Esplorazione del Traffico DNS

Obiettivi dell'Esercitazione

L'obiettivo principale di questa esercitazione era di catturare e analizzare il traffico DNS generato durante un'attività specifica. Gli obiettivi specifici erano:

1. Catturare il traffico DNS.
2. Esplorare il traffico delle query DNS.
3. Esplorare il traffico delle risposte DNS.

Metodologia

1. **Attività svolta**:
    - Dalla macchina Kali Linux, è stato effettuato un ping verso il dominio `google.com` per generare traffico DNS.
2. **Strumento utilizzato**:
    - È stato usato **Wireshark** per catturare e analizzare i pacchetti di rete.
3. **Filtraggio del traffico**:
    - È stato applicato il filtro `dns` per visualizzare esclusivamente i pacchetti DNS catturati.

Analisi del Traffico Catturato

Query DNS

- **Origine**: 10.0.2.15
- **Destinazione**: 10.0.2.3 (server DNS)
- **Tipo di query**:
    - Record A: richiesta dell'indirizzo IPv4 per `google.com`.
    - Record AAAA: richiesta dell'indirizzo IPv6 per `google.com`.

Risposte DNS

- **Origine**: 10.0.2.3 (server DNS)
- **Destinazione**: 10.0.2.15
- **Contenuto delle risposte**:
    - Record A: restituito l'indirizzo IPv4 `216.58.204.142`.
    - Record AAAA: restituito l'indirizzo IPv6 `2a00:1450:4002:414::200e`.

Informazioni aggiuntive

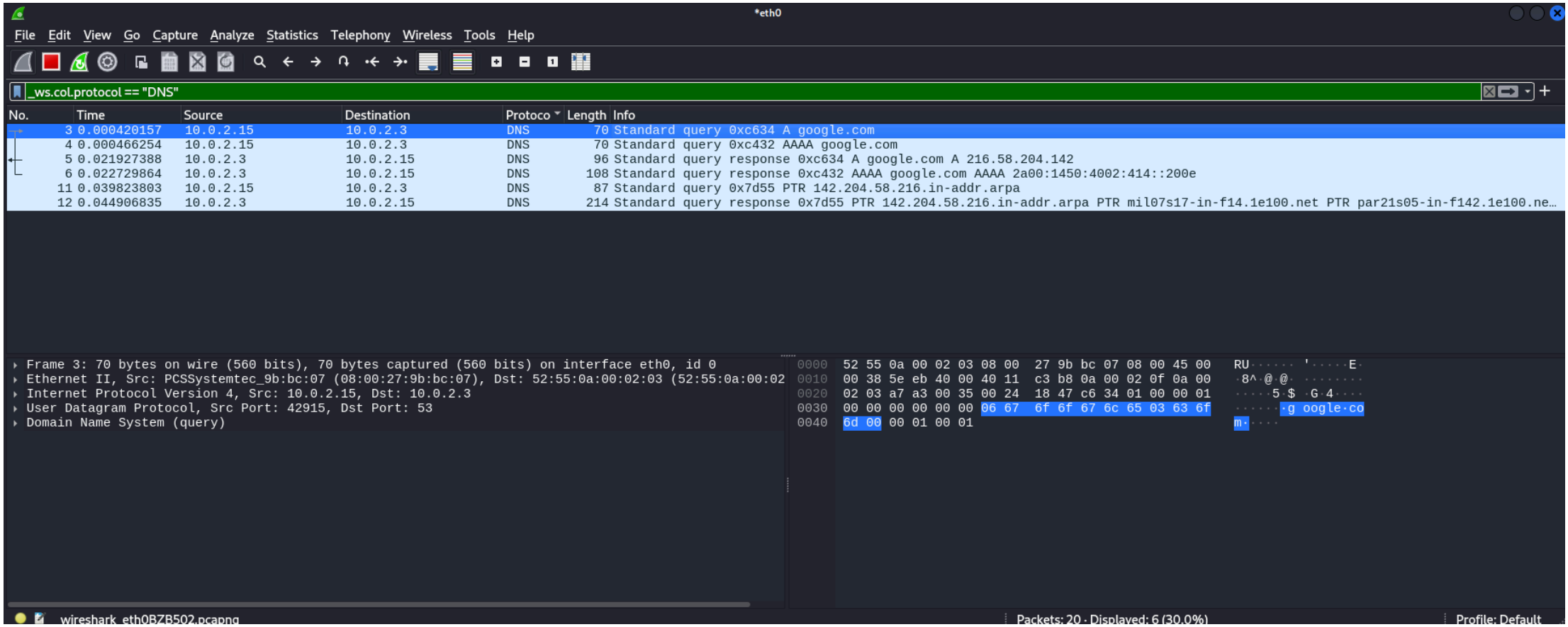
- È stata effettuata una query PTR per ottenere il nome di dominio inverso corrispondente all'indirizzo IP `142.204.58.216`.

Conclusioni

Questa esercitazione ha permesso di comprendere:

- La struttura delle query DNS e delle risposte.
- L'importanza del protocollo DNS nella risoluzione dei nomi di dominio.
- Come utilizzare Wireshark per catturare e analizzare traffico DNS in modo efficace.

Il traffico catturato conferma il corretto funzionamento del processo di risoluzione DNS per il dominio `google.com` e la corretta configurazione della rete.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
_ws.col.protocol == "DNS"
No. Time Source Destination Protoco Length Info
3 0.000420157 10.0.2.15 10.0.2.3 DNS 70 Standard query 0xc634 A google.com
4 0.000466254 10.0.2.15 10.0.2.3 DNS 70 Standard query 0xc432 AAAA google.com
5 0.021927388 10.0.2.3 10.0.2.15 DNS 96 Standard query response 0xc634 A google.com A 216.58.204.142
6 0.022729864 10.0.2.3 10.0.2.15 DNS 108 Standard query response 0xc432 AAAA google.com AAAA 2a00:1450:4002:414::200e
11 0.039823803 10.0.2.15 10.0.2.3 DNS 87 Standard query 0x7d55 PTR 142.204.58.216.in-addr.arpa
12 0.044906835 10.0.2.3 10.0.2.15 DNS 214 Standard query response 0x7d55 PTR 142.204.58.216.in-addr.arpa PTR mil07s17-in-f14.1e100.net PTR par21s05-in-f142.1e100.ne…
Frame 3: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_9b:bc:07 (08:00:27:9b:bc:07), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
User Datagram Protocol, Src Port: 42915, Dst Port: 53
Domain Name System (query)
0000 52 55 0a 00 02 03 08 00 27 9b bc 07 08 00 45 00
0010 00 38 5e eb 40 00 40 11 c3 b8 0a 00 02 0f 0a 00
0020 02 03 a7 a3 00 35 00 24 18 47 c6 34 01 00 00 01
0030 00 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6f
0040 6d 00 00 01 00 01
wireshark_eth0BZB502.pcapng
Packets: 20 · Displayed: 6 (30.0%)
Profile: Default