D8 INTRODUZIONE ALLA SICUREZZA NEI SISTEMI OPERATIVI

PROGETTO (FINE MODULO)

RELAZIONE:

Avviato VB, le macchine Kali (server) e W7 (client).

Configuriamo IP statici di server e client, per Kali da terminale e per W7 da impostazioni di rete:

- Da Kali attraverso sudo nano /etc/network... , poi con sudo reboot e ifconfig di verifica;

- Da W7attraverso impostazioni di rete modificando Internet protocol version 4 Ipv4 con nuovo IP address e come preferred DNS server l'indirizzo IP Kali (server).
  Inoltre possiamo disattivare il firewall di windows per semplicità o modificare una regola ad-hoc che chiamiamo “epicode.internal”.

Ora configuriamo i servizi HTTPS e DNS da Kali con sudo nano /etc/inetsim... : attiviamo rimuovendo # i servizi http, https e dns; modifichiamo il servizio bind address e il servizio dns default ip ed effettuiamo un sudo reboot.

Ora siamo pronti di abilitare servizi tramite inetsim:sudo inetsim da Kali.

Test di connessione per client W7 con kali da prompt cmd terminale tramite ping ip e da Internet explorer su W7. Apertura poi di Wireshark per lancio pacchetti con indirizzo HTTP e prima cattura dei protocolli.

Test di connessione per client W7 allo stesso modo del precedente con configurazione indirizzo HTTPS e lancio di IE da W7. Apertura poi di Wireshark per lancio pacchetti con indirizzo HTTPS e seconda cattura dei protocolli.

Si possono notare dalle due diverse catture (HTTP e HTTPS) da Wireshark le differenze tra i vari pacchetti.