Esplorazione del Traffico DNS

S11L3

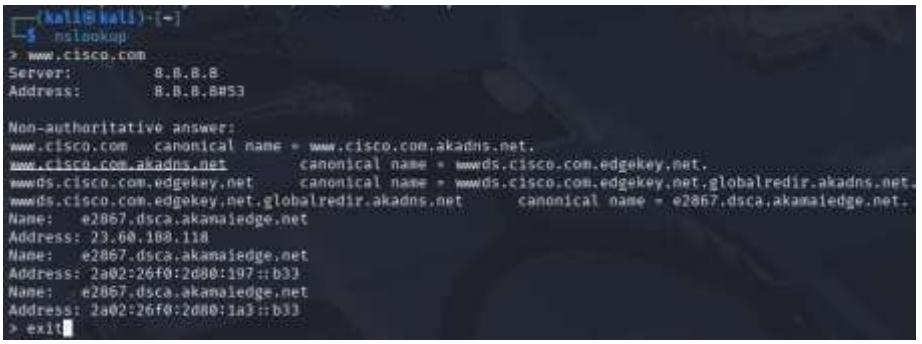
Obiettivi

- Parte 1↵ Catturare il Traffico DNS
- Parte 2↵ Esplorare il Traffico delle Query DNS
- Parte 3↵ Esplorare il Traffico delle Risposte DNS

PRIMO PASSO

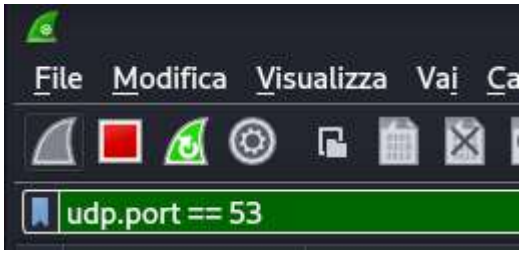
La traccia mi chiede di installare Wireshark, ma avendolo già installato su kali linux userò quello, quindi, procediamo.

Da qui apro un prompt dei comandi , digito **nslookup** per entrare in modalità interattiva. Ho messo il nome di dominio di un sito web, ovvero, www.cisco.com. Exit quando ho finito.



SECONDO PASSO

Ho usato il filro udp.port==53



Seleziono questo log

Domande:

Quali sono gli indirizzi MAC di origine e destinazione?

08:00:27:5c:2a:38(di origine), 08:00:27:50:d3:70(destinazione)

A quali interfacce di rete sono associati questi indirizzi MAC?

Internet protocol verson 4

Quali sono gli indirizzi IP di origine e destinazione?

```
Src: 192.168.200.100, Dst: 8.8.8.8
```

A quali interfacce di rete sono associati questi indirizzi IP?

Gli indirizzi IP sono associati alla mia interfaccia di rete

Quali sono le porte di origine e destinazione?

```
▸ User Datagram Protocol,
    Source Port: 60669
    Destination Port: 53
    Length: 39
```

La porta di origine è 60669, porta destinazione 53

Qual è il numero di porta DNS predefinito?

Sempre la porta 53

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

Lanciando il comando "ifconfig" sul terminale di kali vediamo quello che ha rilevato Wireshark intercettando tutti i pacchetti.

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.200.100  netmask 255.255.255.0  broadcast 192.168.200.255
        inet6 fe80::e8d1:3766:fd69:f407  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:2a:38  txqueuelen 1000  (Ethernet)
        RX packets 450544  bytes 665674344 (634.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 185110  bytes 13504989 (12.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1080 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1080 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.200.1            ether   08:00:27:50:d3:70   C                     eth0
```

TERZO PASSO

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

Mac:

```
Ethernet II, Src: PCSSystemtec_5c:2a:38 (08:00:27:5c:2a:3
▸ Destination: PCSSystemtec_50:d3:70 (08:00:27:50:d3:70)
▸ Source: PCSSystemtec_5c:2a:38 (08:00:27:5c:2a:38)
```

IP:

```
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 8.8.8.8
```

Ecco qui, come avevo gia detto prima

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

Sono inversi rispetto a prima, con la risposta del DNS sta andando nel verso giusto collegando correttamente il protocollo DNS

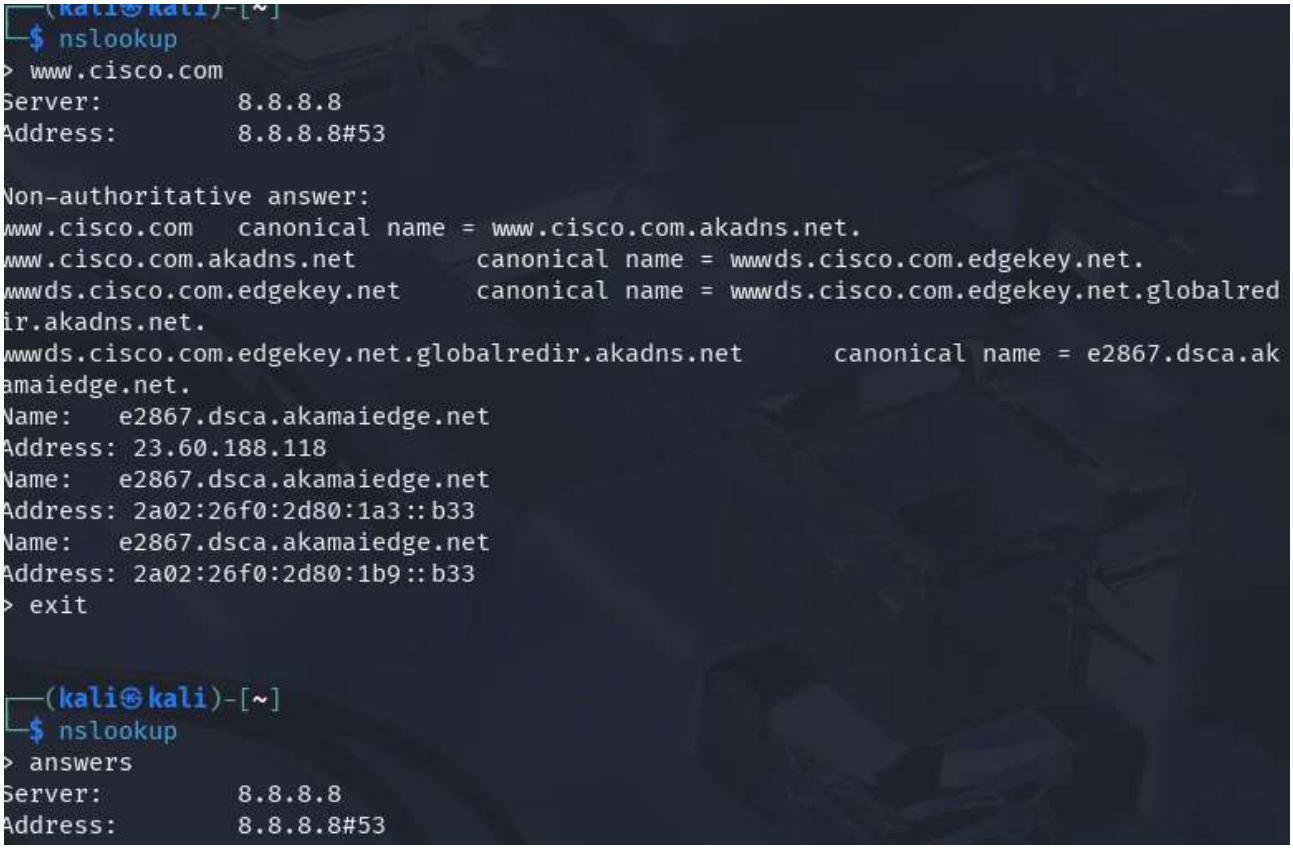
Il server DNS può fare query ricorsive?

Sì, posso fare query ricorsive

```
▾ 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: type A, class IN
      Name: www.cisco.com
```

Come si confrontano i risultati con quelli di nslookup?

La stessa di prima



RIFLESSIONE

1. Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?
   Se tolgo il filtro su Wireshark, vedo tutto il traffico della rete, ogni pacchetto che passa, e se ci sono problemi, con chi parla. Quindi potremmo avere una visione completa.

2. Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?
   Se sono un attaccante lo userei per spiare la rete. Posso idati personali se non sono protetti, anche capire come è fatta la tua rete per trovare punti deboli. È uno strumento molto utile e potente per capire tutto ciò che passa sulla rete.