

Esercizio S10_L3_Wireshark_DNS

Consegna

Obiettivi

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

Scenario

Wireshark è uno strumento open source per la cattura e l'analisi dei pacchetti. Wireshark fornisce una scomposizione dettagliata dello stack dei protocolli di rete.

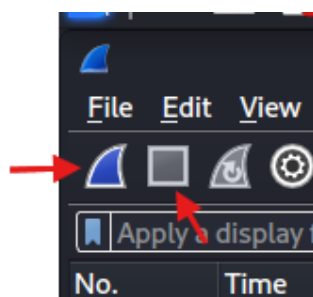
Wireshark permette di filtrare il traffico per la risoluzione dei problemi di rete, investigare problemi di sicurezza e analizzare i protocolli di rete.

Poiché Wireshark permette di visualizzare i dettagli dei pacchetti, può essere usato come strumento di ricognizione da un attaccante. In questo laboratorio, installerai Wireshark e lo userai per filtrare i pacchetti DNS e visualizzare i dettagli sia dei pacchetti di query DNS che di quelli di risposta.

Svolgimento

Per lo svolgimento di questo esercizio è necessario catturare alcune richieste DNS tramite wireshark.

Possiamo avviare il capturing e stopparlo dopo aver eseguito le richieste DNS tramite i due pulsanti qui sotto:



Per simulare delle richieste DNS possiamo utilizzare nslookup ed inserire alcuni indirizzi di siti web di cui richiedere gli ip:

nslookup

```
(kali㉿kali)-[~]
$ nslookup
> google.com
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.209.46
Name:   google.com
Address: 2a00:1450:4002:414::200e

> libero.it
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
Name:   libero.it
Address: 213.209.17.209

> amazon.com
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
Name:   amAzon.com
Address: 205.251.242.103
Name:   amAzon.com
Address: 52.94.236.248
Name:   amAzon.com
Address: 54.239.28.85

> cisco.com
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
Name:   cisco.com
Address: 72.163.4.185
Name:   cisco.com
Address: 2001:420:1101:1::185
```

Una volta stoppato il capturing possiamo analizzare i pacchetti catturati filtrandoli per la porta udp utilizzata per le richieste DNS:

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
5	11.251853317	10.0.2.15	192.168.1.254	DNS	70	Standard query 0xf7b3 A google.com
6	11.276435904	192.168.1.254	10.0.2.15	DNS	86	Standard query response 0xf7b3 A google.com A 142
7	11.277180865	10.0.2.15	192.168.1.254	DNS	70	Standard query 0xb7de AAAA google.com
8	11.283534753	192.168.1.254	10.0.2.15	DNS	98	Standard query response 0xb7de AAAA google.com AA
19	24.837886199	10.0.2.15	192.168.1.254	DNS	69	Standard query 0xb89a A libero.it
20	24.869366096	192.168.1.254	10.0.2.15	DNS	85	Standard query response 0xb89a A libero.it A 213.
21	24.869794940	10.0.2.15	192.168.1.254	DNS	69	Standard query 0x6fe1 AAAA libero.it
22	24.888978317	192.168.1.254	10.0.2.15	DNS	155	Standard query response 0x6fe1 AAAA libero.it SOA
26	32.290361128	10.0.2.15	192.168.1.254	DNS	70	Standard query 0x60a6 A amazon.com
27	32.314296222	192.168.1.254	10.0.2.15	DNS	125	Standard query response 0x60a6 A amazon.com A 205
28	32.314696198	10.0.2.15	192.168.1.254	DNS	70	Standard query 0xb83a AAAA amazon.com
29	32.332937979	192.168.1.254	10.0.2.15	DNS	137	Standard query response 0xb83a AAAA amazon.com SO
33	46.465292913	10.0.2.15	192.168.1.254	DNS	69	Standard query 0x8ec2 A cisco.com
34	46.498133360	192.168.1.254	10.0.2.15	DNS	85	Standard query response 0x8ec2 A cisco.com A 72.1
35	46.498562678	10.0.2.15	192.168.1.254	DNS	69	Standard query 0x2ef3 AAAA cisco.com
36	46.511448675	192.168.1.254	10.0.2.15	DNS	97	Standard query response 0x2ef3 AAAA cisco.com AAA

Ethernet II Section

Quali sono gli indirizzi MAC di origine e destinazione?

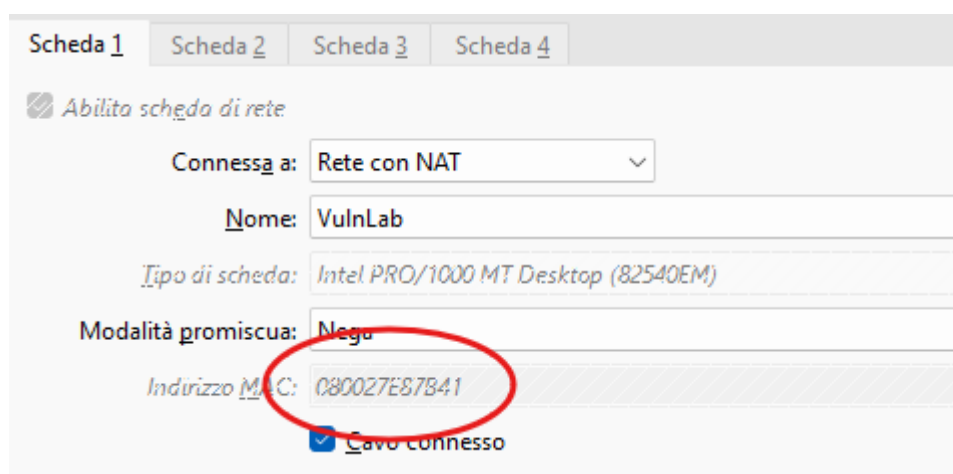
L'indirizzo di origine - Source - è 08:00:27:e8:7b:41

L'indirizzo di destinazione - Destination - è 52:54:00:12:35:00

```
▼ Ethernet II, Src: PCSSystemtec_e8:7b:41 (08:00:27:e8:7b:41), 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_e8:7b:41 (08:00:27:e8:7b:41)
```

A quali interfacce di rete sono associati questi indirizzi MAC?

Nei pacchetti DNS analizzati con Wireshark compaiono due indirizzi MAC. L'indirizzo Source 08:00:27:e8:7b:41 appartiene all'interfaccia di rete virtuale della macchina Kali su VirtualBox. Questo è verificabile sia dalle impostazioni di rete della VM (campo "Indirizzo MAC"), sia dal comando `ip link show` all'interno del sistema, dove compare associato all'interfaccia (es. `eth0`).



L'indirizzo Destination 52:54:00:12:35:00 non è quello del server DNS remoto, ma dell'interfaccia del gateway/bridge virtuale che collega la VM verso l'esterno. In modalità NAT, corrisponde al router virtuale gestito da VirtualBox/QEMU, che riceve le richieste DNS dalla VM e le inoltra su Internet.

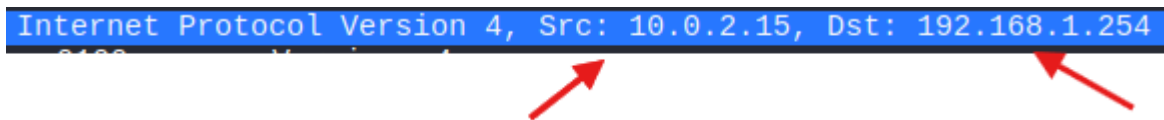
In sintesi: il MAC sorgente identifica l'interfaccia della mia Kali, mentre il MAC destinazione identifica l'interfaccia virtuale del gateway di rete fornito dall'hypervisor.

IPV4 Section

Per rispondere alle prossime domande è necessario spostarsi all'interno della sezione [Internet Protocol Version 4](#):

Quali sono gli indirizzi IP di origine e destinazione?

In questo caso l'ip sorgente è **10.0.2.15**. L'indirizzo IP di destinazione è **192.168.1.254**, che è utilizzato come gateway: la query DNS viene inviata a questo indirizzo affinché il gateway provveda a instradarla verso il server DNS e a restituire la relativa risposta.



A quali interfacce di rete sono associati questi indirizzi IP?

L' IP sorgente: 10.0.2.15 è l'indirizzo assegnato alla VM Kali Linux in VirtualBox ed è associato all'**interfaccia di rete virtuale della VM** in questo caso eth0:

`ip a`

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536
   link/loopback 00:00:00:00:00:00 brd
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft
   inet6 ::1/128 scope host noprefixro
       valid_lft forever preferred_lft
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_
   link/ether 08:00:27:e8:7b:41 brd ff
   inet 10.0.2.15/24 brd 10.0.2.255 sc
       valid_lft 312sec preferred_lft 3
   inet6 fe80::1080:683a:3279:554f/64
       valid_lft forever preferred_lft
```

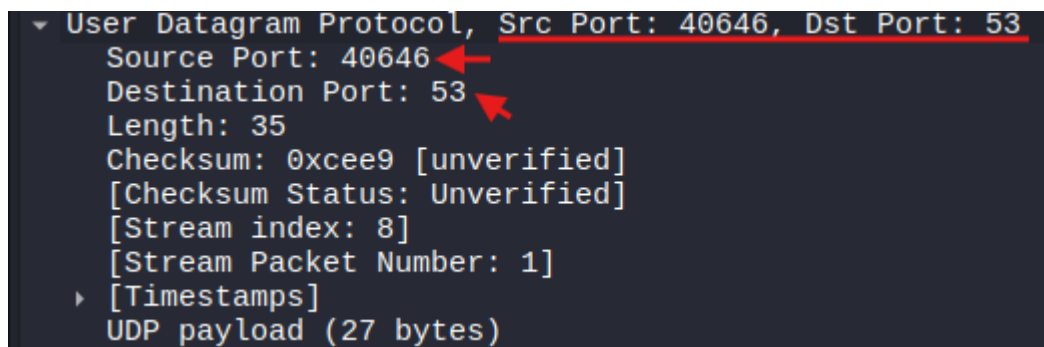
L' IP destinazione: 192.168.1.254 è l'indirizzo del gateway/router che riceve i pacchetti dalla VM per instradarli verso Internet. E' dunque un'interfaccia di rete esterna, tipicamente rappresenta **l'interfaccia LAN del router fisico**.

UDP Section

Spostandoci ora all'interno della sezione User Datagram Protocol possiamo rispondere ai seguenti quesiti:

Quali sono le porte di origine e destinazione?

La porta di origine è la porta effimera 40646 mentre la porta di destinazione è la 53 tipica per l'appunto delle richieste DNS.

A screenshot of the Wireshark packet details pane for a User Datagram Protocol (UDP) packet. The packet list shows a single packet. The details pane is expanded to show the UDP section. The source port is 40646 and the destination port is 53. The length is 35 bytes. The checksum is 0xcee9, marked as unverified. The stream index is 8 and the stream packet number is 1. The payload is 27 bytes.

```
▼ User Datagram Protocol, Src Port: 40646, Dst Port: 53
  Source Port: 40646
  Destination Port: 53
  Length: 35
  Checksum: 0xcee9 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 8]
  [Stream Packet Number: 1]
  [Timestamps]
  UDP payload (27 bytes)
```

Qual è il numero di porta DNS predefinito?

Come spiegato qui sopra, la porta predefinita per il servizio DNS è la 53.

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

Confrontando MAC e IP, si osserva coerenza: l'indirizzo IP sorgente 10.0.2.15 corrisponde al MAC 08:00:27:e8:7b:41 dell'interfaccia della VM Kali, mentre l'indirizzo IP di destinazione 192.168.1.254 corrisponde al MAC 52:54:00:12:35:00 dell'interfaccia gateway/router. Ciò conferma la relazione tra indirizzi di livello 2 e livello 3 nel modello OSI.

DNS QUery Section

L'ultima sessione da analizzare è quella relativa al traffico delle Risposte DNS:

Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione? Come si confrontano con gli indirizzi nei pacchetti di query DNS?

Gli indirizzi MAC ed IP sono ovviamente **invertiti rispetto al pacchetto precedente** in quanto in questo caso il pacchetto è inviato dal Gateway verso la nostra VM.

Esandere Domain Name System (response). Quindi esandere Flags, Queries, e Answers. Osservare i risultati. Il server DNS può fare query ricorsive?

Nei flag DNS troviamo due campi importanti:

- Recursion Desired (RD): 1 → Do query recursively
Questo bit viene impostato dal client nella richiesta e significa che il client chiede al server DNS di **effettuare la risoluzione ricorsiva** per suo conto.
- Recursion Available (RA): 1 → Server can do recursive queries
Questo bit è impostato dal server nella risposta: indica che **il server supporta ed è in grado di eseguire query ricorsive**.

Nel pacchetto entrambi i flag sono impostati, quindi il client ha chiesto una risoluzione ricorsiva ed il server ha confermato di supportarla.

```
▼ 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
  .... .0... .. = Non-authenticated data: Unacceptable
  .... .0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▶ cisco.com: type AAAA, class IN
▼ Answers
  ▶ cisco.com: type AAAA, class IN, addr 2001:420:1101:1::185
  [Request In: 35]
  [Time: 0.020885997 seconds]
```

Osservare i record CNAME e A nei dettagli delle Risposte Answers). Come si confrontano i risultati con quelli di nslookup?

Wireshark mostra il dettaglio grezzo dei pacchetti: nel caso catturato, solo un record AAAA.

Nslookup invece, a seconda della query e del resolver, può restituire più record (A, AAAA, ed eventuali CNAME).

```

▼ Answers
▼ cisco.com: type AAAA, class IN, addr 2001:420:1101:1::185
  Name: cisco.com
  Type: AAAA (28) (IP6 Address)
  Class: IN (0x0001)
  Time to live: 1268 (21 minutes, 8 seconds)
  Data length: 16
  AAAA Address: 2001:420:1101:1::185
[Request In: 35]
[Time: 0.020885997 seconds]

```

Riflessione Finale

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

Rimuovendo il filtro vedremo ovviamente tutto il traffico catturato durante il processo di cattura; appariranno dunque contemporaneamente elementi di livello 2 (Ethernet/MAC), livello 3 (IP) e livello 4+ (TCP/UDP e applicazioni), il che consente di ricostruire la topologia e i servizi esposti.

6	11.276435004	192.168.1.254	10.0.2.15	DNS	86 Standard query response 0xf7b3 A google.com A 142.251.209.46
7	11.277180865	10.0.2.15	192.168.1.254	DNS	70 Standard query 0xb7de AAAA google.com
8	11.283534753	192.168.1.254	10.0.2.15	DNS	98 Standard query response 0xb7de AAAA google.com AAAA 2a00:1450:4002:414::200e
9	12.044893408	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
10	12.568936010	10.0.2.15	10.0.2.3	DHCP	324 DHCP Request - Transaction ID 0xec177def
11	12.574431864	10.0.2.3	10.0.2.15	DHCP	590 DHCP ACK - Transaction ID 0xec177def
12	13.051753046	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
13	14.075779141	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
14	15.101607169	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
15	16.127841283	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
16	17.148026558	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
17	17.596269464	PCSSystemtec_e8:7b:41	PCSSystemtec_a5:6d:19	ARP	42 Who has 10.0.2.3? Tell 10.0.2.15
18	17.597128876	PCSSystemtec_a5:6d:19	PCSSystemtec_e8:7b:41	ARP	60 10.0.2.3 is at 08:00:27:a5:6d:19
19	24.837080109	10.0.2.15	192.168.1.254	DNS	69 Standard query 0x8d9a A libero.it
20	24.869360696	192.168.1.254	10.0.2.15	DNS	85 Standard query response 0x8d9a A libero.it A 213.209.17.209
21	24.869794040	10.0.2.15	192.168.1.254	DNS	69 Standard query 0x6fe1 AAAA libero.it
22	24.888978317	192.168.1.254	10.0.2.15	DNS	155 Standard query response 0x6fe1 AAAA libero.it SOA ns1.italiaonline.it
23	28.172269198	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
24	29.180997913	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
25	30.283981059	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
26	32.296301128	10.0.2.15	192.168.1.254	DNS	70 Standard query 0x60a6 A amazon.com
27	32.314296222	192.168.1.254	10.0.2.15	DNS	125 Standard query response 0x60a6 A amazon.com A 205.251.242.103 A 52.94.236.248 A 54.239.28.85
28	32.314690108	10.0.2.15	192.168.1.254	DNS	70 Standard query 0x8b3a AAAA amazon.com
29	32.332937979	192.168.1.254	10.0.2.15	DNS	137 Standard query response 0x8b3a AAAA amazon.com SOA dns-external-master.amazon.com
30	41.233977512	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
31	42.236006093	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
32	43.260303971	PCSSystemtec_e8:7b:41	Broadcast	ARP	42 Who has 10.0.2.12? Tell 10.0.2.15
33	46.465292913	10.0.2.15	192.168.1.254	DNS	69 Standard query 0x8ec2 A cisco.com
34	46.490133360	192.168.1.254	10.0.2.15	DNS	85 Standard query response 0x8ec2 A cisco.com A 72.163.4.185
35	46.490562678	10.0.2.15	192.168.1.254	DNS	69 Standard query 0x2ef3 AAAA cisco.com
36	46.511448675	192.168.1.254	10.0.2.15	DNS	97 Standard query response 0x2ef3 AAAA cisco.com AAAA 2001:420:1101:1::185

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

Un attaccante può sfruttare Wireshark o strumenti equivalenti sia in modalità passiva (sniffing) sia come supporto per attacchi attivi (MITM). Le tecniche tipiche e gli obiettivi:

1. **Sniffing passivo:** posizionandosi sulla stessa rete fisica o su una rete in cui il traffico è visibile (hub, rete Wi-Fi non isolata, segmenti mal

configurati), **l'attaccante cattura traffico in chiaro** per estrarre credenziali (HTTP basic, FTP, POP3/IMAP non TLS), cookie, token, e-mail e file trasferiti. Anche le query DNS rivelano la navigazione degli utenti.

2. **ARP spoofing / MITM**: combinando ARP poisoning con lo sniffing (o con strumenti di inoltro), l'attaccante intercetta il traffico di un host e lo rilancia, ottenendo **accesso a sessioni TLS non protette correttamente**, potendo tentare downgrade, session hijacking o iniezioni di payload.
3. **Riconoscimento e ricognizione**: Wireshark fornisce dati per **fingerprinting dei sistemi** (TTL, opzioni TCP, banner dei servizi), per mappare servizi esposti, versioni software e possibili vulnerabilità da sfruttare.
4. **Esfiltrazione e lateral movement**: osservando con attenzione, l'attaccante **individua condivisioni di rete (SMB)**, credenziali riutilizzate o protocolli legacy per muoversi lateralmente.
5. **Attacchi basati su informazioni raccolte**: le informazioni raccolte (IP, MAC, servizi, domini visitati) sono usate per **attacchi mirati**: phishing più credibile (usando domini osservati), spoofing di servizi interni, o per compromettere elementi di rete (switch/router) noti.

Conclusioni

L'analisi dei pacchetti DNS con Wireshark ha permesso di ricostruire in modo coerente la mappatura tra i livelli 2 e 3 della rete: gli indirizzi MAC osservati corrispondono all'interfaccia virtuale della VM Kali (VirtualBox) e all'interfaccia del gateway/NAT virtuale, mentre gli indirizzi IP **10.0.2.15** → sorgente, **192.168.1.254** → destinazione identificano il nodo logico che genera la query e il gateway che la inoltra.

L'espansione delle sezioni DNS (Flags, Queries, Answers) ha confermato che il resolver ha eseguito la risoluzione ricorsiva (RD=1 richiesto dal client, RA=1 segnalato dal server) e che le risposte possono includere diversi tipi di record (A, AAAA, SOA), a seconda della query e della zona interrogata. Rimuovendo i filtri si ottiene una vista completa della rete che rivela ARP, DHCP e traffico applicativo, utile per ricostruire topologia, servizi attivi e comportamento dei client.

Dal punto di vista della sicurezza, Wireshark si rivela un'arma a doppio taglio: da un lato facilita il troubleshooting e la comprensione del comportamento di rete; dall'altro, se ottenuta da un attore non autorizzato, può essere sfruttata per ricognizione, sniffing di credenziali in chiaro o attacchi MITM (es. ARP spoofing).