

## 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

```
(kali㉿kali)-[~] $ ip a
 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
      inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
      inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:63:b0:05 brd ff:ff:ff:ff:ff:ff
      inet 192.168.10.4/24 brd 192.168.10.255 scope global dynamic noprefixroute eth0
        valid_lft 313sec preferred_lft 313sec
      inet6 fe80::7142:4798:69a9:b4fb/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

**-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

```
Flags: 0x8180 Standard query response, No error
      1... = Response: Message is a response
      .000 0... = Opcode: Standard query (0)
      ....0 = Authoritative: Server is not an authority for domain
      ....0 = Truncated: Message is not truncated
      ....1 = Recursion desired: Do query recursively
      ....1.. = Recursion available: Server can do recursive queries
      ....0.. = Z: reserved (0)
      ....0.. = Answer authenticated: Answer/authority portion was not authenticated by the
      ....0.. = Non-authenticated data: Unacceptable
      ....0000 = Reply code: No error (0)
```

-Come si confrontano i risultati con quelli di nslookup?

Sono uguali sia in answer sia in nslookup

```
> www.cisco.com      192.168.1.1      192.168.10.4      DNS      271 Standard q
Server: 192.168.1.1      192.168.1.1      192.168.10.4      DNS      85 Standard q
Address: 4 0.0.0.1#53 192.168.1.1#53 192.168.10.4      DNS      141 Standard q

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: 184.25.52.119
Name: e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d:a96::b33
Name: e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d:a81::b33
> exit
```

```
  ↳ www.cisco.com.akadns.net: 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: type CNAME, class IN, cname e2867.dsca.akamaiaedge.net: type A, class IN, addr 184.25.52.119
```

-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.