

REPORT S11/L3

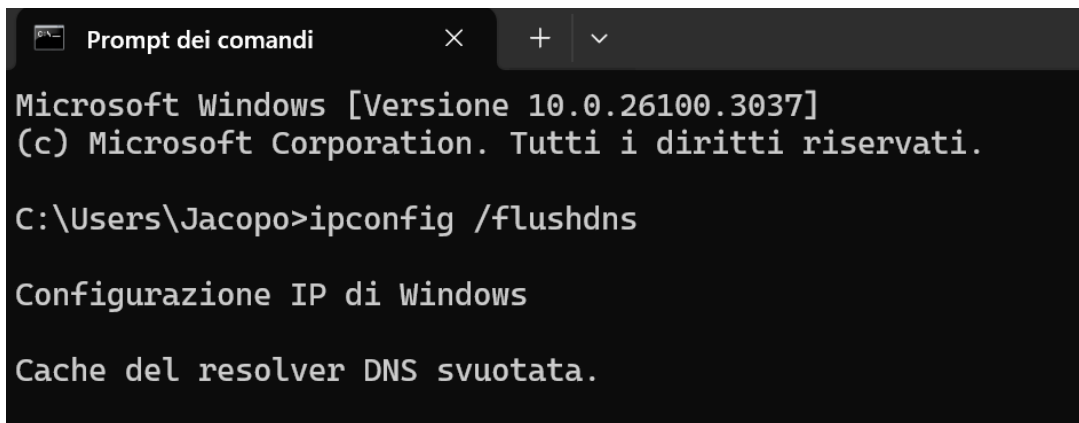
L'esercizio si divide in 3 parti.

- Catturare il Traffico DNS
- Esplorare il traffico delle Query DNS
- Esplorare il traffico delle risposte DNS.

SOLUZIONE

Per prima cosa procedo avviando WIRESHARK e selezionando un interfaccia di rete attiva.

Su windows eseguo il comando **ipconfig /flushdns**.



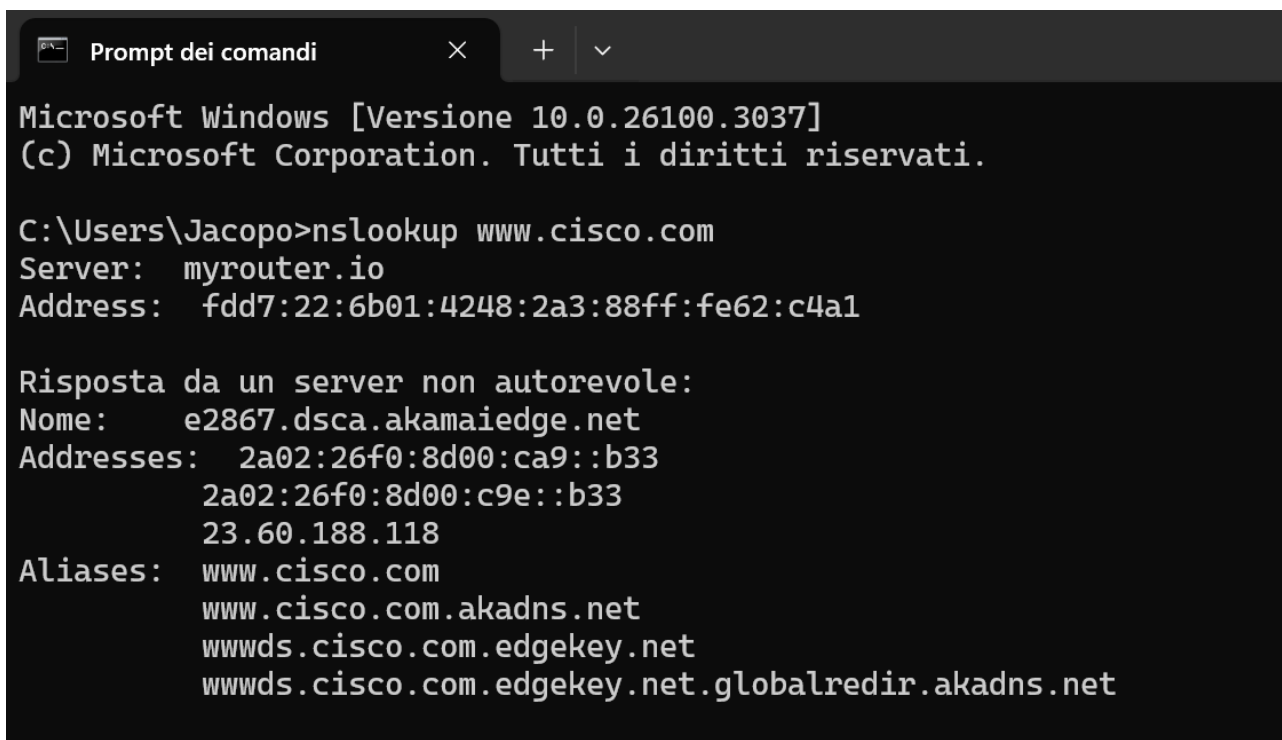
```
Prompt dei comandi
Microsoft Windows [Versione 10.0.26100.3037]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\Jacopo>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.
```

Seguo con **nslookup** www.cisco.com



```
Prompt dei comandi
Microsoft Windows [Versione 10.0.26100.3037]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\Jacopo>nslookup www.cisco.com
Server:  myrouter.io
Address:  fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1

Risposta da un server non autorevole:
Nome:      e2867.dsca.akamaiedge.net
Addresses:  2a02:26f0:8d00:ca9::b33
            2a02:26f0:8d00:c9e::b33
            23.60.188.118
Aliases:   www.cisco.com
            www.cisco.com.akadns.net
            wwwds.cisco.com.edgekey.net
            wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

Stoppo la cattura su wiresharck e vado a filtrare con **udp.port==53**

5.247257	fdd7:22:6b01:4248:a598:b0:3436:e461	fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1	DNS	152	Standard query 0x0001 PTR 1.a.4.c.2.6.e.f.f.f.8.
5.248425	fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1	fdd7:22:6b01:4248:a598:b0:3436:e461	DNS	177	Standard query response 0x0001 PTR 1.a.4.c.2.6.e
5.249353	fdd7:22:6b01:4248:a598:b0:3436:e461	fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1	DNS	98	Standard query 0x0002 A www.cisco.com.Home
5.250243	fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1	fdd7:22:6b01:4248:a598:b0:3436:e461	DNS	98	Standard query response 0x0002 No such name A ww
5.250345	fdd7:22:6b01:4248:a598:b0:3436:e461	fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1	DNS	98	Standard query 0x0003 AAAA www.cisco.com.Home
5.251076	fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1	fdd7:22:6b01:4248:a598:b0:3436:e461	DNS	98	Standard query response 0x0003 No such name AAAA
5.251177	fdd7:22:6b01:4248:a598:b0:3436:e461	fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1	DNS	93	Standard query 0x0004 A www.cisco.com
5.298332	fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1	fdd7:22:6b01:4248:a598:b0:3436:e461	DNS	275	Standard query response 0x0004 A www.cisco.com C
5.300020	fdd7:22:6b01:4248:a598:b0:3436:e461	fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1	DNS	93	Standard query 0x0005 AAAA www.cisco.com

Vado a selezionare un pacchetto che contenga “**Standard query**” e www.cisco.com nella colonna **info**.

Esapando la sezione **Ethernet II** e ne vado ad esaminare i dettagli, osservando in particolare i campi **source e destination**.

```

Frame 20: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{9227951C-8F83-4895-82F4-7488AD654BB3}, id 0
Ethernet II, Src: ASUSTekCOMPU_06:5f:f5 (08:bf:b8:06:5f:f5), Dst: SkyUk_62:c4:a1 (00:a3:88:62:c4:a1)
  Destination: SkyUk_62:c4:a1 (00:a3:88:62:c4:a1)
  Source: ASUSTekCOMPU_06:5f:f5 (08:bf:b8:06:5f:f5)
  Type: IPv6 (0x86dd)
  [Stream index: 0]

```

In questo caso il mac della sorgente sarà associato al pc e il mac destinatario sarà associato al gateway predefinito. Vado ora ad espandere la sezione **IPv4**.

```

Internet Protocol Version 6, Src: fdd7:22:6b01:4248:a598:b0:3436:e461, Dst: fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1
  0110 .... = Version: 6
  ... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  ... 1001 0101 1111 1010 = Flow Label: 0x95ffa
  Payload Length: 44
  Next Header: UDP (17)
  Hop Limit: 64
  Source Address: fdd7:22:6b01:4248:a598:b0:3436:e461
    [Address Space: Unique Local Unicast]
    [Special-Purpose Allocation: Unique-Local]
  Destination Address: fdd7:22:6b01:4248:2a3:88ff:fe62:c4a1

```

Analogamente anche in questo caso i due indirizzi saranno associati rispettivamente al pc e al gateway predefinito.

Vado ora ad espandere la sezione **User datagram protocol**. E individuo la porta sogente e la porta destinatario.

```

User Datagram Protocol, Src Port: 56308, Dst Port: 53
  Source Port: 56308
  Destination Port: 53
  Length: 44
  Checksum: 0x644c [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  [Stream Packet Number: 1]

```

In questo caso avrò che la **Source port** è **56308** e la **Destination Port** è la **53**.

Vado a determinare gli indirizzi IP e MAC sul PC, uso il comando **arp -a**

```

Interfaccia: 192.168.56.1 --- 0xd
Indirizzo Internet    Indirizzo fisico    Tipo
192.168.56.255        ff-ff-ff-ff-ff-ff  statico
224.0.0.22            01-00-5e-00-00-16  statico
224.0.0.251           01-00-5e-00-00-fb  statico
224.0.0.252           01-00-5e-00-00-fc  statico
239.255.255.250       01-00-5e-7f-ff-fa  statico

Interfaccia: 192.168.0.17 --- 0xf
Indirizzo Internet    Indirizzo fisico    Tipo
192.168.0.1           00-a3-88-62-c4-a1  dinamico
192.168.0.135         56-9c-37-bf-0d-d7  dinamico
192.168.0.179         8c-49-62-80-4d-93  dinamico
192.168.0.255         ff-ff-ff-ff-ff-ff  statico
224.0.0.22            01-00-5e-00-00-16  statico
224.0.0.251           01-00-5e-00-00-fb  statico
224.0.0.252           01-00-5e-00-00-fc  statico
239.255.255.250       01-00-5e-7f-ff-fa  statico
255.255.255.255       ff-ff-ff-ff-ff-ff  statico

```

Gli indirizzi catturati da wireshark corrispondo a quelli nella tabella.

Vado ora ad espandere la sezione Domain Name System (Query).

```
▼ 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.Home: type A, class IN
```

Espando contestualmente le sezione Flags e Queries, noto che la flag è impostata per richiamare la query ricorsivamente per l' IP di www.cisco.com.

Vado ora a selezionare una response per controllare l' inverso. In questo caso l' Ip source e il MAC saranno invertiti rispetto a prima.

Un attaccante può usare Wireshark per osservare il traffico e può ottenere informazione sensibile se il traffico non è criptato.