Analisi del Traffico DNS con Wireshark

Michele Storelli

11 giugno 2025

Dettagli del Pacchetto di Query DNS

Indirizzi MAC

- **MAC di Origine:** `80:89:b4:a1:05`
- **MAC di Destinazione:** `80:89:b4:a1:05`
- **Associazione Interfacce:** Entrambi gli indirizzi MAC sono associati all'interfaccia virtuale del *gateway NAT di VirtualBox* (vista dalla VM). Questo riflette la comunicazione tra la VM e il suo gateway virtuale interno.

Indirizzi IP

- **IP di Origine:** `10.0.2.15`
- **IP di Destinazione:** `10.0.2.3`
- **Associazione Interfacce:**
  - L'IP di origine (`10.0.2.15`) è associato all'interfaccia di rete della *macchina virtuale*.
  - L'IP di destinazione (`10.0.2.3`) è associato all'indirizzo del *gateway NAT virtuale* fornito da VirtualBox alla VM.

Porte UDP

- **Porta di Origine:** `37682` (porta effimera assegnata al client)
- **Porta di Destinazione:** `53`
- **Porta DNS Predefinita:** La porta DNS predefinita è `53`.

Confronto MAC e IP con `ifconfig`

- **IP:** L'IP del PC (`10.0.2.15` dall'output `ifconfig` della VM) *corrisponde* all'IP di origine nel pacchetto Wireshark.
- **MAC:** Il MAC del PC (`08:00:27:b4:a1:05` dall'output `ifconfig` della VM) *NON corrisponde* al MAC di origine nel pacchetto Wireshark (`80:89:b4:a1:05`).

- **Osservazione:** La discrepanza MAC è dovuta alla configurazione NAT della VM. Wireshark cattura il traffico che passa tra la VM e il gateway NAT virtuale (che usa il MAC `80:89:b4:a1:05`), non il MAC effettivo della VM. L'IP rimane quello della VM perché la cattura avviene prima che il traffico lasci il dominio NAT.

Dettagli del Pacchetto di Risposta DNS

Indirizzi MAC, IP e Porte

- **MAC di Origine:** `80:89:b4:a1:05`
- **MAC di Destinazione:** `80:89:b4:a1:05`
- **IP di Origine:** `10.0.2.3`
- **IP di Destinazione:** `10.0.2.15`
- **Porta di Origine:** `53`
- **Porta di Destinazione:** `37682`

Confronto con i Pacchetti di Query

- **IP e Porte:** Gli indirizzi IP e i numeri di porta sono *invertiti* tra query e risposta (l'origine della query diventa la destinazione della risposta e viceversa).
- **MAC:** Gli indirizzi MAC rimangono gli stessi (`80:89:b4:a1:05`) in questo contesto di cattura (tra VM e gateway NAT virtuale).

Capacità Ricorsive del Server DNS

- Dalle `Flags` del pacchetto di risposta, si osserva `Recursion available: Server can do recursive queries` (impostato a 1).
- **Risposta:** Sì, il server DNS (Google DNS 8.8.8.8, tramite il gateway NAT virtuale) è in grado di eseguire query ricorsive.

Confronto con i Risultati di `nslookup`

- I record `CNAME` (`www.cisco.com.akadns.net`, `www.cisco.com.edgekey.net`, `e12867.dscb.akamaiedge.net`) e i record `A` (indirizzi IPv4 come `23.205.59.183`) e `AAAA` (indirizzi IPv6) presenti nella sezione `Answers` di Wireshark *corrispondono esattamente* a quelli restituiti dal comando `nslookup www.cisco.com` eseguito nella VM.
- Questo conferma la coerenza e l'accuratezza dei dati di rete osservati.

Riflessioni

1. Cosa si impara rimuovendo il filtro Wireshark?

Rimuovendo il filtro, Wireshark rivela **tutto il traffico** sull'interfaccia. Si può imparare:

- **Protocolli in uso:** HTTP/HTTPS, ARP, ICMP, TCP, UDP, ecc.
- **Comunicazioni:** Quali dispositivi (IP e MAC) comunicano tra loro, sia sulla LAN che verso l'esterno.
- **Applicazioni:** Servizi attivi e relative porte (web, email, streaming).
- **Problemi di rete:** Errori, ritrasmissioni, latenza, congestione.
- **Dati in chiaro:** Potenziale visibilità di credenziali o dati sensibili se non crittografati.

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

Un attaccante con accesso alla rete può usare Wireshark per:

- **Sniffing di Credenziali/Dati Sensibili:** Intercettare password, username e altre informazioni se il traffico non è crittografato.
- **Riconoscimento della Rete (Footprinting):** Mappare la topologia di rete, identificare dispositivi, sistemi operativi, servizi e vulnerabilità.
- **Analisi Comportamentale:** Comprendere il funzionamento delle applicazioni per identificare punti deboli o tecniche di manipolazione.
- **Estrazione di File:** Ricostruire file trasmessi senza crittografia.
- **Rilevamento di Anomalie:** Individuare attività insolite che potrebbero indicare malware o backdoor.