Esplorazione del Traffico DNS

L'obiettivo del laboratorio è comprendere e analizzare il traffico DNS generato dal sistema attraverso strumenti di monitoraggio come Wireshark e tcpdump.
Il traffico DNS include sia le query inviate dal client che le risposte ricevute dal server DNS.

Cattura del traffico DNS

Wireshark
Avvio Wireshark con privilegi di root.
Seleziono l'interfaccia di rete attiva (`eth0` o `wlan0`).
Applico il filtro `udp.port == 53` per catturare solo pacchetti DNS.
Genero traffico DNS con il comando `nslookup www.google.com` e navigo su siti web.

tcpdump
Utilizzo il comando:
sudo tcpdump -i eth0 udp port 53 -w traffico_dns.pcap
per salvare il traffico DNS in un file `.pcap`.

Analisi in Wireshark

Applico il filtro:
dns.flags.response == 0
per visualizzare solo le query DNS.

Osservo i dettagli delle richieste:
- Dominio richiesto: `www.google.com`.
- Tipo di query: `A` (per IPv4) e `AAAA` (per IPv6).
- Server DNS contattato: `8.8.8.8` (Google DNS).

Le query vengono generate correttamente e inoltrate al server DNS configurato.

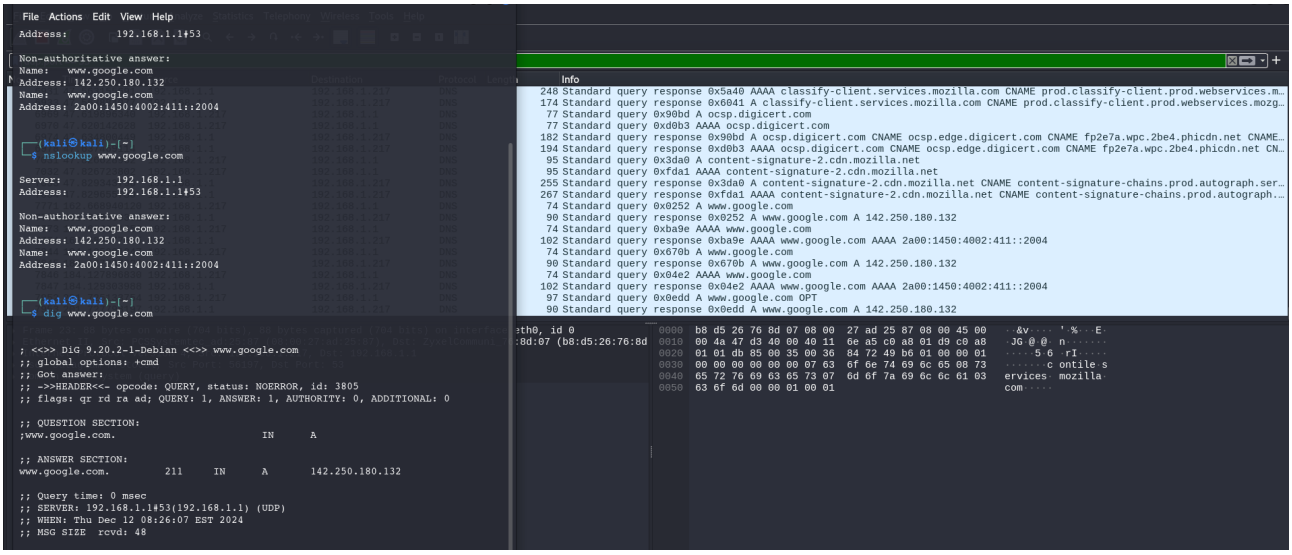
Esplorazione delle risposte DNS

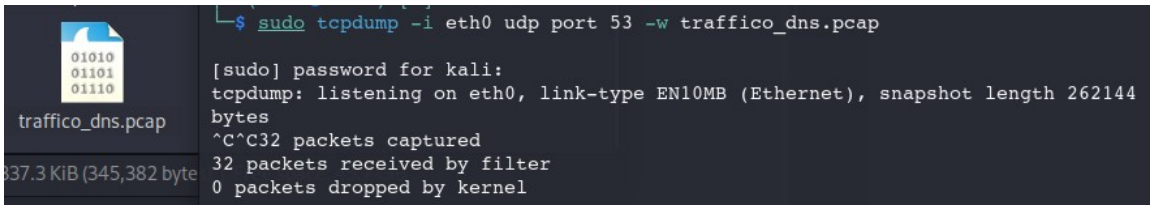
Applico il filtro:
dns.flags.response == 1
per visualizzare solo le risposte DNS.

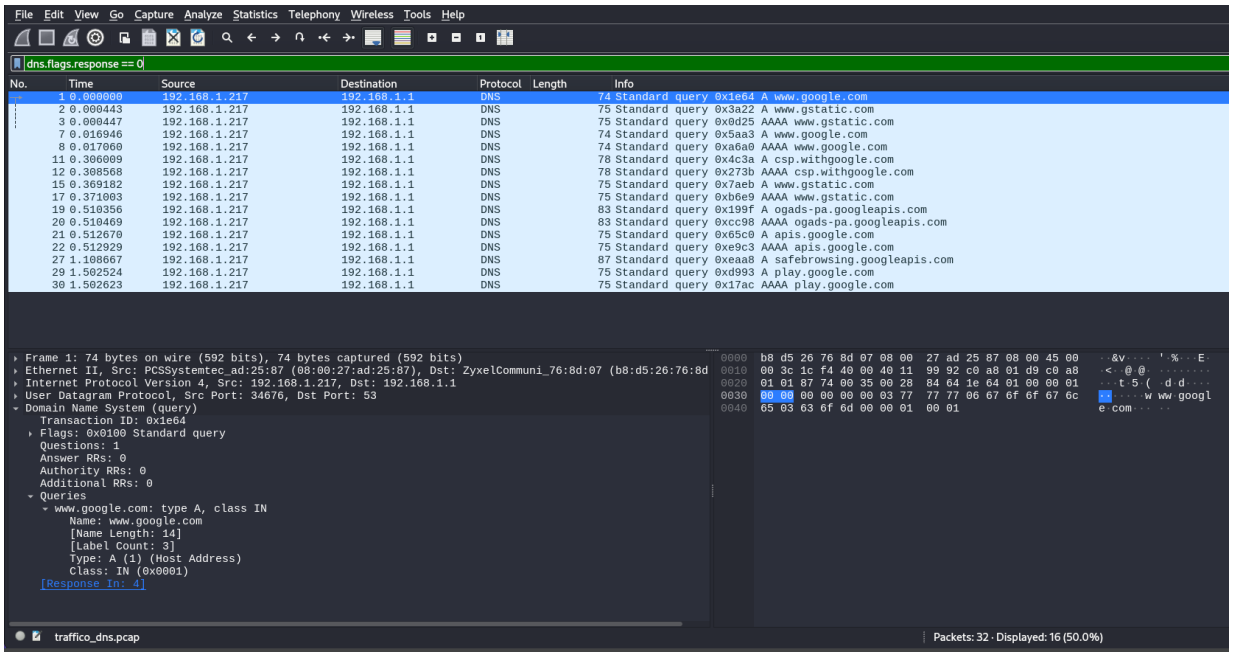
Analizzo i dettagli delle risposte:
- Indirizzo IP restituito: per `www.google.com`, ricevo un indirizzo IPv4 valido (es. `142.250.74.68`).
- Time-to-Live (TTL): i valori tipici variano tra 300 e 600 secondi.
- Dominio non trovato: per domini inesistenti osservo l'errore `NXDOMAIN`.

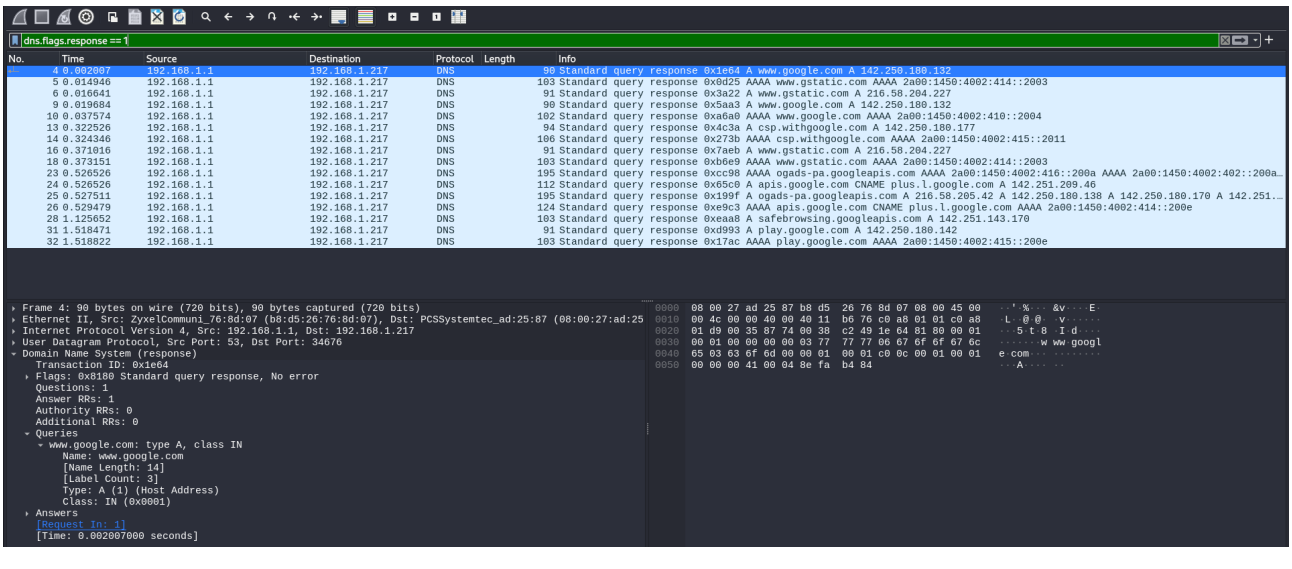
Il server DNS risponde correttamente alle richieste valide.
Gli errori vengono gestiti correttamente per domini non esistenti.

L'esplorazione del traffico DNS dimostra l'importanza del protocollo DNS nella risoluzione dei nomi di dominio.
Questo laboratorio mi fornisce competenze pratiche nell'uso di strumenti di analisi come Wireshark e tcpdump, utili per monitorare e diagnosticare il traffico di rete.


File Actions Edit View Help
Address: 192.168.1.1#53
Non-authoritative answer:
Name: www.google.com
Address: 142.250.180.132
Name: www.google.com
Address: 2a00:1450:4002:411::2004
(kali㉿kali)-[~]
$ nslookup www.google.com
Server: 192.168.1.1
Address: 192.168.1.1#53
Non-authoritative answer:
Name: www.google.com
Address: 142.250.180.132
Name: www.google.com
Address: 2a00:1450:4002:411::2004
(kali㉿kali)-[~]
$ dig www.google.com
; <<>> DiG 9.20.2-1-Debian <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3805
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.google.com. IN A
;; ANSWER SECTION:
www.google.com. 211 IN A 142.250.180.132
;; Query time: 0 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Thu Dec 12 08:26:07 EST 2024
;; MSG SIZE rcvd: 48
Info
248 Standard query response 0x5a40 AAAA classify-client.services.mozilla.com CNAME prod.classify-client.prod.webservices.m…
174 Standard query response 0x6041 A classify-client.services.mozilla.com CNAME prod.classify-client.prod.webservices.mozg…
77 Standard query 0x90bd A ocsp.digicert.com
77 Standard query 0xd0b3 AAAA ocsp.digicert.com
182 Standard query response 0x90bd A ocsp.digicert.com CNAME ocsp.edge.digicert.com CNAME fp2e7a.wpc.2be4.phicdn.net CNAME…
194 Standard query response 0xd0b3 AAAA ocsp.digicert.com CNAME ocsp.edge.digicert.com CNAME fp2e7a.wpc.2be4.phicdn.net CN…
95 Standard query 0x3da0 A content-signature-2.cdn.mozilla.net
95 Standard query 0xfda1 AAAA content-signature-2.cdn.mozilla.net
255 Standard query response 0x3da0 A content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.autograph.ser…
267 Standard query response 0xfda1 AAAA content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.autograph.…
74 Standard query 0x0252 A www.google.com
90 Standard query response 0x0252 A www.google.com A 142.250.180.132
74 Standard query 0xba9e AAAA www.google.com
102 Standard query response 0xba9e AAAA www.google.com AAAA 2a00:1450:4002:411::2004
74 Standard query 0x670b A www.google.com
90 Standard query response 0x670b A www.google.com A 142.250.180.132
74 Standard query 0x04e2 AAAA www.google.com
102 Standard query response 0x04e2 AAAA www.google.com AAAA 2a00:1450:4002:411::2004
97 Standard query 0x0edd A www.google.com OPT
90 Standard query response 0x0edd A www.google.com A 142.250.180.132
eth0, id 0
:8d:07 (b8:d5:26:76:8d
0000 b8 d5 26 76 8d 07 08 00 27 ad 25 87 08 00 45 00 ··&v···· '·%···E·
0010 00 4a 47 d3 40 00 40 11 6e a5 c0 a8 01 d9 c0 a8 ·JG·@·@· n·····
0020 01 01 db 85 00 35 00 36 84 72 49 b6 01 00 00 01 ·····5·6 ·rI·····
0030 00 00 00 00 00 00 07 63 6f 6e 74 69 6c 65 08 73 ·······c ontile·s
0040 65 72 76 69 63 65 73 07 6d 6f 7a 69 6c 6c 61 03 ervices· mozilla·
0050 63 6f 6d 00 00 01 00 01 com·····


traffico_dns.pcap
337.3 KiB (345,382 byte
$ sudo tcpdump -i eth0 udp port 53 -w traffico_dns.pcap
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C^C32 packets captured
32 packets received by filter
0 packets dropped by kernel


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.flags.response == 0
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.217 192.168.1.1 DNS 74 Standard query 0x1e64 A www.google.com
2 0.000443 192.168.1.217 192.168.1.1 DNS 75 Standard query 0x3a22 A www.gstatic.com
3 0.000447 192.168.1.217 192.168.1.1 DNS 75 Standard query 0x0d25 AAAA www.gstatic.com
7 0.016946 192.168.1.217 192.168.1.1 DNS 74 Standard query 0x5aa3 A www.google.com
8 0.017060 192.168.1.217 192.168.1.1 DNS 74 Standard query 0xa6a0 AAAA www.google.com
11 0.306009 192.168.1.217 192.168.1.1 DNS 78 Standard query 0x4c3a A csp.withgoogle.com
12 0.308568 192.168.1.217 192.168.1.1 DNS 78 Standard query 0x273b AAAA csp.withgoogle.com
15 0.369182 192.168.1.217 192.168.1.1 DNS 75 Standard query 0x7aeb A www.gstatic.com
17 0.371003 192.168.1.217 192.168.1.1 DNS 75 Standard query 0xb6e9 AAAA www.gstatic.com
19 0.510356 192.168.1.217 192.168.1.1 DNS 83 Standard query 0x199f A ogads-pa.googleapis.com
20 0.510469 192.168.1.217 192.168.1.1 DNS 83 Standard query 0xcc98 AAAA ogads-pa.googleapis.com
21 0.512670 192.168.1.217 192.168.1.1 DNS 75 Standard query 0x65c0 A apis.google.com
22 0.512929 192.168.1.217 192.168.1.1 DNS 75 Standard query 0xe9c3 AAAA apis.google.com
27 1.108667 192.168.1.217 192.168.1.1 DNS 87 Standard query 0xeaa8 A safebrowsing.googleapis.com
29 1.502524 192.168.1.217 192.168.1.1 DNS 75 Standard query 0xd993 A play.google.com
30 1.502623 192.168.1.217 192.168.1.1 DNS 75 Standard query 0x17ac AAAA play.google.com
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: ZyxelCommuni_76:8d:07 (b8:d5:26:76:8d
Internet Protocol Version 4, Src: 192.168.1.217, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 34676, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x1e64
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.google.com: type A, class IN
Name: www.google.com
[Name Length: 14]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
[Response In: 4]
0000 b8 d5 26 76 8d 07 08 00 27 ad 25 87 08 00 45 00 ··&v···· '·%···E·
0010 00 3c 1c f4 40 00 40 11 99 92 c0 a8 01 d9 c0 a8 ·<··@·@· ········
0020 01 01 87 74 00 35 00 28 84 64 1e 64 01 00 00 01 ···t·5·(·d·d····
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c ·······w ww·googl
0040 65 03 63 6f 6d 00 00 01 00 01 e·com····
traffico_dns.pcap
Packets: 32 · Displayed: 16 (50.0%)


dns.flags.response == 1
No. Time Source Destination Protocol Length Info
4 0.002007 192.168.1.1 192.168.1.217 DNS 90 Standard query response 0x1e64 A www.google.com A 142.250.180.132
5 0.014946 192.168.1.1 192.168.1.217 DNS 103 Standard query response 0x0d25 AAAA www.gstatic.com AAAA 2a00:1450:4002:414::2003
6 0.016641 192.168.1.1 192.168.1.217 DNS 91 Standard query response 0x3a22 A www.gstatic.com A 216.58.204.227
9 0.019684 192.168.1.1 192.168.1.217 DNS 90 Standard query response 0x5aa3 A www.google.com A 142.250.180.132
10 0.037574 192.168.1.1 192.168.1.217 DNS 102 Standard query response 0xa6a0 AAAA www.google.com AAAA 2a00:1450:4002:410::2004
13 0.322526 192.168.1.1 192.168.1.217 DNS 94 Standard query response 0x4c3a A csp.withgoogle.com A 142.250.180.177
14 0.324346 192.168.1.1 192.168.1.217 DNS 106 Standard query response 0x273b AAAA csp.withgoogle.com AAAA 2a00:1450:4002:415::2011
16 0.371016 192.168.1.1 192.168.1.217 DNS 91 Standard query response 0x7aeb A www.gstatic.com A 216.58.204.227
18 0.373151 192.168.1.1 192.168.1.217 DNS 103 Standard query response 0xb6e9 AAAA www.gstatic.com AAAA 2a00:1450:4002:414::2003
23 0.526526 192.168.1.1 192.168.1.217 DNS 195 Standard query response 0xcc98 AAAA ogads-pa.googleapis.com AAAA 2a00:1450:4002:416::200a AAAA 2a00:1450:4002:402::200a…
24 0.526526 192.168.1.1 192.168.1.217 DNS 112 Standard query response 0x65c0 A apis.google.com CNAME plus.l.google.com A 142.251.209.46
25 0.527511 192.168.1.1 192.168.1.217 DNS 195 Standard query response 0x199f A ogads-pa.googleapis.com A 216.58.205.42 A 142.250.180.138 A 142.250.180.170 A 142.251.…
26 0.529479 192.168.1.1 192.168.1.217 DNS 124 Standard query response 0xe9c3 AAAA apis.google.com CNAME plus.l.google.com AAAA 2a00:1450:4002:414::200e
28 1.125652 192.168.1.1 192.168.1.217 DNS 103 Standard query response 0xeaa8 A safebrowsing.googleapis.com A 142.251.143.170
31 1.518471 192.168.1.1 192.168.1.217 DNS 91 Standard query response 0xd993 A play.google.com A 142.250.180.142
32 1.518822 192.168.1.1 192.168.1.217 DNS 103 Standard query response 0x17ac AAAA play.google.com AAAA 2a00:1450:4002:415::200e
Frame 4: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: ZyxelCommuni_76:8d:07 (b8:d5:26:76:8d:07), Dst: PCSSystemtec_ad:25:87 (08:00:27:ad:25
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.217
User Datagram Protocol, Src Port: 53, Dst Port: 34676
Domain Name System (response)
Transaction ID: 0x1e64
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
www.google.com: type A, class IN
Name: www.google.com
[Name Length: 14]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
Answers
[Request In: 1]
[Time: 0.002007000 seconds]
0000 08 00 27 ad 25 87 b8 d5 26 76 8d 07 08 00 45 00 ··'·%··· &v····E·
0010 00 4c 00 00 40 00 40 11 b6 76 c0 a8 01 01 c0 a8 ·L··@·@· ·v····
0020 01 d9 00 35 87 74 00 38 c2 49 1e 64 81 80 00 01 ···5·t·8 ·I·d····
0030 00 01 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c ·······w ww·googl
0040 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 e·com··· ········
0050 00 00 00 41 00 04 8e fa b4 84 ···A···· ··