Esercizio.

Preparazione CyberOps.

Passo 1: Installare Wireshark

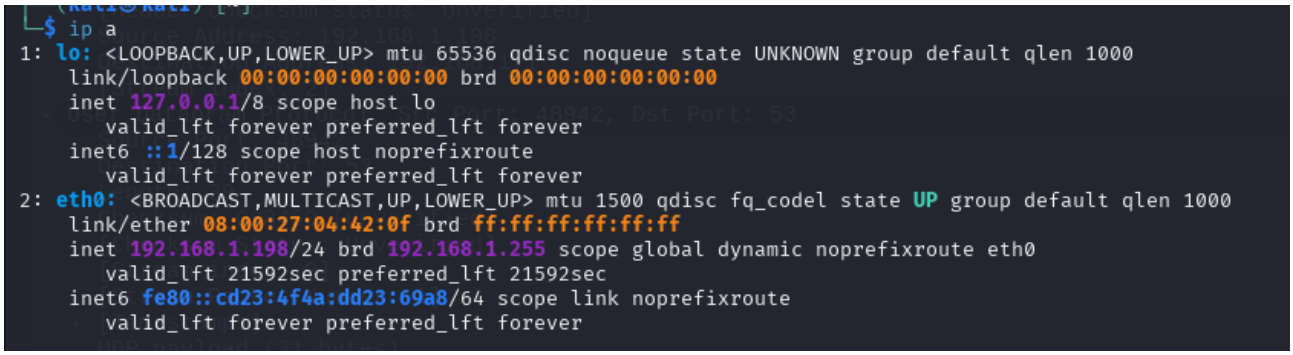
Passo 2: Catturare il traffico DNS

1) Pulire la cache DNS e catturare i pacchetti.

Parte 2: Esplorare il Traffico delle Query DNS.

Inserire udp.port == 53 nella casella del filtro e fare clic sulla freccia (o premere invio) per visualizzare solo i pacchetti DNS.

1) **Quali sono gli indirizzi MAC di origine e destinazione?** L'indirizzo MAC d'origine è 08:00:27:04:42:0f l'indirizzo di destinazione è d4:35:1d:d0:b2:4d.
2) **A quali interfacce di rete sono associati questi indirizzi MAC?** Eth0
3) **Quali sono gli indirizzi IP di origine e destinazione?** L'IP d'origine è 192.168.1.198 mentre l'IP di destinazione è 192.168.1.1
4) **A quali interfacce di rete sono associati questi indirizzi IP?** Eth0
5) **Quali sono le porte di origine e destinazione?** La porta di origine è 48942 mentre la porta di destinazione è 53.
6) **Qual è il numero di porta DNS predefinito?** Il numero di porta DNS predefinito è la 53.
7) **Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?**



Vedo che gli indirizzi MAC e IP sono uguali agli indirizzi d'origine della richiesta DNS.

PARTE 3: Esplorare il Traffico delle Risposte DNS

Selezionare il corrispondente pacchetto DNS di risposta che ha Standard query response e A www.cisco.com nella colonna Info.

8) **Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?**
   Indirizzi MAC e IP d'origine e porta d'origine: d4:35:1d:d0:b2:4d - 192.168.1.1 - 53
   Indirizzi MAC e IP e porta di destinazione: 08:00:27:04:42:0f - 192.168.1.198 - 48942
9) **Come si confrontano con gli indirizzi nei pacchetti di query DNS?** Nella query gli indirizzi e le porte erano invertiti.
10) **Il server DNS può fare query ricorsive?** Sì

```
.... ...1 .... .... = Recursion desired: Do query recursively
.... .... 1... .... = Recursion available: Server can do recursive queries
```

11) **Come si confrontano i risultati con quelli di nslookup?**

```
Queries
  www.cisco.com: type A, class IN
Answers
  www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
  www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
  wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
  wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
  e2867.dsca.akamaiedge.net: type A, class IN, addr 23.49.196.116
```

```
┌──(kali㉿kali)-[~]
└─$ nslookup
> www.cisco.com
Server:         192.168.1.1
Address:        192.168.1.1#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: 23.49.196.116
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:8d00:cb6::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:8d00:c9e::b33
> exit
```

Wireshark mostra il traffico di rete in generale e il contenuto del pacchetto della risposta DNS mentre nslookup permette di interrogare in modo specifico i server DNS, verificare la propagazione dei record e capire la struttura del sistema DNS.

Riflessione.

12) **Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?**
   Wireshark ha catturato un'analisi topologica di alcuni dispositivi della rete e il traffico della rete.
13) **Come può un attaccante compromettere la sicurezza della tua rete?** Un attaccante ottenute le informazioni sull'ambiente di rete potrebbe iniziare ad effettuare scansioni per vedere se i dispositivi connessi hanno delle porte aperte o servizi vulnerabili.