**Relazione esercitazione 1: Simulazione rete complessa**

Data la consegna, andiamo ad impostare un’architettura CLIENT-SERVER in ambiente di laboratorio virtuale (Win7 / Kali Linux) attraverso i seguenti step:

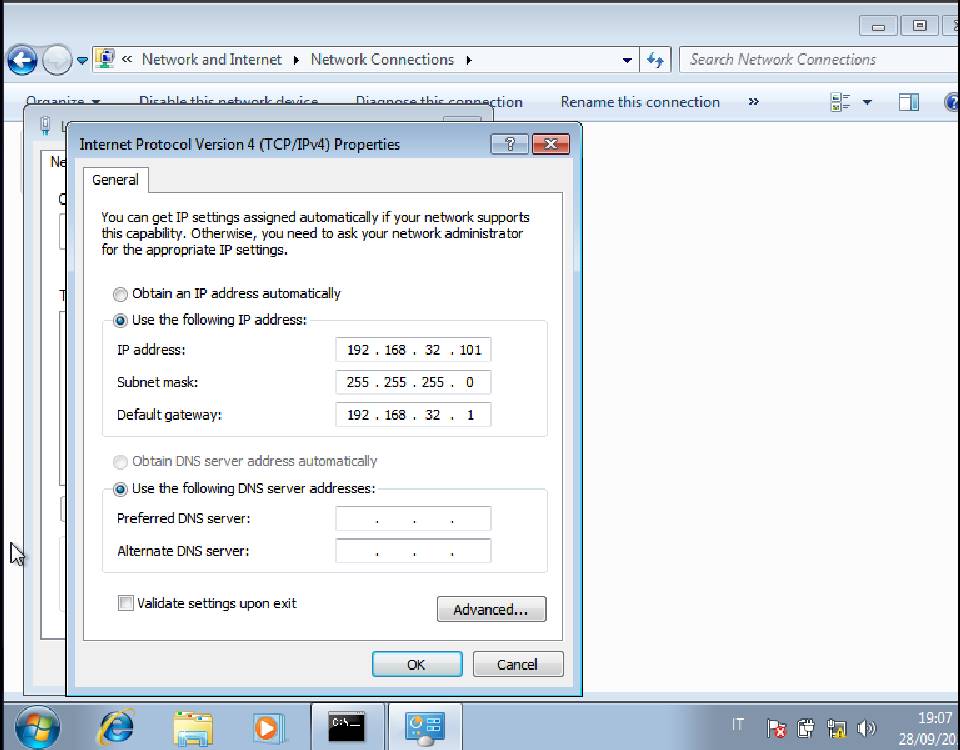
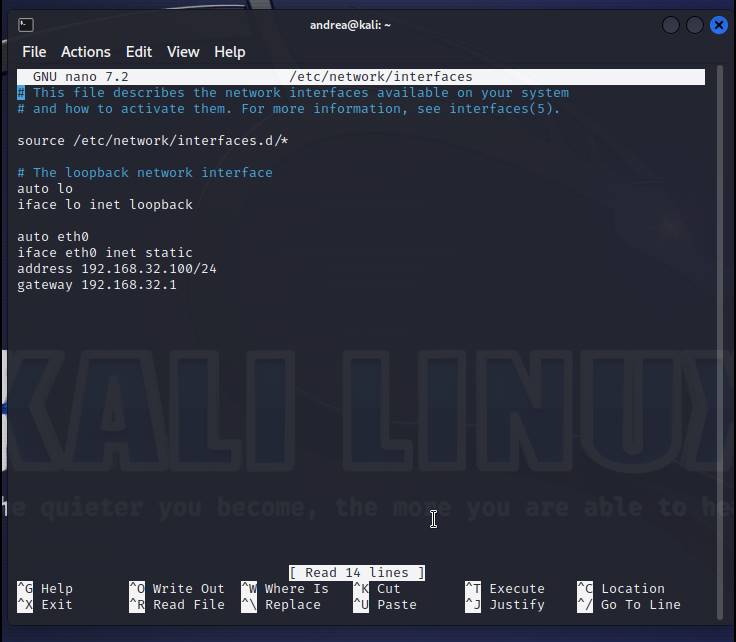
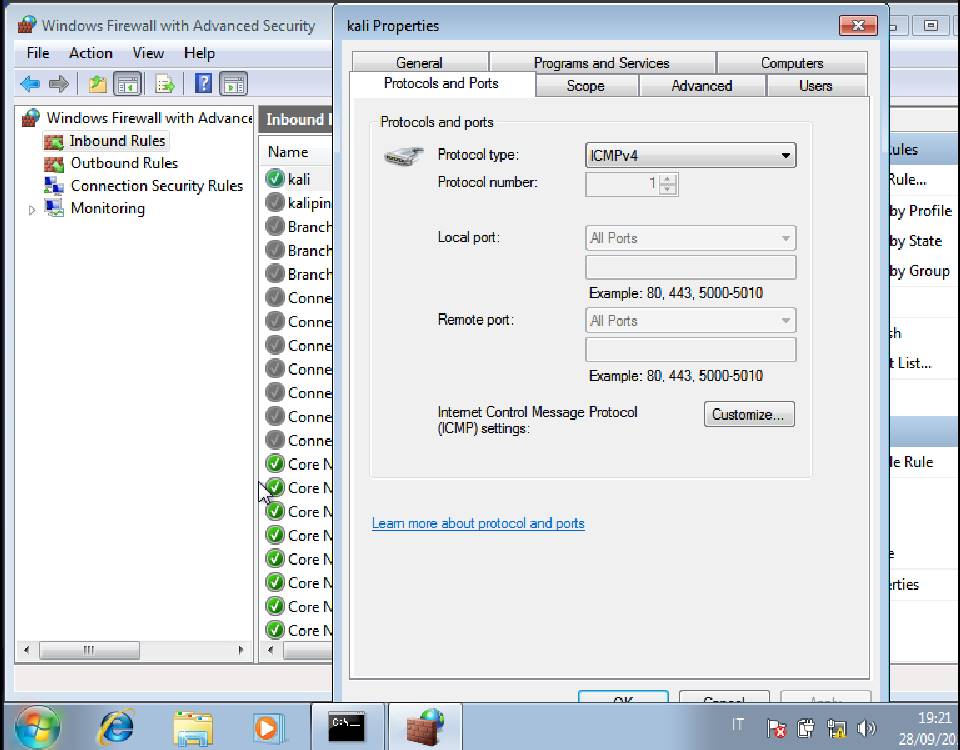
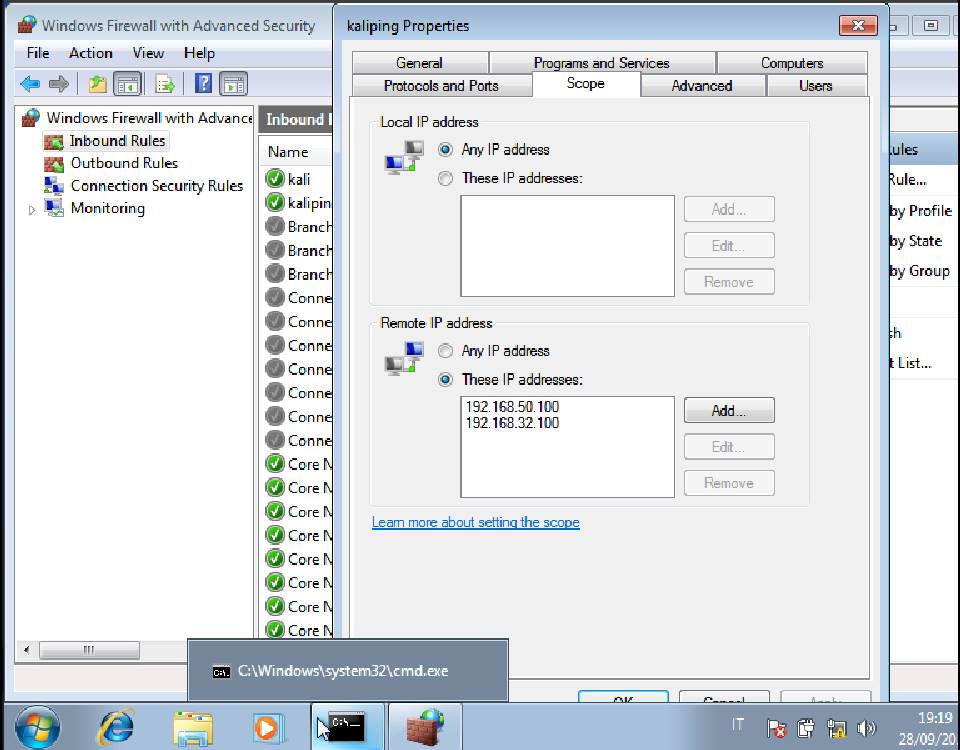
1. Dopo aver installato le macchine virtuali richiesta, impostare gli indirizzi IPV4 su Kali Linux (192.168.32.100) e su Win7 (192.168.32.101) tramite i terminali e riavviare Kali per salvare;
2. Impostare il FIREWALL di Win7 in modo tale che permetta all’IP di Kali di mettersi in contatto. Creare la regola inserendo l’indirizzo IP a cui si vuole dare il permesso (figura1) oppure impostando il protocollo ICMPv4 dare il permesso a tutti gli indirizzi IP;

Figura 2

Figura 1

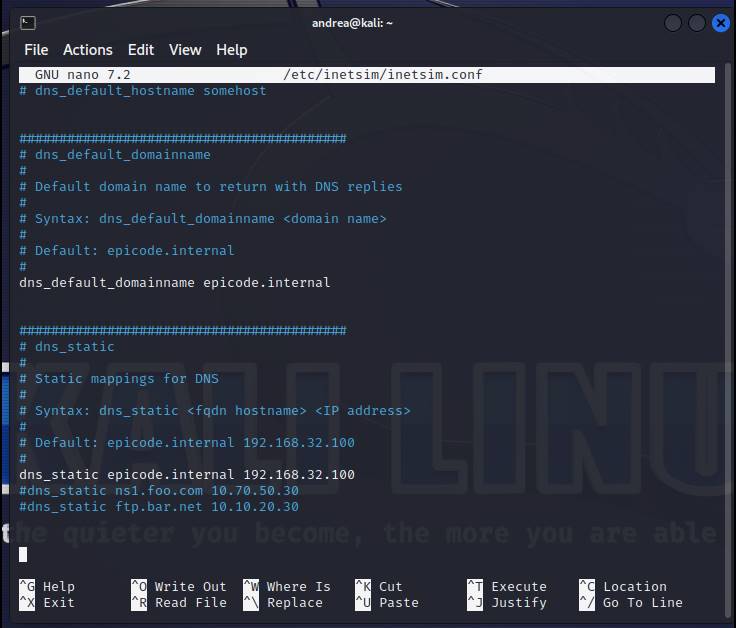
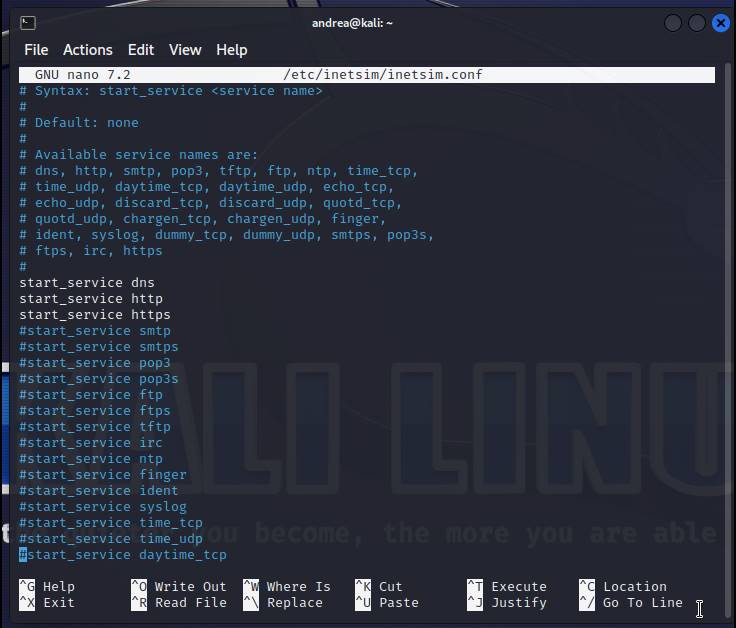
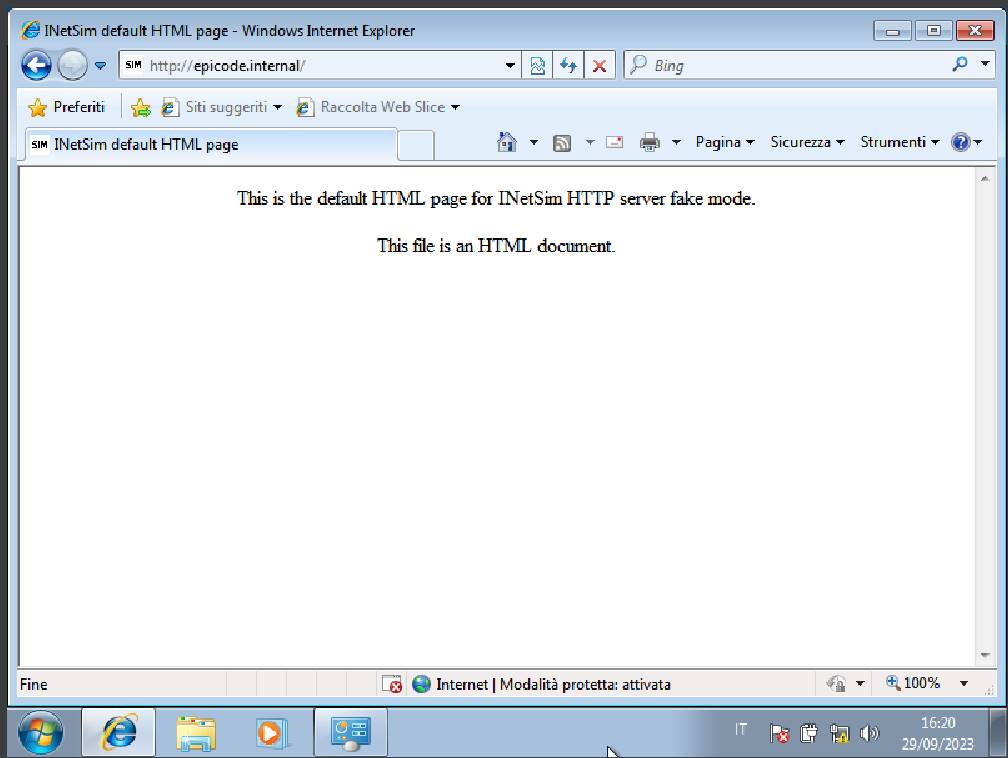
1. Configurare InetSim da terminale su Kali tramite ***‘sudo nano /etc/inetsim/inetsim.conf’*** per abilitare il servizio HTTPS, HTTP e DNS in modo che quest’ultimo dia il dominio ‘***epicode.internal’*** in risposta all’indirizzo IP 192.168.32.100;
2. Una volta impostati aprire Explorer da Windows 7 e scrivere nell’URL il dominio ***‘https://epicode.internal’*** per avere il sito InetSim con protocollo HTTPS (figura3) e ***‘http://epicode.internal’*** per avere quello in protocollo HTTP (figura 4);

Figura 4

1. A questo punto procediamo con l’utilizzo di WIRESHARK per monitorare i pacchetti di rete e possiamo anche notare gli indirizzi MAC di sorgente e destinazione;

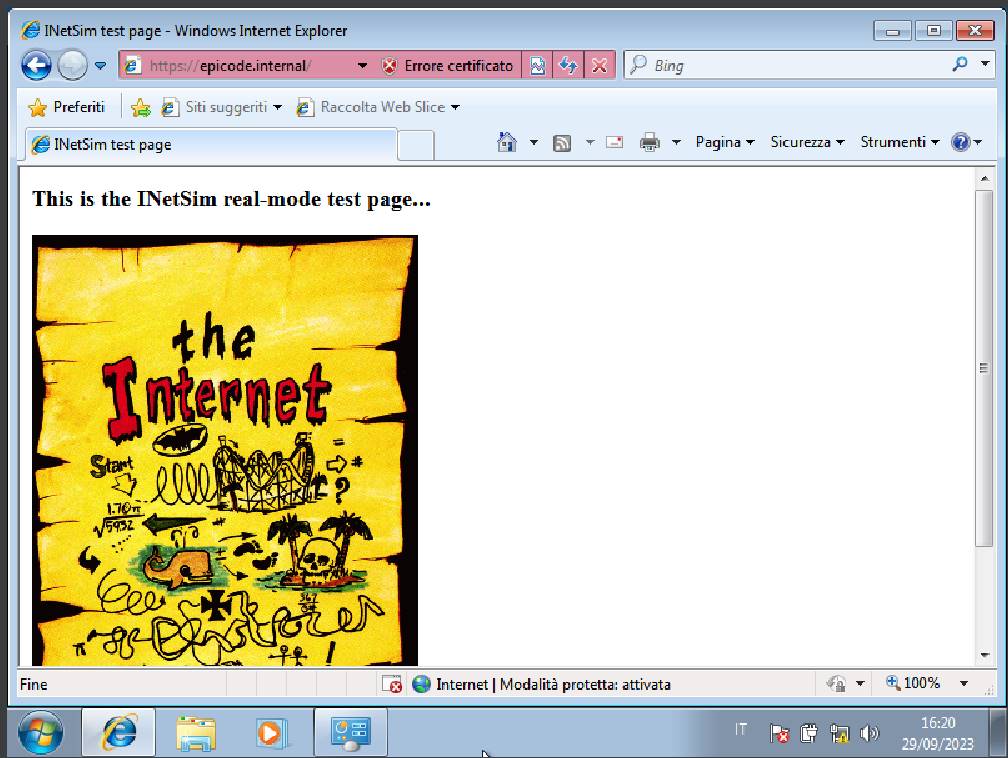
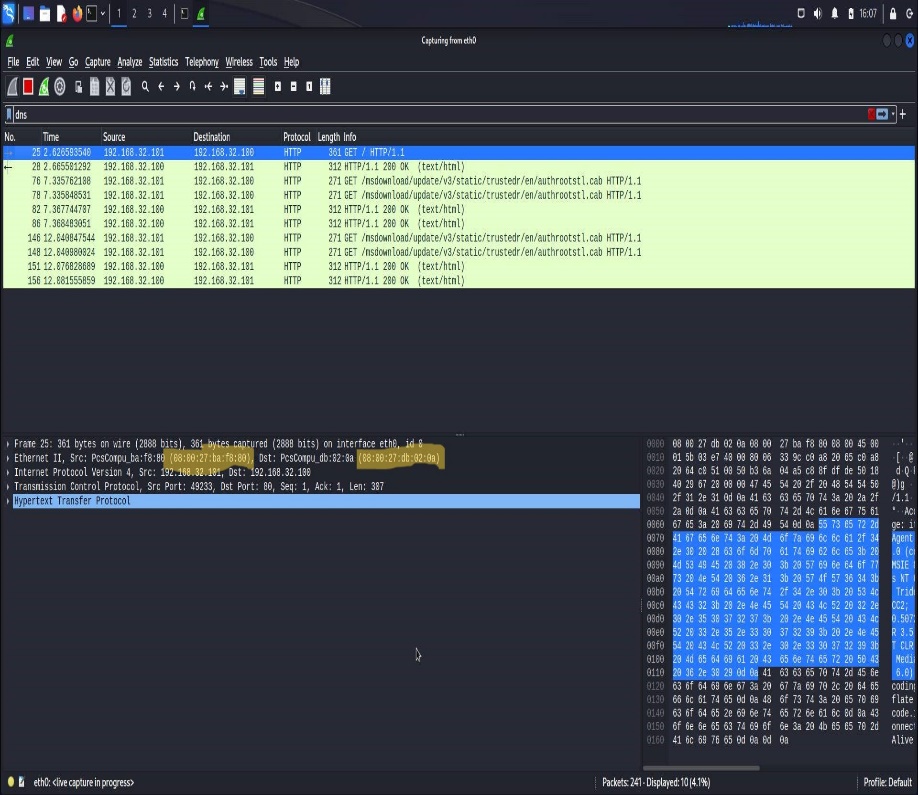


Figura 3



1. Infine eseguiamo lo stesso ***‘’sniffing’’*** di pacchetti in HTTPS e possiamo notare che i dati sono criptati. Proprio questo rende il protocollo più sicuro rispetto a quello HTTP.

