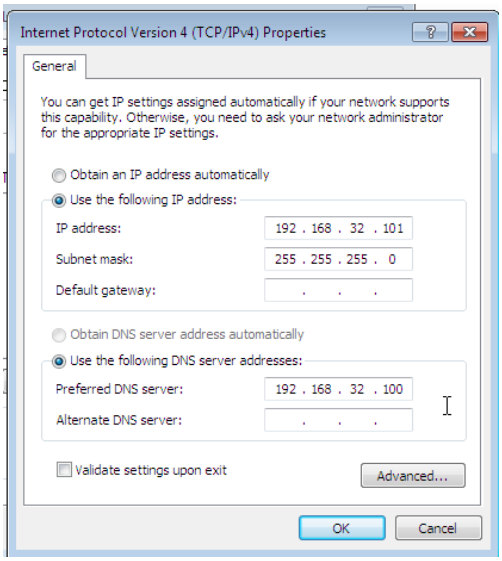
Di giampietro Gabriele **28-10-2022**

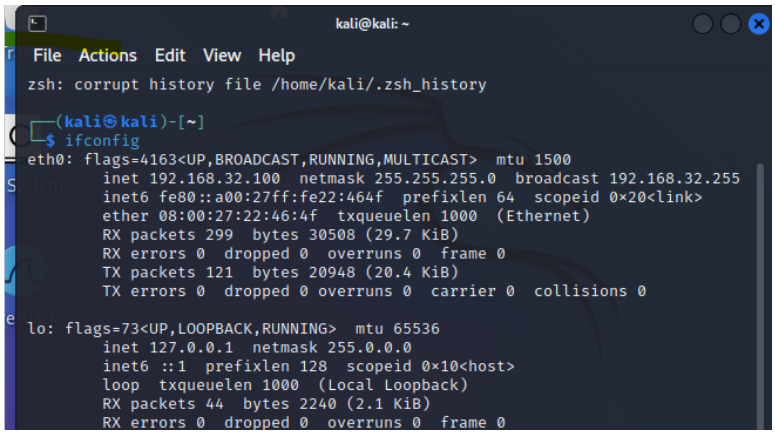
Esercitazione, costruzione di una rete complessa: simulare in ambiente di laboratorio virtuale un'architettura di rete che permetta ad un client di richiedere tramite web browser una risorsa all'hostname epicode.internal, controllare attraverso Wireshark la comunicazione evidenziando i MAC address di sorgente e destinazione. Catturare inoltre il traffico dati cambiando il server HTTP e HTTPS costatando se vi sono differenze.

FASE 1

Nella prima fase della nostra esercitazione abbiamo settato gli ip di entrambe le nostre VM, cosi impostati: Windows 7 192.168.32.100; Kali 192.168.32.100.

Come possiamo vedere nelle figure seguenti, ho già impostato l'ip 192.168.32.100 corrispondente alla VM Kali come DNS server del client che nel nostro caso sarà la VM Window7 (nelle sue properties TCP/ipv4).

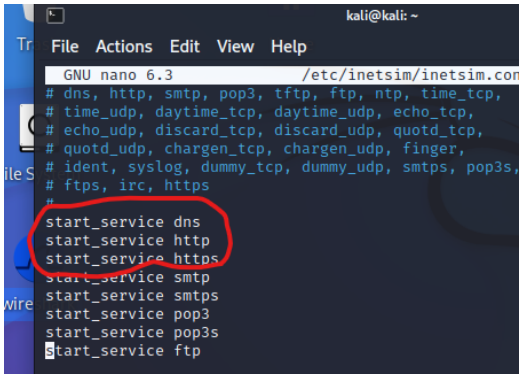




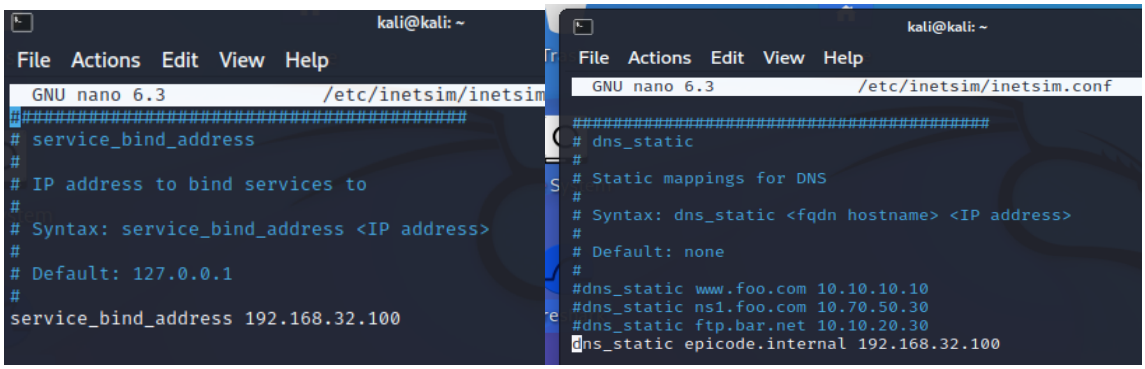
FASE 2

Nella seconda fase ho impostato la configurazione del tool Inetsim su Kali, così da avere la nostra simulazione di server DNS che andrà così a tradurre la ricerca del nostro client da ip al nostro hostname epico.internal. Il comando per aprire il settaggio: sudo nano /etc/inesim/inetsim.conf .

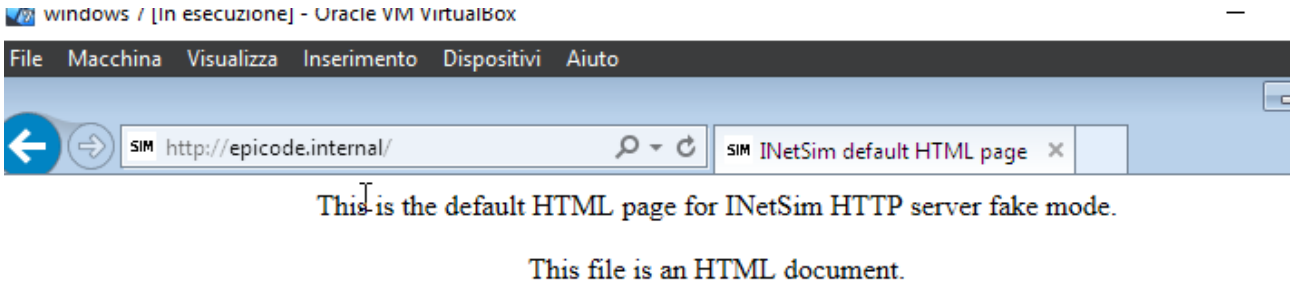
Come possiamo vedere nelle figure seguenti, il servizio server HTTP e HTTPS sono già attivi di default sul tool Inetsim sulla stringa start_service cerchiata in rosso, ovviamente anche il servizo di DNS.



Poi continuando con il settaggio di Inetsim ho impostato il comando service_bind_address con l'ip192.168.32.100, così da aprire il traffico dati di tutte le macchine nella nostra rete interna, quindi Windows 7, proprio verso Kali nel quale simuleremo appunto il nostro server. Ed infine imposteremo nella sezione dns_static: dns_static epicode.internal 192.168.32.100.

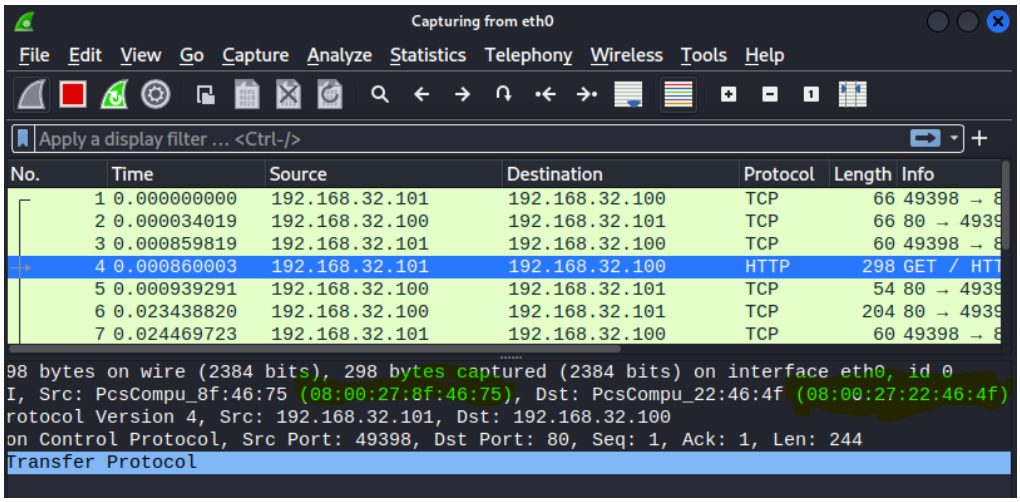


Controllando sul browser del VM Windows 7 e cercando epicode.internal riusciamo così a raggiungere il sito di prova generato dal server simulato da Inetsim su la VM Kali.

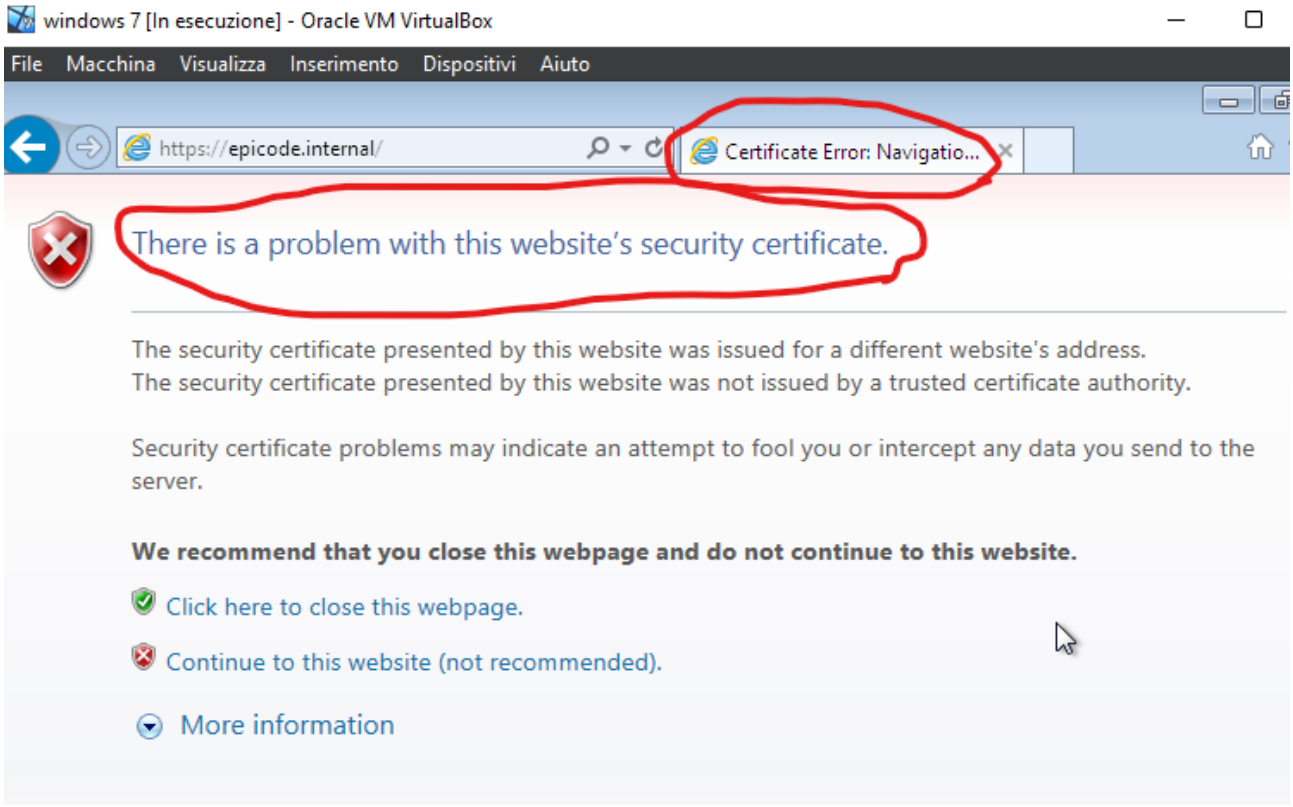


FASE 3

Nell'ultima fase attraverso il tool Wireshark (selezionando Eth0) ho potuto cattura il traffico dati dei vari protocolli, in questo caso controllando per primo il protocollo HTTP. Come vediamo dalla figura che segue possiamo evidenziare nel pacchetto selezionato il MAC address di sorgente: 08:00:27:8f:46:75 e il MAC address di destinazione: 08:00:27:22:46:4f (evidenziati in verde nella figura, mentre nella riga sotto abbiamo i rispettivi indirizzi ip).



In fine abbiamo controllato sempre attraverso Wireshark (selezionando Eth0) se ci fosse differenza nei pacchetti trasmessi nel protocollo HTTPS. Sempre attraverso la VM Windows 7, nel browser avviamo la nostra ricerca di epicode.internal ma modificando in HTTPS nel url e da subito notiamo come il Firewall di windows ci avvisa della pericolosità della pagina visitata, questo già dimostra come l'HTTPS in questo caso non riuscendo ad avere la certezza che il dominio sia sicuro ci informa la rischiosità del dominio visitato, dando errore del suo certificato di sicurezza come vediamo cerchiato in rosso nella figura.



Anche attraverso Wireshark possiamo notare la differenza di trasmissione protocolli, dove alcuni vengo definiti non criptati e nel protocollo TCP vediamo il Flag RST (richiesta di reset della connessione) come possiamo vedere cerchiato in rosso nella figura seguente.