AMATO SARA

S11 L4

### **Lab – Exploring DNS Traffic**

#### **Obiettivi**

L’obiettivo del laboratorio è esplorare il traffico DNS utilizzando Wireshark, analizzando i dettagli dei pacchetti di query e risposta DNS. Questo esercizio aiuta a comprendere come funziona il protocollo DNS e il suo ruolo nella rete, fornendo una visione dettagliata dei livelli del protocollo e delle potenziali vulnerabilità di rete.

#### **Risorse Necessarie**

* 1 PC con accesso a internet e Wireshark installato.

#### **Scenario**

Wireshark è un potente strumento open source per la cattura e l'analisi dei pacchetti. Permette di filtrare il traffico, diagnosticare problemi di rete, analizzare i protocolli e identificare potenziali vulnerabilità. Tuttavia, il suo uso improprio può rappresentare una minaccia alla sicurezza della rete.

### **Parte 1: Cattura del Traffico DNS**

#### **Passaggio 1: Installazione di Wireshark**

1. Scaricare l'ultima versione stabile di Wireshark da [www.wireshark.org](http://www.wireshark.org).
2. Seguire le istruzioni per l’installazione, evitando l'installazione di USBPcap se non necessaria.

#### **Passaggio 2: Cattura del traffico DNS**

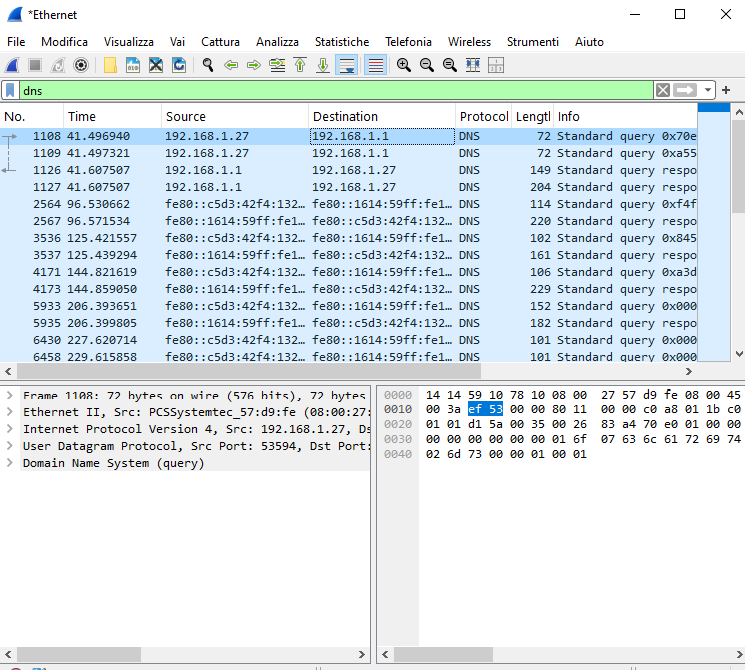
1. **Avvio di Wireshark**:
   * Selezionare un'interfaccia di rete attiva per la cattura del traffico.
2. **Cancellazione della cache DNS**:
   * Windows: Aprire il prompt dei comandi e digitare:  
     ipconfig /flushdns

Linux: Usare uno dei seguenti comandi in base al servizio in uso:  
sudo systemd-resolve --flush-caches

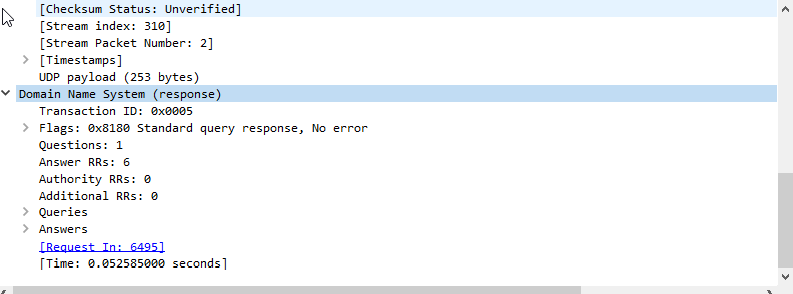
* + sudo systemctl restart systemd-resolved.service
  + macOS: Nel terminale, eseguire:  
    sudo killall -HUP mDNSResponder

1. **Eseguire una query DNS**:
   * Aprire il prompt dei comandi o il terminale, digitare nslookup e inserire il nome del dominio, ad esempio www.cisco.com.
   * Uscire dalla modalità interattiva con il comando exit.
2. **Interrompere la cattura del traffico** cliccando sul pulsante “Stop capturing packets”.

### **Parte 2: Analisi del Traffico DNS Query**

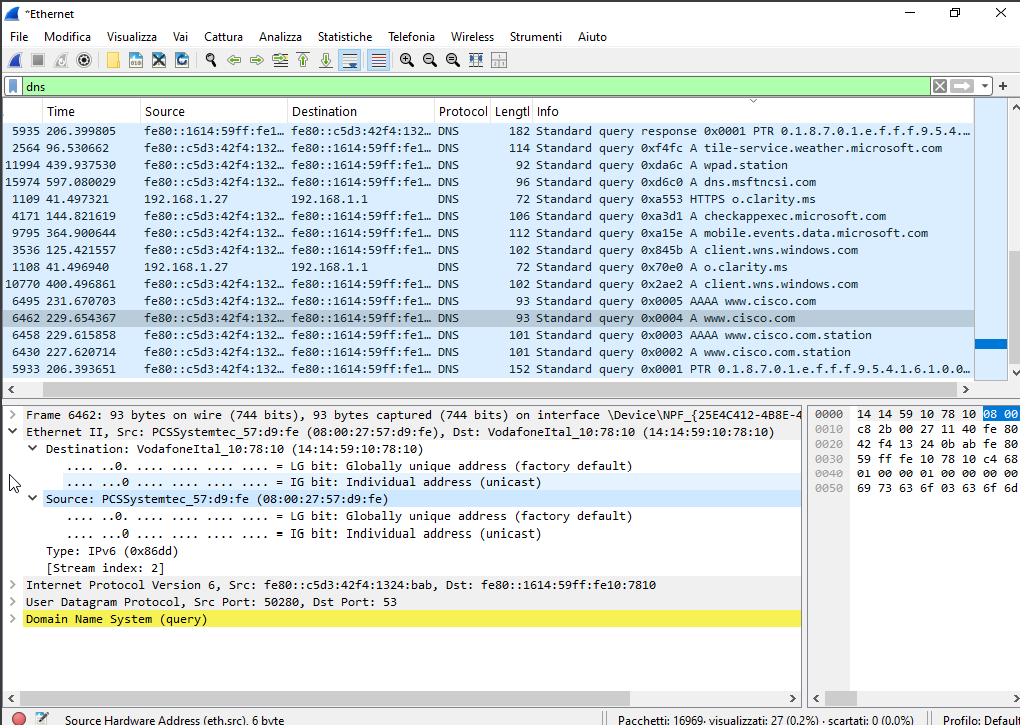


1. **Filtrare i pacchetti DNS**:
   * Inserire udp.port == 53 nella barra dei filtri di Wireshark per visualizzare solo i pacchetti DNS.
2. **Selezione del pacchetto**:
   * Trovare un pacchetto che contenga **Standard query** e il nome del dominio richiesto (es. A www.cisco.com).
3. **Analisi dettagliata del pacchetto**:
   * Espandere le seguenti sezioni:
     + **Ethernet II**:
       - Osservare i campi:
         * **MAC sorgente**: Indica la scheda di rete del PC.
         * **MAC destinazione**: Indica il gateway predefinito o il server DNS locale.
     + **Internet Protocol Version 4**:
       - **IP sorgente**: Indirizzo IP del PC.
       - **IP destinazione**: Indirizzo IP del gateway o del server DNS.
     + **User Datagram Protocol (UDP)**:
       - **Porta sorgente**: Porta temporanea assegnata dal PC (es. 57729).
       - **Porta destinazione**: Porta standard DNS (**53**).
4. **Confronto degli indirizzi IP e MAC**:
   * Utilizzare il comando arp -a e ipconfig /all (Windows) o ifconfig (Linux/macOS) per verificare gli indirizzi IP e MAC del PC.
   * Confrontare i risultati con quelli dei pacchetti DNS catturati in Wireshark.
5. **Dettagli sulla query DNS**:
   * Espandere la sezione **Domain Name System (query)**.
   * Notare che il flag indica che la query è ricorsiva.



### **Parte 3: Analisi del Traffico DNS Response**

1. **Selezione del pacchetto di risposta DNS**:
   * Trovare un pacchetto con **Standard query response** e il dominio richiesto (es. A www.cisco.com).
2. **Analisi dettagliata**:
   * Osservare i campi:
     + **MAC e IP sorgente** nella risposta: corrispondono a quelli di destinazione nella query.
     + **MAC e IP destinazione** nella risposta: corrispondono a quelli di sorgente nella query.
     + **Porta sorgente**: **53** (porta DNS).
     + **Porta destinazione**: Porta temporanea del PC.
3. **Dettagli della risposta DNS**:
   * Espandere **Domain Name System (response)** per visualizzare Flags, Queries e Answers.
   * Notare che il server DNS supporta query ricorsive.
   * Verificare i record **CNAME** e **A** nella sezione Answers. Questi dovrebbero corrispondere ai risultati di nslookup.



### **Riflessioni Finali**

1. **Osservazioni rimuovendo i filtri**:
   * Senza filtri, Wireshark mostra altri tipi di traffico come:
     + **DHCP**: Per l’assegnazione degli indirizzi IP.
     + **ARP**: Per la risoluzione degli indirizzi IP in MAC.
   * Questi pacchetti offrono informazioni sulla configurazione della rete locale.
2. **Uso di Wireshark da parte di un attaccante**:
   * Un attaccante con accesso alla LAN può:
     + Intercettare pacchetti non crittografati per ottenere credenziali o dati sensibili.
     + Analizzare la topologia di rete per pianificare attacchi.
   * La crittografia del traffico (es. HTTPS, SSH) riduce significativamente questo rischio.