Analizzatori di Rete:

Wireshark è il Principale

Strumento come KIT di DIAGNOSTICA ma anche per Acquisire Nozioni Sulle Reti

Analizzando una Rete la si Va a Studiare

Analizzatore di Protocollo: Guardo i Pacchetti (GRUPPI BYTE) che si Chiama PDU (Protocol Datagram Unit)

→ DA USARE

Protocollo Trasferisce Segmenti di BYTE

Grazie All' Imbustamento Multiplo 2 Entità si Parlano a lvl fisico

Sembra che 2 Entità si Parlano allo Stesso livello in ORIZZONTALE Attraverso un PROTOCOLLO ma in Realtà NON è così perchè comunicano tutti a Livello FISICO

PROTOCOLLO = Convenzione, dare Significato ai BIT Tra 2 Entità dello Stesso livello (SEMANTICA DEI BIT)

Protocolli Sono Scampi di PDU, ad Esempio TCP Serve il 3-WAY HANDSHAKE (IMPLEMENTAZIONE DEL PROTOCOLLO)

Protocollo da Significato ai BIT.

PDU composto da Header e Payload. → PDU diventa PAYLOAD del Lvl SOTTOSTANTE

Grazie All' Imbustamento (SEPPUR INEFFICIENTE) ho la MODULARITÀ tra Livelli (CHE SONO INDIPENDENTI TRA DI LORO)

È Come una LETTERA: Lettera Interna con Contenuto
Busta con INFO per Spedizione

HEADER: Indirizzo Mittente } STRETTAMENTE NECESSARI
Indirizzo Destinazione }

ANALIZZATORI

① Catturano PDU

② Interpretano Queste PDU ⇒ Possono Restituire all' Utente la possibilità di leggere le INFO (DEBUGGER DELLE RETI)

L'Altra Metà di WIRESHARK è che CATTURA IL TRAFFICO e può anche Interpretarlo ma come può anche INTERPRETARE Traffico già Catturato

Utile Anche Separare Momento Cattura da Quello dell' Analisi

Coinvolge HARDWARE (scheda di Rete) → Basso livello

Coinvolge la Grafica → Più USER FRIENDLY

Ci deve ESSERE Sempre una Scheda di Rete, ma ci Sono più Interfacce:

- Ethernet
- Wi Fi
- Bluecthooth
- USB (teethering con Telefono Esempio)

Ragionare In Termine di INTERFACCIA perchè è QUELLA che lavora anche Sugli HOST e NON Solo sui ROUTER.

Provare su Terminale: ifconfig -a

che mi Va ad Elencare tutte le Interfacce di Rete disponibili sia Attive che NON

Interfaccia LOOPBACK c'è Sempre anche in Mancanza di Altre

→ Interfaccia di Rete Virtuale con Me Stesso per fadi Comunicare Come Se fossero in RETE ma Sono Sullo Stesso PC.

Esempio: Programma di Chat devo Usare Wireshark e Cattucare Sulla LOOPBACK

Virtual Machine ti da ILLUSIONE di Avere un HARWARE che NON HAI perchè è un VIRTUALIZZATORE e non EMULATORE

Ci Sarà Anche SCHEDA DI RETE VIRTUALE che Viene Segnata assieme alle Altre fisiche della mia Macchina.

Stessa Cosa per DOCKER (container)

LIVELLO BASSO WIRESHARK ⇒ Libreria pcap che comunica con S.O. e lo Deve Scavalcare su un INTERFACCIA specifica.

PDU Ethernet di Lvl. 2 : Mittente e Destinazione con Indirizzi MAC a 48 Bit ed è Importante l'ordine Qui

(NON LVL 3) ⇔ PRIMA DESTINATARIO ⇒ Ricevitore è la prima cosa che legge dopo il PREABOLO, così POI non ascolta più SE NON è per Lui

Per Sync del Ricevitore

① Si Scarica il DISPOSITIVO
② Spreco Tempo

Sistema Operativo ha Questo Compito

Quando faccio DEBUG Voglio Catturare tutto Quello che Passa e NON Solo Quelli Indirizzati a Me o BroadCast (FF:FF:FF:FF:FF:FF)

e NON tutto

MODALITÀ PROMISCUA ⇒ Un flag che Se Messo a 1 della Scheda di Rete che Passa di lì Viene passato alla CPU (Quindi a WIRESHARK) e viene Copiato Nel file di Copiatura.

Qualsiasi PDU che Arriva viene Mandato un INTERRUPT e può

diventare molto ma macchina pesante come processo (poiché Wireshark consuma troppo e quindi posso decidere quale delle 2 attivare)

Processo SW che agisce su HW deve essere lanciato come ADMIN quindi con SUDO davanti (permessi di ROOT)

2 TIPI DI FILTRI:

Qualcosa che lascia passare o meno Qualcosa

definito da un EXP. Booleana

① FILTRO DI CATTURA ⇒ chi rispetta L'ESPRESSIONE BOOLEANA viene copiato altrimenti NO. (alleggerire il lavoro)

② FILTRO DI VISUALIZZAZIONE ⇒ Data una cattura decido cosa visualizzare per SEMPLIFICARE LA VISUALIZZAZIONE

COME VIRTUALIZZO:

HOST-ONLY ⇒ Come tirare un cavo punto punto alla macchina host

DEFAULT

NAT ⇒ VirtualBox fa da NAT per macchina virtuale e NON ci devo pensare più io (ed io ho già 2 NAT avendo IP PRIVATO)

BRIDGED ⇒ Come se GUEST e HOST fossero su una LAN switchata e devo mettergli un IP (diventa sorella del HOST)

Comandi Utili:

Ping ⇒ Verificare la Raggiungibilità di un Computer con RTT, Round Trip Time (tempo tra invio e risposta). Utilizzando ICMP come Protocollo

Internet Control Protocol ⇒ Per scampio di Informazione sui Malfunzionamenti

TraceRoute ⇒ Strumento per Tracciare il Percorso di un pacchetto dalla sorgente alla destinazione. Vengono Mostrate tutte le Interfacce dei Router Attraversate, a volte ci sono **** dai Router che non Condividono info (Malware)

NsLookup ⇒ Per Interrogare i Server DNS per ottenere da un hostname un IP o Viceversa. Ci sono 2 Modalità:

1. **Interativa:** Di default, effettua più Interrogazioni e Mostra i Risultati Singoli
2. **Non Interativa:** Una Sola Interrogazione

If Config ⇒ Per Configurare e Controllare un Interfaccia di rete

Route ⇒ Visualizzare e Modificare le Tabelle di Routing

WhoIs ⇒ Mediante Appositi db Stabilire Info