nslookup ⇒ Scoprire IP associato ad un NOME

www.univr.it

Ho il riferimento a chi paga questo servizio, quindi la persona

WhoIs ⇒ Mi dice CHI, ma in Carne ed Ossa, Nome e Cognome di chi ha Quell'IP oppure DOMINIO

univr.it

Ma Sono Ben diversi

WHOIS [SITO]
NSLOOKUP [DOMINIO]
WHOIS DELL'[IP]

ESERCIZIO TIPO ESAME PER CAPIRE SE UN AZIENDA SI È FATTA IL SITO WEB DA SOLA o MENO

WIRESHARK Interpreta i pacchetti Essendo che Conosce i protocolli e anche da che Pezzo di Hardware Arriva

HEADER DEL LVL PRECEDENTE mi da la Semantica dei BIT (non posso trovare Semantica all'interno della Sequenz.)

ETHERNET:

- PREAMBOLO ⇒ per Sincronizzarsi con il RICEVITORE
- DST. MAC e POI SOURCE MAC
- CAMPO DA 2 BYTE PER IL PROTOCOL TYPE

dello Standard 802.3 nel campo di 2 BYTE si Chiama LEN, ovvero la lunghezza del PAYLOAD.

→ Sul CAVO NON esiste il Vuoto, devo Sapere QUANDO Smettere di LEGGERE

→ Questa Soluzione però è Stata poco Utilizzata ed ha Prevalso Quella Vecchia.

PACCHETTI BROADCAST ⇒ con MAC con tutti 48 Bit a 1 (FF:...)

ARP ⇒ da Indirizzo MAC ad IP

Cavo ETH Moderno è attaccato allo SWITCH, quindi fa da COMMUTATORE e quindi su Quel Cavo gira Solamente il Mio Traffico + Broadcast (IL CHE AUMENTA SICUREZZA ed EFFICIENZA)

Ed è da QUI che se faccio Cattura ETHERNET catturo molto BROADCAST.

ARP POISONING ⇒ confondere Lo SWITCH per Vedere il Traffico degli ALTRI

Anche su ETH posso Configurare una PSW per Autenticarsi ma è raro visto che QUANDO CI SI COLLEGA si sa chi è...il Contrario del WI-FI dove è fortemente Consigliata

Devo CONOSCERE Benissimo come si APRE una CONNESSIONE HTTP che si Basa su TCP

→ Assicura AFFIDABILITÀ che COSTA in Termini di EFFICIENZA

DNS Basato su UDP (PROTOCOLLO DI LVL APPLICAZIONE) ed infatti Necessita di 2 pacchetti

In TCP posso Raggruppare tutti i pacchetti Mentre UDP NO

SSH ⇒ secure

FTP = Non è Sicuro, PSW disponibile su WIRESHARK

→ NON credere che sia Sicuro se ci Sono ** mentre digito la PSW.
Bisogna ASSOLUTAMENTE USARE PROTOCOLLI CIFRATI

Tempi di Viaggio su INTERNET variano, come anche la STRADA e per QUESTO il ROUND TRIP TIME varierà Sempre

TRACEROUTE ⇒ Mostra tutti gli HOP che Vengono Attraversati, non funziona Sempre (CONFIGURAZIONE DEL ROUTER)

Rispondere ai ICMP diventa una VULNERABILITÀ perchè ci SI RIVELA (si fa vedere che ci siamo) e quindi spesso si disabilita la RISPOSTA