RISPOSTE

-Quali sono gli indirizzi MAC di origine e destinazione?

Destination 52:55:c0:a8:0a:01

Source 08:00:27:63:b0:05

-A quali interfacce di rete sono associati questi indirizzi MAC?

Interfaccia di rete eth0 (MAC)

-Quali sono gli indirizzi IP di origine e destinazione?

Destination 192.168.1.1

Source 192.168.10.4

-A quali interfacce di rete sono associati questi indirizzi IP?

Interfaccia di rete eth0 (RETE)

-Quali sono le porte di origine e destinazione?

Destination port 53

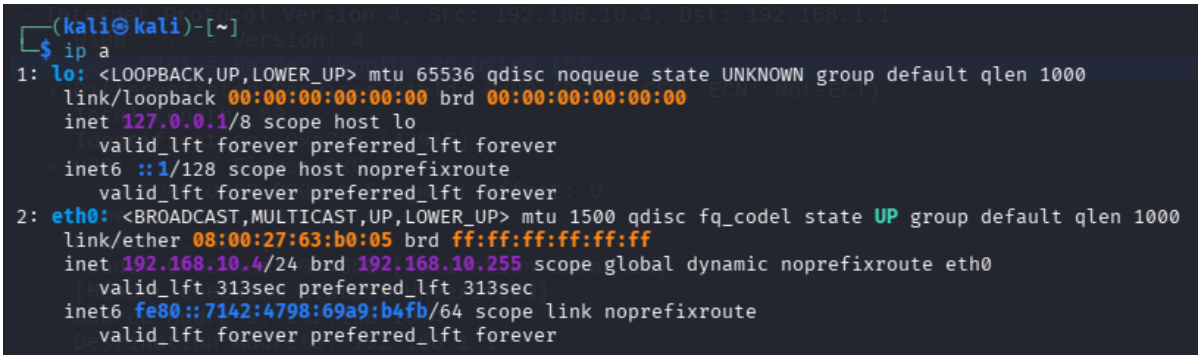
Source port 46841

-Qual è il numero di porta DNS predefinito?

La porta predefinita per il DNS è 53

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

Sono uguali



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

Destination 08:00:27:63:b0:05

Source 52:55:c0:a8:0a:01

Destination IP 192.168.10.4

Source IP 192.168.1.1

Destination port 46841

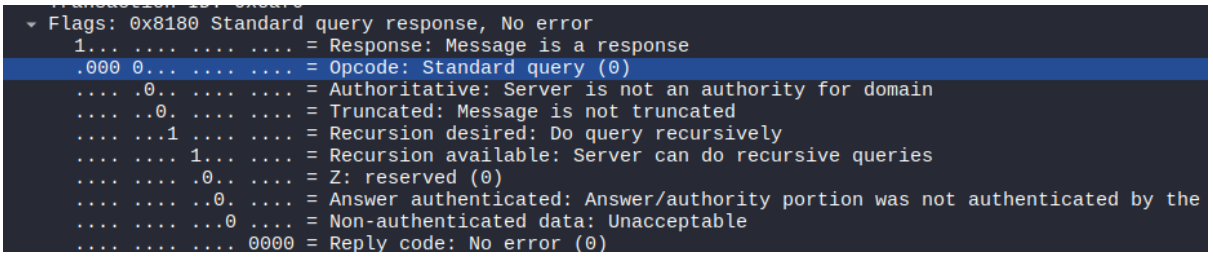
Source port 53

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

Gli indirizzi e le porte sono invertiti rispetto alla query(il destinatario diventa la sorgente e la sorgente diventa destinatario)

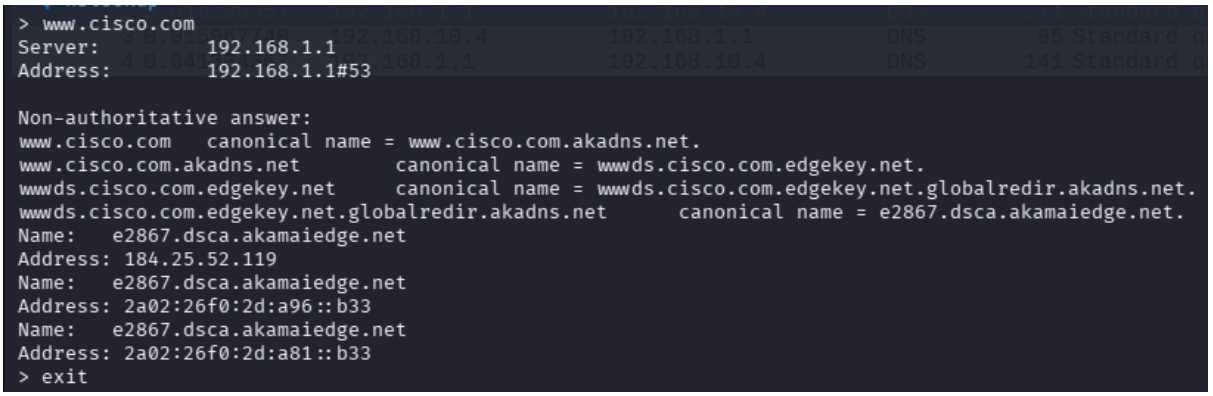
-Il server DNS può fare query ricorsive?

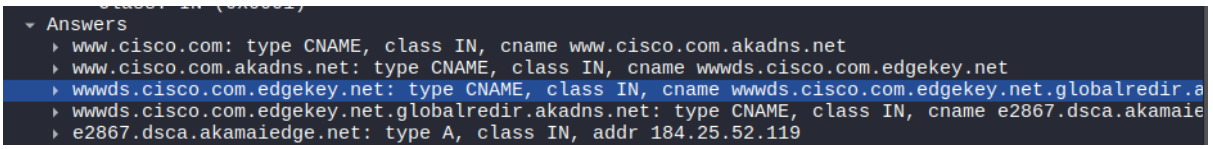
si



-Come si confrontano i risultati con quelli di nslookup?

Sono uguali sia in answer sia in nslookup





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

Se si rimuove il filtro si vede tutti i pacchetti in background, si vede anche L'ARP, DHCP, DNS, ecc.

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

Intercettazione in chiaro

Se un utente accede a siti o servizi che non usano la crittografia (come HTTP, FTP o Telnet invece di HTTPS, SFTP o SSH), un attaccante può vedere nomi utente e password leggendo semplicemente il contenuto dei pacchetti.

Ricognizione della rete (Sniffing)

Analizzando il traffico, un malintenzionato può mappare l'intera infrastruttura:

- **Individuazione dispositivi:** Capire quanti PC, server e smartphone sono connessi.
- **Sistemi Operativi:** Identificare se usi Windows, Linux o iOS (tramite i campi TTL o le stringhe User-Agent).
- **Vulnerabilità:** Scoprire quali versioni di software stai usando. Se vede traffico da un software obsoleto, cercherà un "exploit" specifico per quel programma.