per il DNS.

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

E' stato lanciato il comando **ifconfig** per visualizzare gli indirizzi MAC e IP su Kali.

```
(kalivm@vboxkalivm)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.56.113 netmask 255.255.255.0 broadcast 192.168.56.255  
    inet6 fe80::a6f:6796:bb9c:1843 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:1f:b0:09 txqueuelen 1000 (Ethernet)  
    RX packets 3  bytes 456 (456.0 B)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 32  bytes 3412 (3.3 KiB)  
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Come detto prima, riportano alle informazioni rilevate su Wireshark, infatti l'IPv4 è lo stesso rilevato in **Internet Protocol Version 4** e l'indirizzo MAC lo stesso trovato in **Ethernet II** come indirizzo MAC di origine.

Esplorare il Traffico delle Risposte DNS

Standard query response A.

Questo pacchetto mostra la risposta ad una richiesta DNS.

Quesiti.

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

```
Ethernet II, Src: PCSSystemtec_83:66:5a (08:00:27:83:66:5a), Dst: PCSSyst
  Destination: PCSSystemtec_1f:b0:09 (08:00:27:1f:b0:09)
  Source: PCSSystemtec_83:66:5a (08:00:27:83:66:5a)
  Type: IPv4 (0x0800)
  [Stream index: 2]
Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.113
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 241
  Identification: 0x7ab0 (31408)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
```

- 1) L'indirizzo MAC di origine è 08 : 00 : 27 : 83 : 66 : 5a, mentre l'IP di origine è 192.168.56.1

```
Source Address: 192.168.56.1
Destination Address: 192.168.56.113
```

- 2) L'indirizzo IP e l'indirizzo MAC di destinazione del pacchetto di richiesta sono diventati gli indirizzi di origine del pacchetto di risposta e viceversa.

Il server DNS può fare query ricorsive?

```
Queries
  www.cisco.com: type A,
  e2867.dsca.akamaiedge.net: type A, class IN, addr 104.85.9.21
  Request ID: 41
```

Sì, il server DNS può effettuare query responsive con record A.

Come si confrontano i risultati con quelli di nslookup?

```
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: 2001:41a8:47:a81::b33
Name: e2867.dsca.akamaiedge.net
Address: 2001:41a8:47:a83::b33
> exit
```

Confrontando i risultati di nslookup con quelli ottenuti da Wireshark si nota che l'indirizzo IP e il dominio di risposta è lo stesso.

Riflessione

- 1) **Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?**
- 2) **Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?**

- 1) Rimosso il filtro DNS, si possono vedere dispositivi e IP attivi, il tipo di traffico utilizzato, richieste e risposte DNS complete ed eventuali informazioni sui dispositivi.
- 2) Un attaccante potrebbe usare WireShark per eseguire uno sniffing del traffico, mappare la rete, visualizzare richieste DNS e catturare dati sensibili con attacchi **ARP poisoning** e **DCHP spoofing**, effettuando quindi attacchi **MITM** (Man-In-The-Middle).