S11/L3

Parte 1 – Catturare il traffico DNS

1. **Cattura del traffico**

   a. Ho avviato Wireshark e selezionato l'interfaccia di rete attiva

   b. Ho svuotato la cache DNS sul mio sistema tramite questo script:

   => **sudo systemctl restart systemd-resolved.service**

3. c. Ho aperto un terminale e digita **nslookup**, poi esegui la query:

   > nslookup

   > www.cisco.com

d. Ho digitato exit per uscire da nslookup => sono ritornato in Wireshark ed ho premuto il pulsante **Stop** per interrompere la cattura.

4. **Applicare il filtro DNS**
   - Nel campo del filtro in alto digita

     udp.port == 53

     e premi Invio per far vedere solo i pacchetti DNS.

Parte 2 – Esplorare il traffico delle query DNS

1. **Individuare il pacchetto di query**
    - Ho cercato tra i pacchetti filtrati quello che in info riportava:
    - **Standard query A www.cisco.com**

2. **Dettagli livello Ethernet**
    - Ho esteso **Ethernet II** nel riquadro Packet Details.
        - **Domanda:** Quali sono gli indirizzi MAC di origine e destinazione?

          Mac di Destinazione: 1e:f6:4c:39:6f:64

          Mac di Origine: c2:b4:53:c0:93:98
        - **Domanda:** A quali interfacce di rete sono associati questi MAC?
            - Il MAC di origine appartiene alla scheda di rete del mio PC; quello di destinazione alla scheda del router/DNS server locale.

3. **Dettagli livello IP**
    - Ho esteso **Internet Protocol Version 4**.
        - **Domanda:** Quali sono gli indirizzi IP di origine e destinazione?
            - **Origine (IP PC):** 192.168.64.10
            - **Destinazione (IP DNS):** 192.168.64.1
        - **Domanda:** A quali interfacce di rete sono associati questi IP?
            - L'IP di origine è quello assegnato al mio PC; l'IP di destinazione è l'indirizzo del DNS server (tipicamente il router o un server interno).

4. **Dettagli livello UDP**
    - Ho esteso **User Datagram Protocol (UDP)**.
        - **Domanda:** Quali sono le porte di origine e destinazione?
            - **Porta sorgente (effimera):** 35220

        - **Porta destinazione:** 53
    - **Domanda:** Qual è il numero di porta DNS predefinito?
        - **53**

5. **Confronto con indirizzi MAC/IP locali**
    - Sul mio PC:
        - **Linux/macOS: ifconfig** o **ip address**
    - **Domanda:** Confronta gli indirizzi MAC e IP di Wireshark con quelli restituiti dal tuo sistema. Qual è l'osservazione?
        - Il MAC / IP del PC mostrato da Wireshark corrisponde a quello elencato dal sistema operativo.
6. **Flag e query DNS**
    - Ho esteso **Domain Name System (query)**, poi **Flags** e **Queries**.
    - Ho costatato che il flag **RD** (Recursion Desired) è impostato, quindi la query richiede risoluzione ricorsiva.

Parte 3 – Esplorare il traffico delle risposte DNS

1. **Individuare il pacchetto di risposta**
    - Ho cercato il pacchetto con **Standard query response A www.cisco.com**.
2. **MAC, IP e porte**
    - Ho esteso Ethernet II, IPv4 e UDP.
        - **Domanda:** Quali sono gli indirizzi MAC e IP e le porte di origine e destinazione?
            - **MAC sorgente (DNS):** 1e:f6:4c:39:6f:64
            - **MAC destinazione (PC):** c2:b4:53:c0:93:98
            - **IP sorgente (DNS):** 192.168.64.1
            - **IP destinazione (PC):** 192.168.64.10
            - **Porta sorgente:** 53
            - **Porta destinazione:** 35220

- **Domanda:** Come si confrontano con gli indirizzi nei pacchetti di query?
  - Sono invertiti rispetto alla query: la sorgente iniziale muta in destinazione e viceversa.

3. **Flag e record DNS**
   - Ho esteso **Domain Name System (response)**, poi **Flags**, **Queries**, **Answers**.
     - **Domanda:** Il server DNS può fare query ricorsive?
       - Si il flag **RA** (Recursion Available) risulta impostato a 1, indica supporto alla ricorsione.
     - **Domanda:** Osserva i record CNAME e A. Come si confrontano con quelli di nslookup?
       - **Answers record A:** 104.85.9.21
       - N**slookup:** riporta lo stesso indirizzo IP per www.cisco.com.

Riflessione

1. **Rimuovendo il filtro UDP 53**
   - Vedi tutto il traffico: **ARP, DHCP, HTTP/HTTPS, DNS** inverso, **mDNS**.
   - Puoi scoprire quali host comunicano, quali protocolli usano, tempi di latenza, volumi di traffico.

2. **Uso di Wireshark da parte di un attaccante**
   - **Sniffing**: di pacchetti non cifrati (**HTTP, FTP, SMTP**): cattura credenziali, cookie, dati sensibili.
   - **Ricognizione**: scoperta della topologia di rete, indirizzi **IP** e **MAC** di dispositivi critici.
   - **Session hijacking**: sfruttamento di informazioni di sessione non protette.
   - **Analisi**: del traffico **DNS** può rivelare quali domini gli utenti stanno visitando.