

ESERCIZIO S11 L3

Pratica S11/L3 PDF

Esplorazione del Traffico DNS

Esplorazione del Traffico DNS

Obiettivi

- Parte 1: Catturare il Traffico DNS
- Parte 2: Esplorare il Traffico delle Query DNS
- Parte 3: Esplorare il Traffico delle Risposte DNS

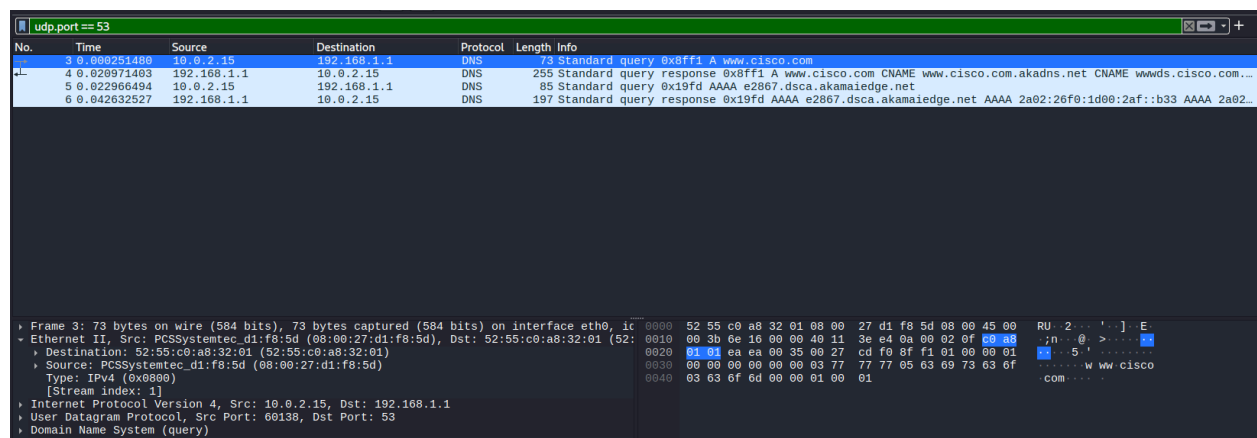
Risorse Richieste

1 PC con accesso a internet e Wireshark installato

SVOLGIMENTO

Parte 2 Esplorare il Traffico delle Query DNS

Quali sono gli indirizzi MAC di origine e destinazione?



Destination: **52:55:c0:a8:32:01 (52:55:c0:a8:32:01)**

Source: **PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)**

A quali interfacce di rete sono associati questi indirizzi MAC?

L'indirizzo MAC della Source **d1:f8:5d (08:00:27:d1:f8:5d)** è associata all'interfaccia di rete **PCSSystemtec**.

L'indirizzo MAC della Destination **52:55:c0:a8:32:01 (52:55:c0:a8:32:01)** rappresenta l'interfaccia di rete della destinazione.

Quali sono gli indirizzi IP di origine e destinazione?

```

> Frame 3: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:55:c0:a8:32:01 (52:55:c0:a8:32:01)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0x6e16 (28182)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x3ee4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 192.168.1.1
    [Stream index: 0]
> User Datagram Protocol, Src Port: 60138, Dst Port: 53

```

Indirizzo IP Source : 10.0.2.15

Indirizzo destinazione: 192.168.1.1

A quali interfacce di rete sono associati questi indirizzi IP?

L'indirizzo IP di origine **10.0.2.15** è associato all'interfaccia di rete **eth0**.

L'Indirizzo Ip di destinazione **192.168.1.1** è associato al dispositivo che sta rispondendo

Quali sono le porte di origine e destinazione?

```

> User Datagram Protocol, Src Port: 60138, Dst Port: 53
  Source Port: 60138
  Destination Port: 53
  Length: 39
  Checksum: 0xcdf0 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Stream Packet Number: 1]
  > [Timestamps]
  UDP payload (31 bytes)

```

Source Port: 60138

Destination Port : 53

Qual è il numero di porta DNS predefinito?

Il numero di porta DNS predefinito è **53** e viene utilizzato per la maggior parte delle query DNS standard.

Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?

L'osservazione è che i risultati ottenuti tramite il comando da terminale (ifconfig) **corrispondono esattamente** ai dati registrati da Wireshark per l'indirizzo IP e l'indirizzo MAC di origine.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    ether 08:00:27:d1:f8:5d txqueuelen 1000 (Ethernet)
    RX packets 6337 bytes 8507193 (8.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2122 bytes 163714 (159.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16 bytes 880 (880.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 880 (880.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Parte 3 Esplorare il Traffico delle Risposte DNS

Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?

Source Address: **52:55:c0:a8:32:01 (52:55:c0:a8:32:01)**

Destination Address: **PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)**

Source Port: **53**

Destination Port: **60138**

```

▼ Ethernet II, Src: 52:55:c0:a8:32:01 (52:55:c0:a8:32:01), Dst: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
  ► Destination: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
  ► Source: 52:55:c0:a8:32:01 (52:55:c0:a8:32:01)
  Type: IPv4 (0x0800)

▼ User Datagram Protocol, Src Port: 53, Dst Port: 60138
  Source Port: 53
  Destination Port: 60138
  Length: 221
  Checksum: 0xa994 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Stream Packet Number: 2]
  ► [Timestamps]
  UDP payload (213 bytes)

```

Come si confrontano con gli indirizzi nei pacchetti di query DNS?

Il confronto con gli indirizzi nei pacchetti di query DNS riporta che l'indirizzo sorgente e destinazione si sono invertiti.

Il server DNS può fare query ricorsive?

La sezione Recursion available conferma che il server DNS può fare query ricorsive.

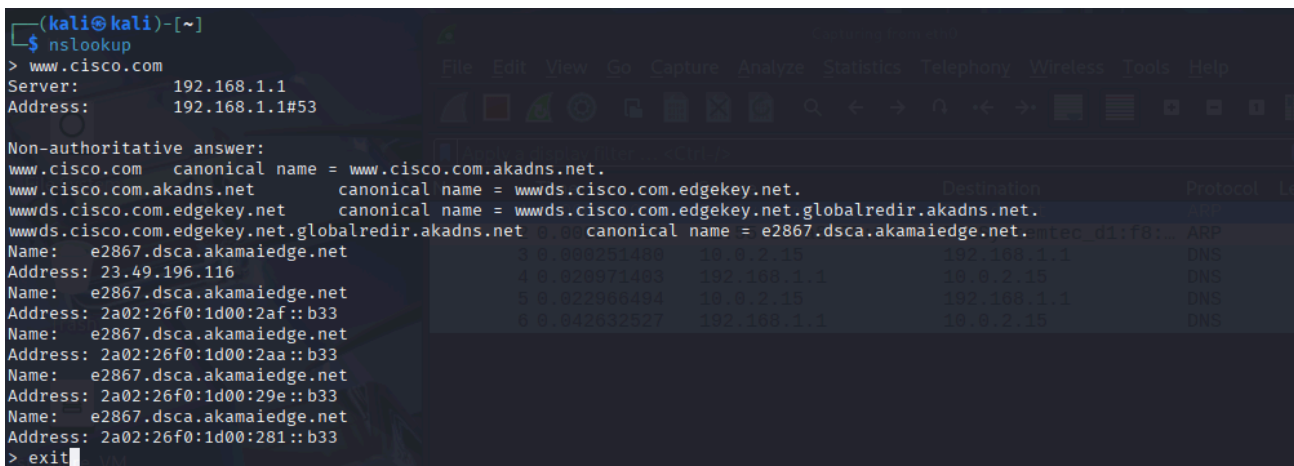
```

▼ Domain Name System (response)
  Transaction ID: 0x8ff1
  ► 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)

```

Come si confrontano i risultati con quelli di nslookup?

nslookup è uno strumento specifico per i DNS, mentre Wireshark è uno strumento per l'analisi di tutto il traffico di rete e permette di ispezionare ogni singolo pacchetto per un'analisi più dettagliata.



The screenshot shows a Kali Linux terminal window with the following output from the `nslookup` command:

```

(kali@kali)-[~]
$ nslookup
> www.cisco.com
Server:      192.168.1.1
Address:     192.168.1.1#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: 23.49.196.116
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:1d00:2af::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:1d00:29e::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:1d00:281::b33
> exit

```

Overlaid on the terminal is a Wireshark packet capture window showing a list of DNS packets. The table below represents the data visible in the Wireshark packet list:

No.	Time	Source	Destination	Protocol	Length
3	0.000251488	10.0.2.15	192.168.1.1	DNS	100
4	0.020671483	192.168.1.1	10.0.2.15	DNS	100
5	0.022660484	10.0.2.15	192.168.1.1	DNS	100
6	0.042632527	192.168.1.1	10.0.2.15	DNS	100

```

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 23.49.196.116

```

Riflessione

1. Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?

Rimuovendo il filtro `udp.port == 53`, Wireshark mostra tutti i pacchetti di rete catturati

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_d1:f8:...	Broadcast	ARP	42	Who has 192.168.50.1? Tell 10.0.2.15
2	0.000244984	52:55:c0:a8:32:01	PCSSystemtec_d1:f8:...	ARP	64	192.168.50.1 is at 52:55:c0:a8:32:01
3	0.000251480	10.0.2.15	192.168.1.1	DNS	73	Standard query 0x8ff1 A www.cisco.com
4	0.020971403	192.168.1.1	10.0.2.15	DNS	255	Standard query response 0x8ff1 A www.cisco.com CNAME www.cisco.com.akadns.net C...
5	0.022966494	10.0.2.15	192.168.1.1	DNS	85	Standard query 0x19fd AAAA e2867.dsca.akamaiedge.net
6	0.042632527	192.168.1.1	10.0.2.15	DNS	197	Standard query response 0x19fd AAAA e2867.dsca.akamaiedge.net AAAA 2a02:26f0:1d6...

Traffico ARP: Le prime due righe mostrano il protocollo **ARP (Address Resolution Protocol)**.

Il pacchetto 1 è una richiesta ARP

Il pacchetto 2 è la risposta ARP

2. Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?

Un attaccante può usare Wireshark per compromettere la sicurezza della tua rete in diversi modi, principalmente attraverso lo **sniffing (intercettazione)** del traffico non crittografato.

Cattura di dati sensibili: Un attaccante può usare Wireshark per catturare credenziali di accesso (nomi utente e password) se vengono trasmesse in chiaro su protocolli non sicuri come HTTP, Telnet, o FTP.

Man-in-the-Middle (MITM): Un attaccante può combinare Wireshark con attacchi come l'ARP Spoofing. L'attaccante può ingannare i dispositivi sulla rete, facendoli credere che il suo computer sia il router. Tutto il traffico destinato a internet passerà attraverso il computer dell'attaccante, che lo intercetterà con Wireshark prima di inoltrarlo.

Mappatura della rete: Un attaccante può usare Wireshark per mappare la topologia della rete, identificando gli indirizzi IP e MAC di tutti i dispositivi, i sistemi operativi, i servizi in esecuzione e i tipi di traffico. Questa intelligence può essere usata per pianificare attacchi più mirati.

Analisi dei protocolli: L'analisi del traffico può rivelare vulnerabilità in protocolli poco conosciuti o configurati male, che possono essere sfruttate per sferrare attacchi più sofisticati.