

Relazione Esplorazione Traffico DNS

Nella prima immagine utilizzo il comando specifico per l'interrogazione del **Server DNS** e per la richiesta delle informazioni specifiche su un certo Dominio, in questo caso Vodafone, e successivamente con il comando specifico mi metto in ascolto sulla porta che voglio scansionare con **Wireshark** come illustrato di seguito:

- **nslookup vodafone.com**
- **sudo tcpdump -i eth0 port 53**

```
(kali@kali)-[~]
$ nslookup vodafone.com

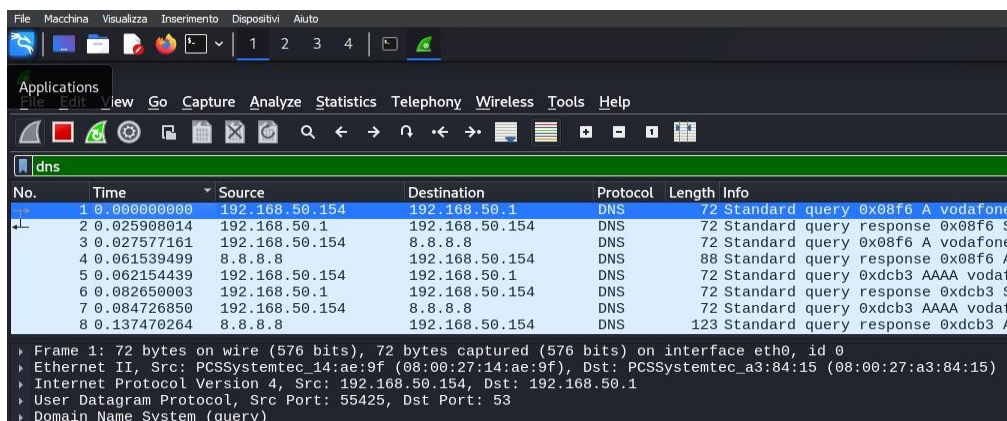
;; Got SERVFAIL reply from 192.168.50.1, trying next server
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   vodafone.com
Address: 147.75.40.150
;; Got SERVFAIL reply from 192.168.50.1, trying next server
```

```
(kali@kali)-[~]
$ sudo tcpdump -i eth0 port 53

[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:59:58.374096 IP 192.168.50.154.38960 > pfSense.home.arpa.domain: 54770+ A? contile.services.mozilla.com. (46)
08:59:58.374155 IP 192.168.50.154.38960 > pfSense.home.arpa.domain: 4851+ AAAA? contile.services.mozilla.com. (46)
08:59:58.429382 IP pfSense.home.arpa.domain > 192.168.50.154.38960: 54770 ServFail 0/0/0 (46)
08:59:58.430476 IP pfSense.home.arpa.domain > 192.168.50.154.38960: 4851 ServFail 0/0/0 (46)
08:59:58.430732 IP 192.168.50.154.36571 > dns.google.domain: 54770+ A? contile.services.mozilla.com. (46)
08:59:58.430789 IP 192.168.50.154.36571 > dns.google.domain: 4851+ AAAA? contile.services.mozilla.com. (46)
08:59:58.440348 IP 192.168.50.154.58548 > pfSense.home.arpa.domain: 48098+ PTR? 1.50.168.192.in-addr.arpa. (43)
08:59:58.441091 IP pfSense.home.arpa.domain > 192.168.50.154.58548: 48098* 1/0/0 PTR pfSense.home.arpa. (70)
08:59:58.441250 IP 192.168.50.154.53454 > pfSense.home.arpa.domain: 57040+ PTR? 154.50.168.192.in-addr.arpa. (45)
08:59:58.441922 IP pfSense.home.arpa.domain > 192.168.50.154.53454: 57040 NXDomain* 0/1/0 (104)
08:59:58.443266 IP 192.168.50.154.48397 > pfSense.home.arpa.domain: 17952+ PTR? 8.8.8.8.in-addr.arpa. (38)
08:59:58.468545 IP dns.google.domain > 192.168.50.154.36571: 54770 1/0/0 A 34.117.188.166 (62)
08:59:58.468546 IP dns.google.domain > 192.168.50.154.36571: 4851 0/1/0 (127)
```

Dopo aver utilizzato il comando illustrato e descritto in precedenza, utilizzo il comando nel filtro di ricerca di **Wireshark**, per ricercare il traffico specifico di rete **DNS (Domain Name System)**, come illustrato di seguito:



Nella prossima immagine e passaggio sul tool di cattura di rete Wireshark, sempre nel filtro di ricerca, scrivo il comando per il solo traffico di rete DNS e come illustrato di seguito, seleziono riga (blue scuro), la **Standard query (www.google.com)**

- **udp.port == 53**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.154	192.168.50.1	DNS	72	Standard query 0x08f6 A Vodafone.com
2	0.025900014	192.168.50.1	192.168.50.154	DNS	72	Standard query response 0x08f6 Server
3	0.027577161	192.168.50.154	8.8.8.8	DNS	72	Standard query 0x08f6 A Vodafone.com
4	0.061539499	8.8.8.8	192.168.50.154	DNS	88	Standard query response 0x08f6 A Vodafone.com
5	0.062154439	192.168.50.154	192.168.50.1	DNS	72	Standard query 0xdc3 AAAA Vodafone.com
6	0.082650003	192.168.50.1	192.168.50.154	DNS	72	Standard query response 0xdc3 Server
7	0.084726850	192.168.50.154	8.8.8.8	DNS	72	Standard query 0xdc3 AAAA Vodafone.com
8	0.137470264	8.8.8.8	192.168.50.154	DNS	123	Standard query response 0xdc3 AAAA Vodafone.com
14	1462.5343525	192.168.50.154	192.168.50.1	DNS	74	Standard query 0xbc34 A www.google.com
17	1462.5678518	192.168.50.1	192.168.50.154	DNS	74	Standard query response 0xbc34 Server
18	1462.5688353	192.168.50.154	8.8.8.8	DNS	74	Standard query 0xbc34 A www.google.com
19	1462.5705260	8.8.8.8	192.168.50.154	DNS	90	Standard query response 0xbc34 A www.google.com
20	1462.5709115	192.168.50.154	192.168.50.1	DNS	74	Standard query 0x6ef3 AAAA www.google.com
21	1462.6135067	192.168.50.1	192.168.50.154	DNS	74	Standard query response 0x6ef3 Server
22	1462.6142138	192.168.50.154	8.8.8.8	DNS	74	Standard query 0x6ef3 AAAA www.google.com
23	1462.6512431	8.8.8.8	192.168.50.154	DNS	102	Standard query response 0x6ef3 AAAA www.google.com

Nel prossimo passaggio ed immagine, clicco ed espando la voce **Ethernet II** nel quale posso visualizzare tutti i dettagli della comunicazione, e nello specifico, campi di origine e di destinazione.

Nel seguente passaggio l'indirizzo MAC sorgente viene associato alla NIC sul PC e l'indirizzo MAC della destinazione viene associato al Gateway predefinito.

Se è presente un Server DNS locale, l'indirizzo MAC di destinazione sarebbe l'indirizzo MAC del server DNS locale.

```

▼ Ethernet II, Src: PCSSystemtec_a3:84:15 (08:00:27:a3:84:15), Dst: PCSSystemtec_14:ae:9f (08:00:27:14:ae:9f)
  ▼ Destination: PCSSystemtec_14:ae:9f (08:00:27:14:ae:9f)
    Address: PCSSystemtec_14:ae:9f (08:00:27:14:ae:9f)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
  ▼ Source: PCSSystemtec_a3:84:15 (08:00:27:a3:84:15)
    Address: PCSSystemtec_a3:84:15 (08:00:27:a3:84:15)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)

```

Dopo aver analizzato la scheda **Ethernet II**, vado ad analizzare, espandendo, la scheda **Internet Protocol Version 4**, nel quale posso notare che l'indirizzo **IP sorgente** (di origine) viene associato alla scheda di rete del mio PC, e l'indirizzo **IP di destinazione**, viene associato al Gateway predefinito, come possiamo vedere di seguito:

```
▼ Internet Protocol Version 4, Src: 192.168.50.154, Dst: 192.168.50.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xfef0 (65264)
  ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x95d4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.50.154
    Destination Address: 192.168.50.1
  ▼ User Datagram Protocol, Src Port: 58623, Dst Port: 53
    Source Port: 58623
    Destination Port: 53
    Length: 40
    Checksum: 0xe625 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  ▶ [Timestamps]
    UDP payload (32 bytes)
```

Nella seguente immagine dopo aver analizzato nei dettagli **Internet Protocol Version 4** possiamo notare la **Source Port: 58623** e come visto in precedenza e come agito prima, tramite specifico comando per l'ascolto su una determinata porta: **53 (Destination Port)**, come illustrato di seguito:

```
▼ User Datagram Protocol, Src Port: 58623, Dst Port: 53
  Source Port: 58623
  Destination Port: 53
  Length: 40
  Checksum: 0xe625 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  ▶ [Timestamps]
    UDP payload (32 bytes)
```

Successivamente all'analisi effettuata sulla **Source Port (58623)** e la **Destination Port (53)**, posso notare nell'analisi del Domain Name System, che il flag delle query è settato per un'interrogazione ricorsiva sull'indirizzo www.google.com, come possiamo notare di seguito:

```
Domain Name System (query)
Transaction ID: 0xbc34
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.google.com: type A, class IN
  [Response In: 17]
```

Nella seguente immagine vado ad identificare il traffico di risposta del DNS con il comando specifico che mi restituisca la risposta:

- `dns.flags.response == 1`

