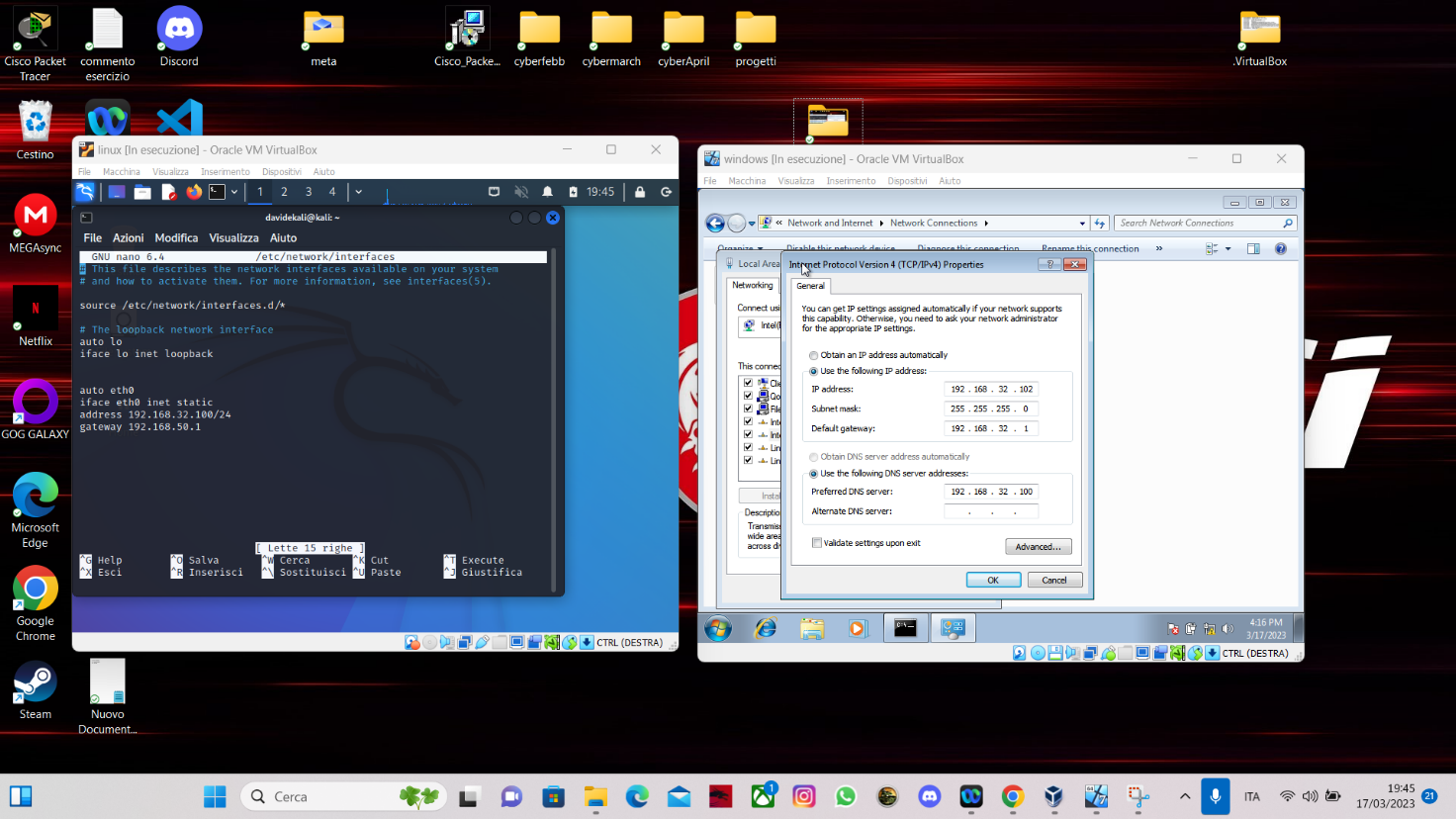
PROGETTO



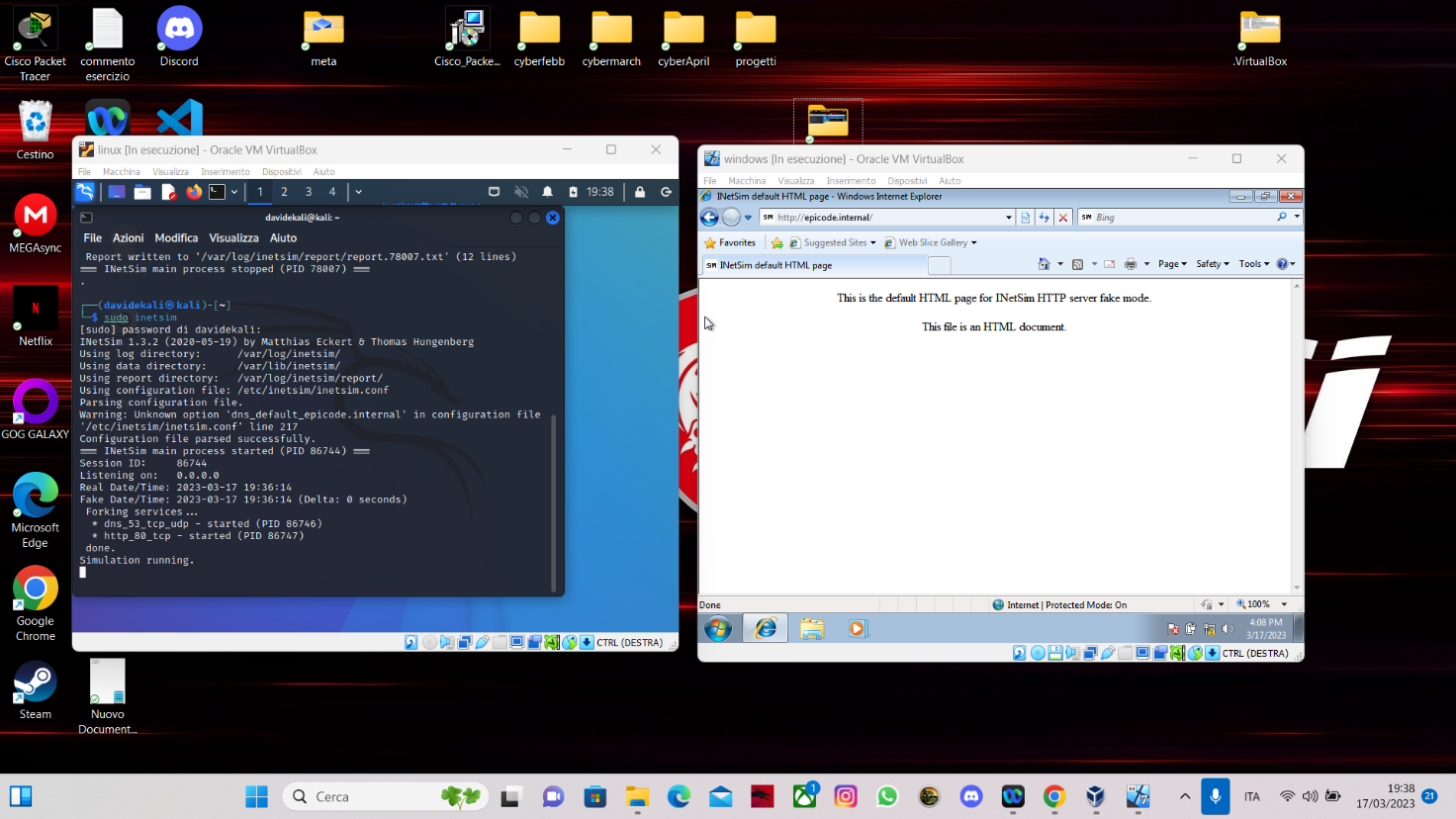
Step1: come si evince dall’immagine noteremo che gli indirizzi ip sono stati inserite staticamente

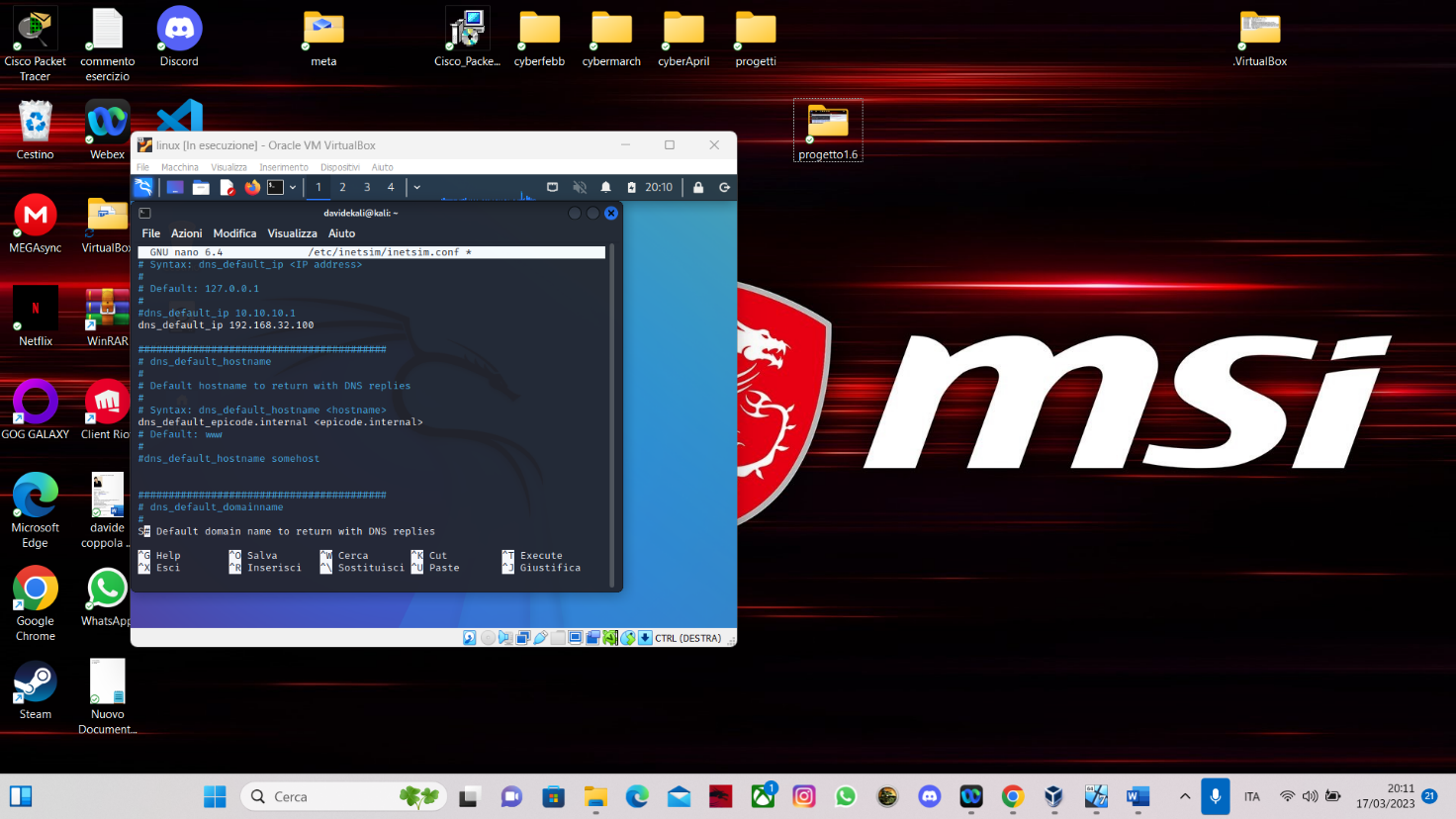
Linux---🡪 dal terminale ho usato il comando sudo nano /etc/network/interfaces

Windows----🡪 per windows sono dovuto andare sul pannello di controllo: selezionato la voce network and internet, andare su cambiare impostazioni, su l’interfaccia local area connection , selezionare le sue proprietà ed impostare come protocollo ipv4 , e da li immetere gli indirizzi statici come potete vedere in foto

Step2 verificare che le macchine comunicano

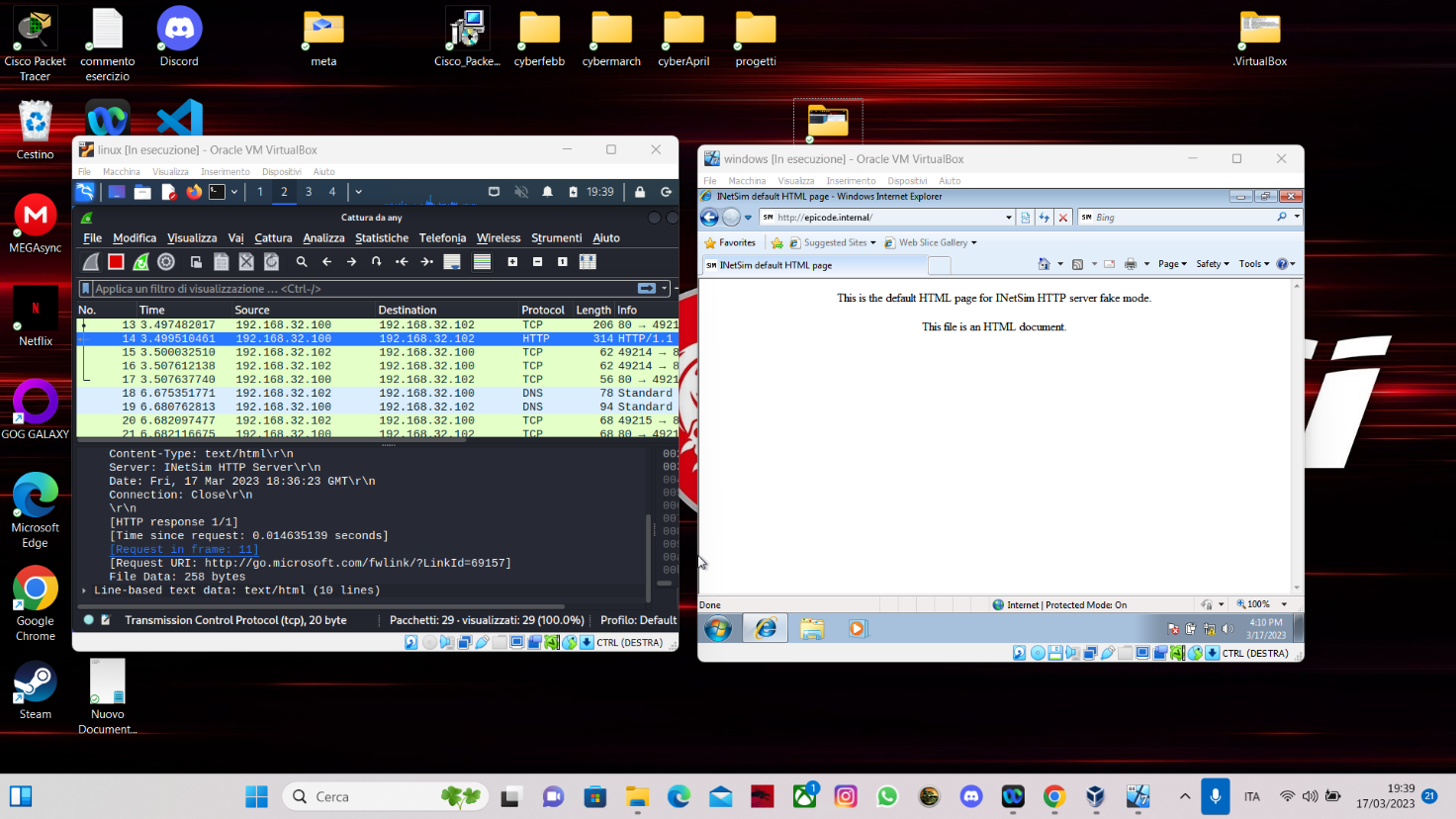
Per verificare che le macchine comunicano , basta semplicemente pingare i loro rispettivi ping tramite i loro i terminali, ma ricordiamo una cosa ,windows ha il firewall , per far si che kali pinga con windows bisogna cambiare le regole del firewall in modo tale che l’indirizzo ip di kali sarà registrato come amico e dunque il firewall lascerà passare i rispettivi pacchetti

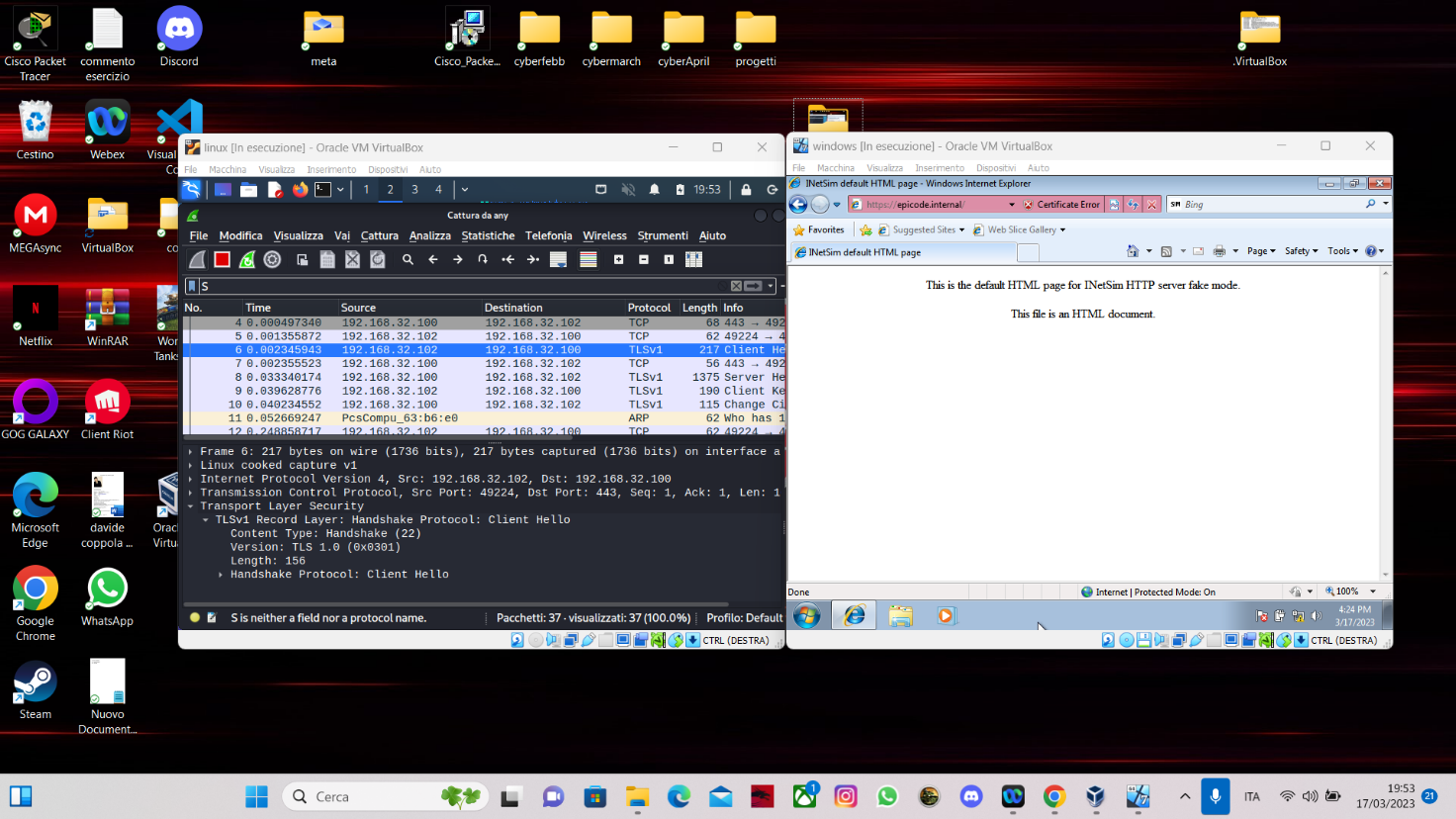




Step3 usare la macchina kali linux come server DNS per windows e configurare il nome <epicode.internal>

Come default , tramite la nostra inetsim come vedrete nelle figura sopra una volta configurato il dns,http,https , andiamo sulla macchina virutale windows aprire

Internet explorer e digitare sulla ricerca il nome di epicode.internal

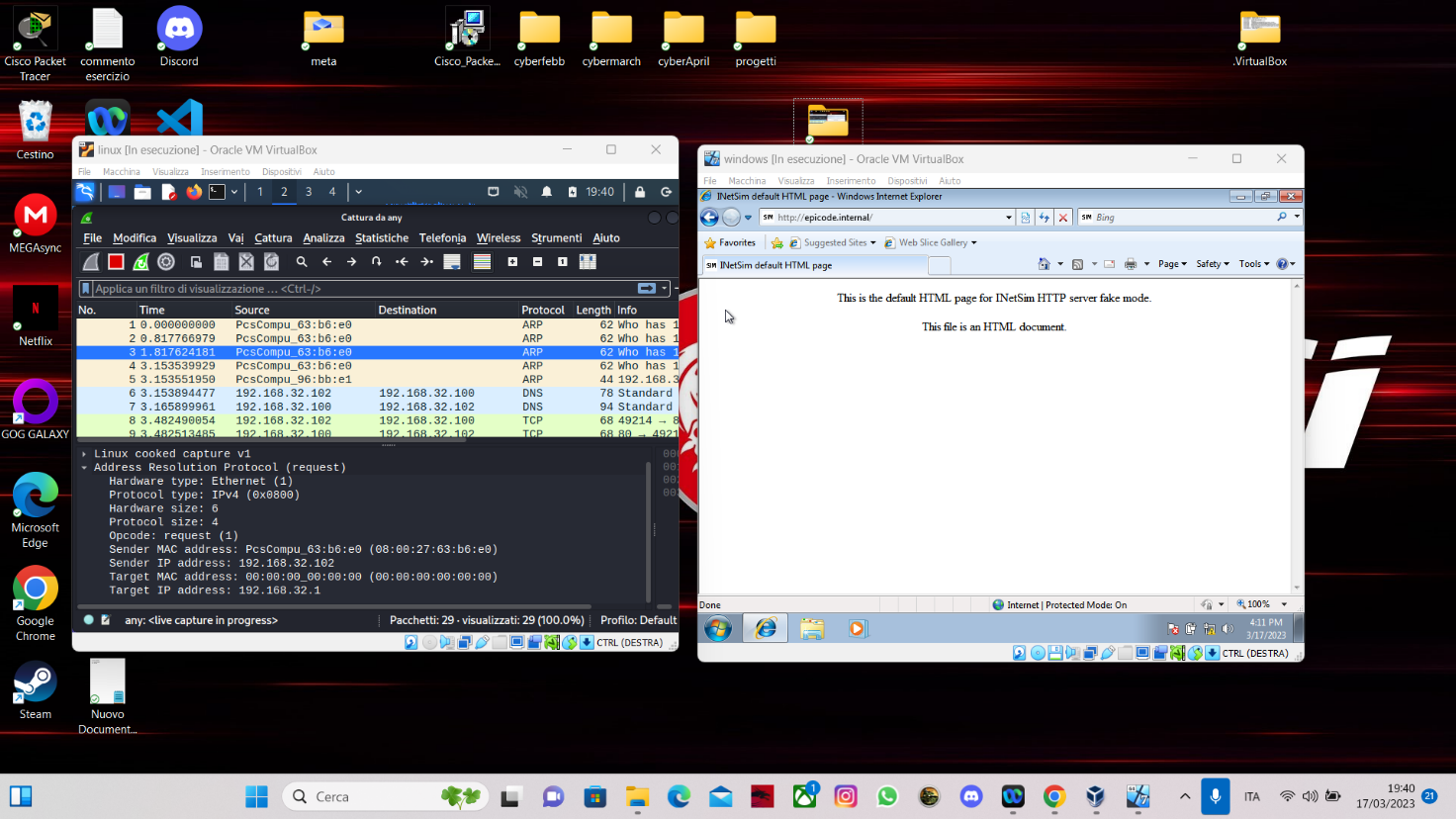
Step4 arrivati a questo punto utilizziamo il nostro tool di sniffing WIRESHARK usato per catturare e tracciare i rispettivi pacchetti che si scambiano il nostro client con il nostro server, usando il protocollo http piu avanti Vedremo il protocollo di https, e commenteremo le rispettive differenze tra pacchetti tracciati

Step5 questa volta come enunciato nello step precedente , siamo andati a fare le stesse esecuzione ma stavolta usando il protocollo hhtps, in primo luogo l’occhio cade subito sul tipo di protocollo catturato

Da WIRESHAR e noteremo l’acronimo tls , ma questo perché??

Perche https è un protocollo cifrato in quanto permette di scambiare le informazioni tra client e server in

modo sicuro



Step finale tracciare gli indirizzi MAC

Come si evince in figura per verificare gli indirizzi mac troviamo in un pacchetto catturato il protocollo ARP

ma cosa significa arp?? , ADDRESS RESOLUTION PROTOCOL , la quale funzione è fornire la mappatura tra l’indirizzo ip e appunto l’indirizzo mac

Differenze tra http/https

quando catturiamo i paccchetti con wireshark, si ottiene una traccia di tutti i pacchetti che attraversano l'interfaccia in cui viene

seguito wireshark, se andiamo a sostituire un server https con un server http cosa vedremo??

la differenza dei pacchetti catturati dipendono principalmente dal protocollo utilizzato per la comunicazione tra il client e il server.

in particolare, con un server https la comunicazione tra client e server avverrà tramite una crittografia che usa protocolli SSL/TLS

che renderà illeggibili i pacchetti a chiunque non sia autorizzato a decifrarli.

Invece se utilizziamo un server hhtp ,la comunicazione tra client e server non è protetta da crittografia alcuna,questa assenza di

mancata protezione causerà che, tutti i pacchetti catturati da enti esterni non autorizzati saranno visibilmente leggibili,dunque un

black hat potrà leggere informazioni sensibili come per esempio :intestazione http, i dati del corpo e della richiesta,credenziali e

altre informazioni sensibili leggibili che viaggiano in rete