Esplorazione del traffico DSN

profilo studente

- **Gabriel Giustinelli**
- **Epicode Cyber Security**
- **classe** CS0525
- **data** 12/02/2026

Progetto

in questo laboratorio useremo wireshark che è uno strumento per la cattura e l'analisi dei pacchetti che ci permette:

- 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.
- visualizzare i dettagli dei pacchetti.
- e può essere usato come strumento di ricognizione da un attaccante.

Useremo la macchina virtuale Kali linux collegata a internet e con wireshark andiamo a catturare il traffico DNS della nostra macchina verso il sito web con nome di dominio **www.cisco.com** , andando ad estrarre il traffico e per esplorare le query del DNS e rispondere alle domande del compito.

Risposte alle domande

Quali sono gli indirizzi MAC di origine e destinazione?

- **Sorgente (Source):** `52:54:00:12:35:00` (è il MAC del router virtuale NAT di QEMU/KVM o VirtualBox).
- **Destinazione (Destination):** `08:00:27:bc:64:df` (è il MAC della scheda di rete Kali).

A quali interfacce di rete sono associati questi indirizzi MAC?

MAC `08:00:27:bc:64:df` (Destinazione nella risposta):

- È associato all'**interfaccia di rete virtuale della tua VM Kali** (solitamente chiamata **`eth0`**).
- *Nota tecnica:* Il prefisso `08:00:27` identifica univocamente le schede di rete virtuali generate da **VirtualBox**.

MAC `52:54:00:12:35:00` (Origine nella risposta):

- È associato all'**interfaccia del Gateway predefinito** della rete NAT (il router virtuale che gestisce la comunicazione tra la tua VM e internet).

- *Nota tecnica:* Il prefisso `52:54:00` è tipico delle interfacce di rete virtuali di **QEMU/KVM**, che spesso agiscono come motore di rete in vari ambienti di virtualizzazione.

Quali sono gli indirizzi IP di origine e destinazione?

- **Indirizzo IP di Origine (Source):** `10.0.2.3`
- **Indirizzo IP di Destinazione (Destination):** `10.0.2.15`

A quali interfacce di rete sono associati questi indirizzi IP?

- **IP `10.0.2.3` (Origine):** È associato all'interfaccia del **Server DNS virtuale** della rete NAT (che solitamente coincide con il gateway predefinito fornito dal software di virtualizzazione).
- **IP `10.0.2.15` (Destinazione):** È associato all'interfaccia di rete locale della **Macchina Virtuale Kali** (interfaccia `eth0`).

Quali sono le porte di origine e destinazione?

Porta di Origine (Source Port): 53
Porta di Destinazione (Destination Port): `58273`

Qual è il numero di porta DNS predefinito

Il numero di porta DNS predefinito è **53**.

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

L'osservazione principale è che gli indirizzi (sia MAC che IP) e i numeri di porta sono **esattamente invertiti** tra i due pacchetti.

- **Nel pacchetto di Query (Domanda):** Il tuo computer era la **Sorgente** (Source) perché stava inviando la richiesta, mentre il server DNS era la **Destinazione** (Destination).
- **Nel pacchetto di Risposta (Risultato):** Il server DNS è diventato la **Sorgente** (Source) perché sta inviando i dati richiesti, e il tuo computer è diventato la **Destinazione** (Destination).

Esplorare il Traffico delle Risposte DNS

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

Indirizzi MAC (Livello Ethernet II):

- **Origine (Source):** `52:54:00:12:35:00` (Gateway NAT).
- **Destinazione (Destination):** `08:00:27:bc:64:df` (Tua VM Kali).

Indirizzi IP (Livello IPv4):

- **Origine (Source):** `10.0.2.3` (Server DNS).
- **Destinazione (Destination):** `10.0.2.15` (Tua VM Kali).

Numeri di Porta (Livello UDP):

- **Porta di Origine:** 53 (Porta standard DNS).
- **Porta di Destinazione:** 58273 (Porta dinamica della richiesta).

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

L'osservazione principale è che gli indirizzi e le porte sono **esattamente invertiti**.

- Nel pacchetto di **Query**, la tua VM (`10.0.2.15` con porta `58273`) era la **Sorgente** perché stava inviando la domanda, mentre il server DNS (`10.0.2.3` sulla porta `53`) era la **Destinazione**.
- Nel pacchetto di **Risposta** (quello che vedi ora), il server DNS è diventato la **Sorgente** perché sta fornendo il dato, e la tua VM è diventata la **Destinazione** per ricevere l'informazione.

Il server DNS può fare query ricorsive?

Sì, il server può eseguire query ricorsive. il flag **"Recursion available"** è impostato (bit a 1). Questo bit indica che il server DNS interrogato (con IP `10.0.2.3`) è in grado di cercare le informazioni contattando altri server DNS autorevoli se non conosce già la risposta, restituendo il risultato finale (l'IP di Cisco) invece di rimandare ad altri server.

Come si confrontano i risultati con quelli di nslookup?

Record CNAME: Sia in Wireshark (sotto la sezione *Answers*) che in `nslookup`, vedrai che `www.cisco.com` è in realtà un alias. Wireshark mostra il record di tipo **CNAME** che punta a

un nome di dominio più complesso (ad esempio legato ad Akamai o altri servizi di distribuzione contenuti).

Record A: Entrambi gli strumenti elencano alla fine gli stessi indirizzi IPv4 (Record di tipo **A**). In Wireshark li trovi espandendo ogni voce delle "Answers", mentre in `nslookup` compaiono sotto la voce "Addresses".

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

- **Protocolli di Background**
- **Traffico di Gestione**
- **Comunicazioni Applicative**
- **Broadcast e Multicast**

2. Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?
Un attaccante può utilizzare Wireshark come uno strumento di **ricognizione passiva** estremamente potente. modi principali:

- **Intercettazione di Credenziali (Sniffing)**
- **Analisi del Traffico per il Profiling**
- **Riconoscimento della Topologia di Rete**
- **Data Exfiltration**
- **Session Hijacking**