Report Laboratorio – Cisco CyberOps Giorno 3

Obiettivi

Questo laboratorio ha come obiettivo l'analisi del traffico DNS utilizzando Wireshark e nslookup. Sono state generate query DNS per www.cisco.com, catturate con Wireshark e analizzate per osservare indirizzi MAC, IP, porte UDP e flag DNS, oltre a confrontare i risultati con l'output del comando nslookup.

Scenario

Il client Kali Linux (IP 10.0.2.15) effettua una query DNS al server Google 8.8.8.8. Wireshark cattura i pacchetti di query e risposta. In parallelo, il comando nslookup fornisce le informazioni sui record CNAME e A associati al dominio www.cisco.com.

Analisi della Query DNS

La query DNS viene inviata dal client al server DNS con i seguenti dettagli:
- MAC sorgente: 08:00:27:18:0d:98
- MAC destinazione: 52:54:00:12:35:00
- IP sorgente: 10.0.2.15
- IP destinazione: 8.8.8.8
- Porta sorgente: 43100 (porta effimera)
- Porta destinazione: 53 (DNS)
- Flags DNS: Recursion Desired attivo
- Query: www.cisco.com, Type A, Class IN

Analisi della Risposta DNS

La risposta DNS dal server al client contiene i seguenti dettagli:
- MAC sorgente: 52:54:00:12:35:00
- MAC destinazione: 08:00:27:18:0d:98
- IP sorgente: 8.8.8.8
- IP destinazione: 10.0.2.15
- Porta sorgente: 53
- Porta destinazione: 43100
- Flags DNS: Recursion Available impostato, no error
- Record Answers: CNAME multipli e record A con indirizzo IPv4 23.60.188.118 e indirizzi IPv6

- Confronto con nslookup: i risultati coincidono esattamente con i record CNAME e A mostrati da nslookup

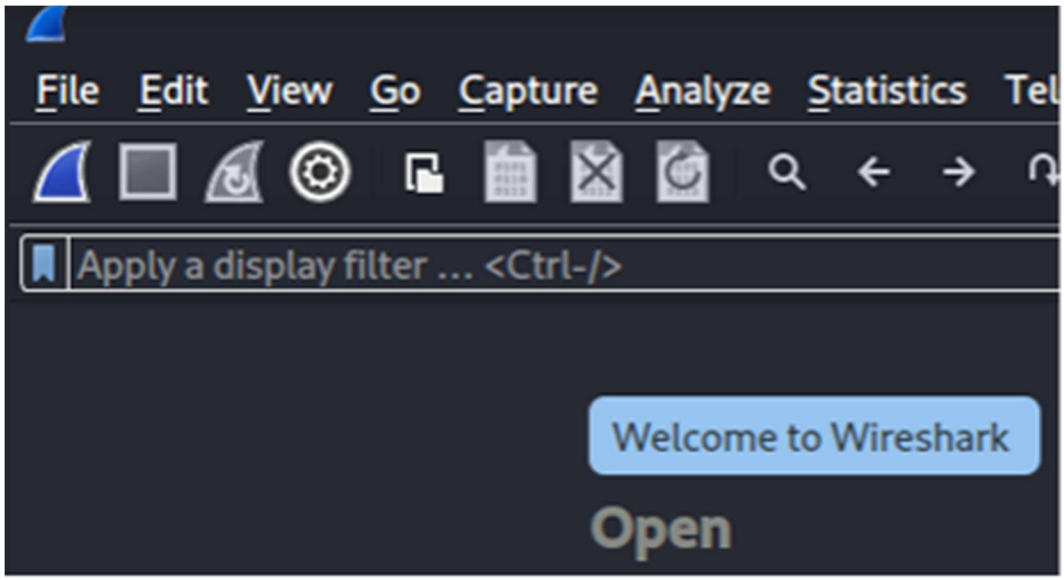
Riflessioni Finali

Analizzando il traffico senza filtri si possono osservare anche pacchetti ARP, ICMP e altre query DNS generate da applicazioni in background, fornendo una visione più ampia della rete. Un attaccante potrebbe sfruttare Wireshark per intercettare query DNS e dedurre i siti visitati, oltre a poter eseguire attacchi di DNS spoofing o poisoning.

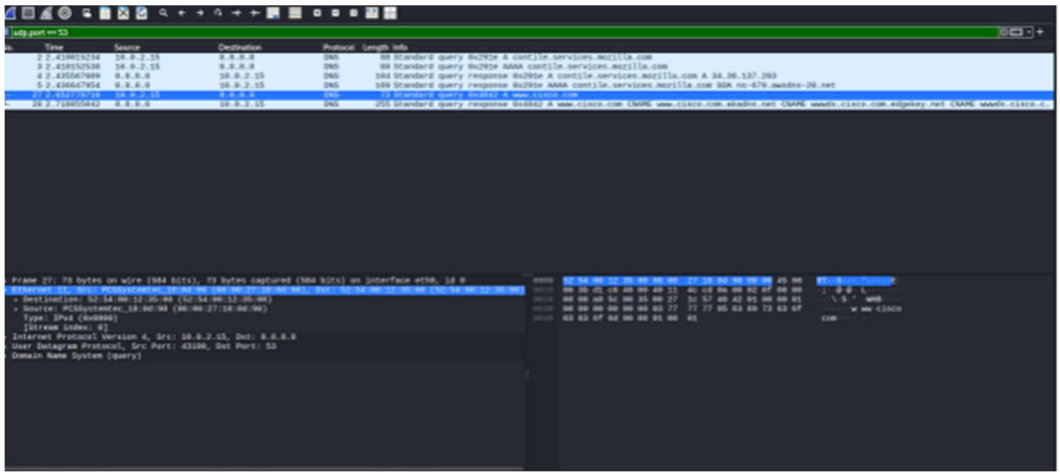
Conclusioni

Questo esercizio ha permesso di comprendere il funzionamento delle query e delle risposte DNS, analizzando i dettagli a livello Ethernet, IP e UDP. Inoltre, si è verificata la coerenza tra i pacchetti catturati e l'output del comando nslookup, rafforzando l'importanza dell'analisi del traffico per scopi di sicurezza e troubleshooting.

Screenshot del Laboratorio

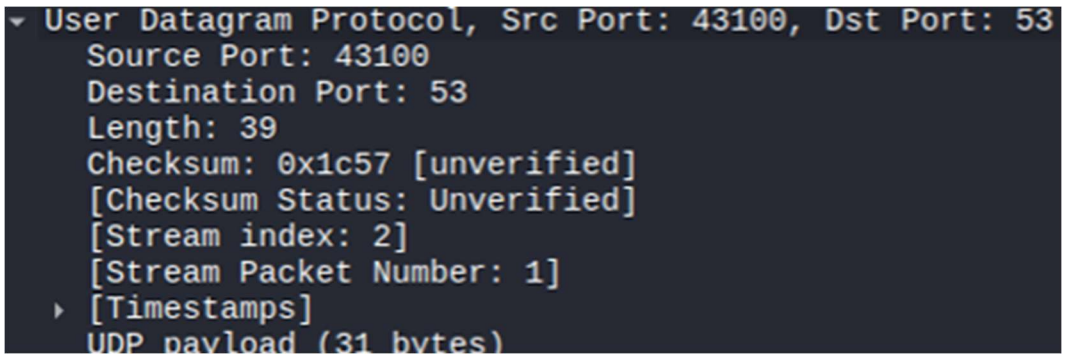


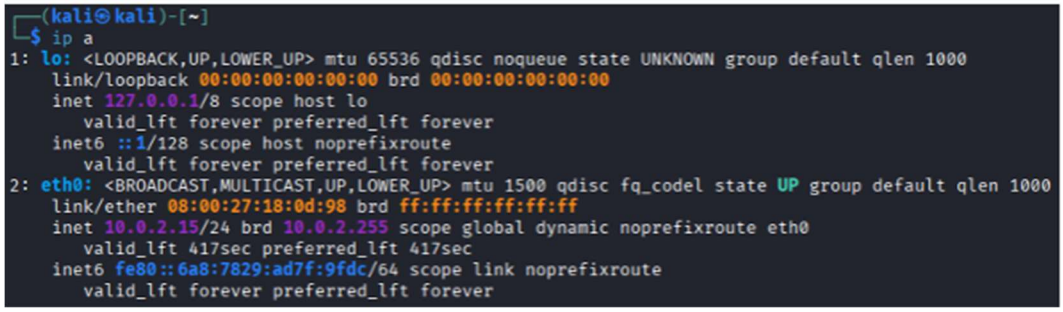
```
┌──(kali㉿kali)-[~]
└─$ nslookup
> www.cisco.com
Server:         8.8.8.8
Address:        8.8.8.8#53

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: 23.60.188.118
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:691::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:699::b33
> exit
```

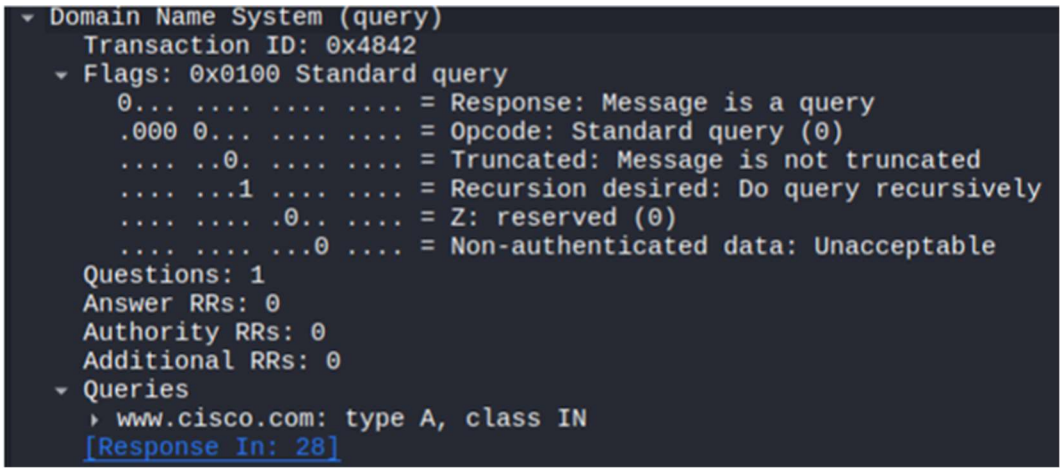


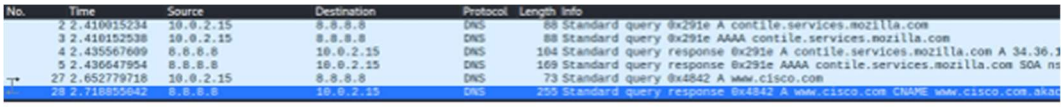
```
▸ Frame 27: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
▾ Ethernet II, Src: PCSSystemtec_18:0d:98 (08:00:27:18:0d:98), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
  ▸ Destination: 52:54:00:12:35:00 (52:54:00:12:35:00)
  ▸ Source: PCSSystemtec_18:0d:98 (08:00:27:18:0d:98)
    Type: IPv4 (0x0800)
    [Stream index: 0]
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 43100, Dst Port: 53
▸ Domain Name System (query)
```

```
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0xd1c6 (53702)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x4ccd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 8.8.8.8
    [Stream index: 1]
```

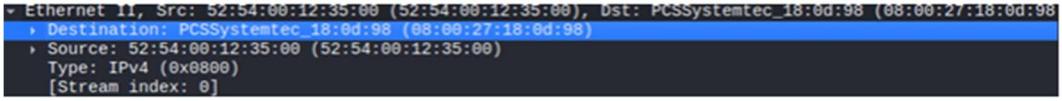

User Datagram Protocol, Src Port: 43100, Dst Port: 53
Source Port: 43100
Destination Port: 53
Length: 39
Checksum: 0x1c57 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (31 bytes)


(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 08:00:27:18:0d:98 brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
valid_lft 417sec preferred_lft 417sec
inet6 fe80::6a8:7829:ad7f:9fdc/64 scope link noprefixroute
valid_lft forever preferred_lft forever

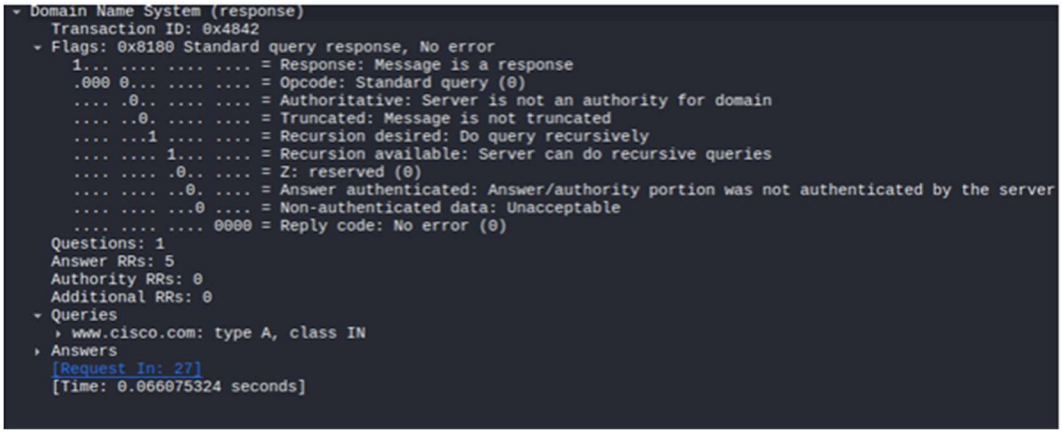

Domain Name System (query)
Transaction ID: 0x4842
Flags: 0x0100 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.cisco.com: type A, class IN
[Response In: 28]



No.	Time	Source	Destination	Protocol	Length	Info
2	2.410015234	10.0.2.15	8.8.8.8	DNS	88	Standard query 0x291e A contile.services.mozilla.com
3	2.410152538	10.0.2.15	8.8.8.8	DNS	88	Standard query 0x291e AAAA contile.services.mozilla.com
4	2.435567609	8.8.8.8	10.0.2.15	DNS	104	Standard query response 0x291e A contile.services.mozilla.com A 34.36.1
5	2.436647954	8.8.8.8	10.0.2.15	DNS	169	Standard query response 0x291e AAAA contile.services.mozilla.com SOA ns
27	2.652779718	10.0.2.15	8.8.8.8	DNS	73	Standard query 0x4842 A www.cisco.com
28	2.718855642	8.8.8.8	10.0.2.15	DNS	255	Standard query response 0x4842 A www.cisco.com CNAME www.cisco.com.akac



```
▾ Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSSystemtec_18:0d:98 (08:00:27:18:0d:98)
  ▸ Destination: PCSSystemtec_18:0d:98 (08:00:27:18:0d:98)
  ▸ Source: 52:54:00:12:35:00 (52:54:00:12:35:00)
    Type: IPv4 (0x0800)
    [Stream index: 0]
```



```
▾ Domain Name System (response)
    Transaction ID: 0x4842
  ▾ 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 server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.cisco.com: type A, class IN
  ▸ Answers
    [Request In: 27]
    [Time: 0.066075324 seconds]
```

```
      .... ..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 server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.cisco.com: type A, class IN
  ▾ Answers
    ▸ www.cisco.com: 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
    ▸ wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
    ▸ e2867.dsca.akamaiedge.net: type A, class IN, addr 23.60.188.118
    [Request In: 27]
    [Time: 0.066075324 seconds]
```

```
       valid_lft 565sec preferred_lft 565sec
    inet6 fe80::6a8:7829:ad7f:9fdc/64 scope link noprefixr
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ nslookup
> www.cisco.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.cisco.com   canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net        canonical name = wwwds.cis
wwwds.cisco.com.edgekey.net     canonical name = wwwds.cis
wwwds.cisco.com.edgekey.net.globalredir.akadns.net      ca
Name:   e2867.dsca.akamaiedge.net
Address: 23.60.188.118
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d00:691::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d00:699::b33
> exit
```