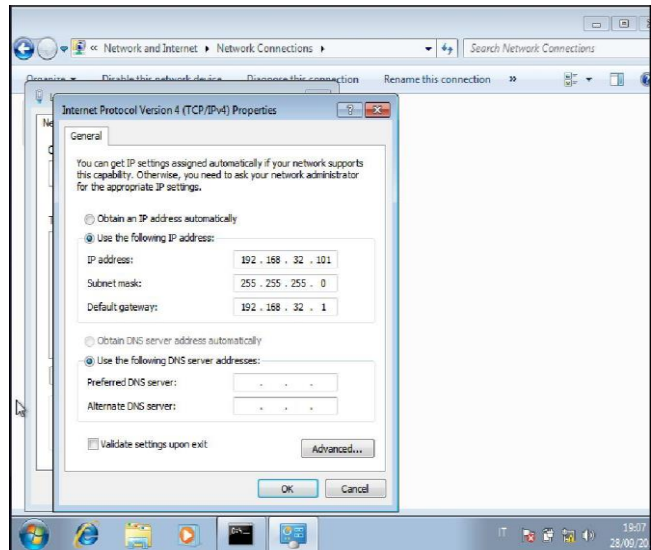
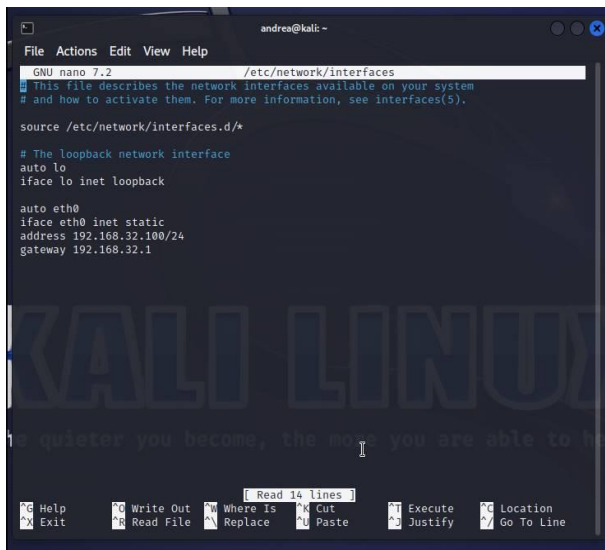


Relazione esercitazione 1: Simulazione rete complessa

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

- A. 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;



- B. 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;

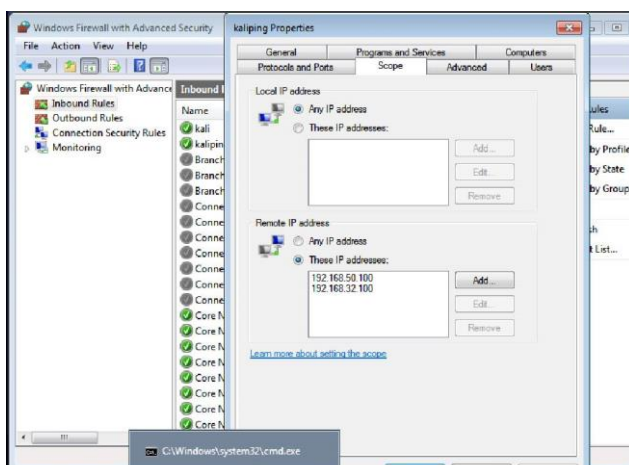


Figura 1

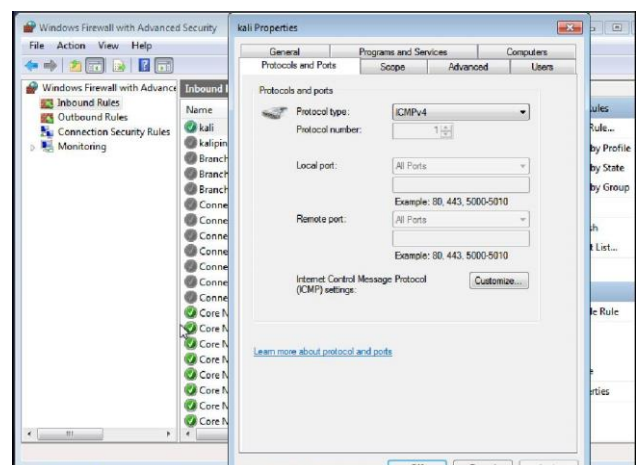
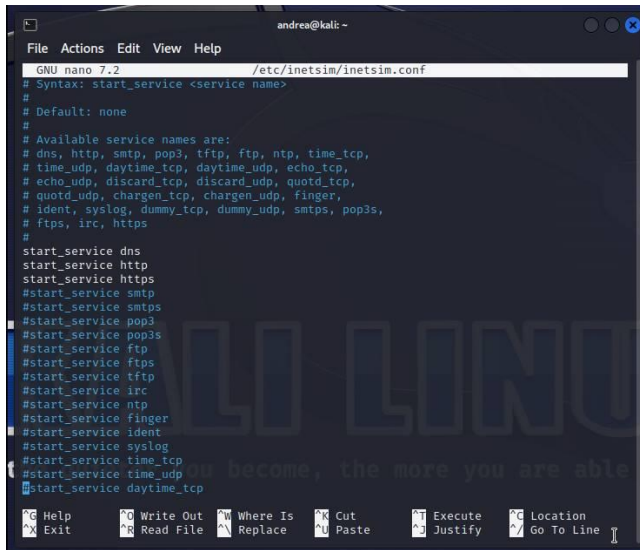
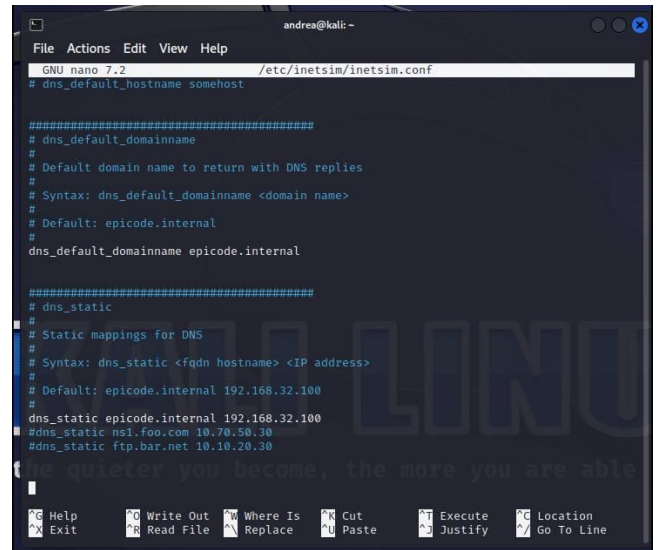


Figura 2

- C. 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;



```
GNU nano 7.2 /etc/inetsim/inetsim.conf
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
```



```
GNU nano 7.2 /etc/inetsim/inetsim.conf
# dns_default_hostname somehost
#
#####
# dns_default_domainname
#
# Default domain name to return with DNS replies
# Syntax: dns_default_domainname <domain name>
# Default: epicode.internal
# dns_default_domainname epicode.internal
#
#####
# dns_static
#
# Static mappings for DNS
# Syntax: dns_static <fqdn hostname> <IP address>
# Default: epicode.internal 192.168.32.100
# dns_static epicode.internal 192.168.32.100
# dns_static ns1.foo.com 10.70.50.30
# dns_static ftp.bar.net 10.10.20.30
```

- D. 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);

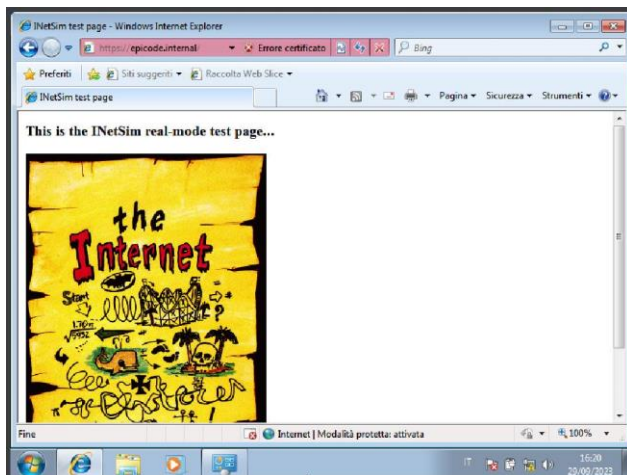


Figura 3

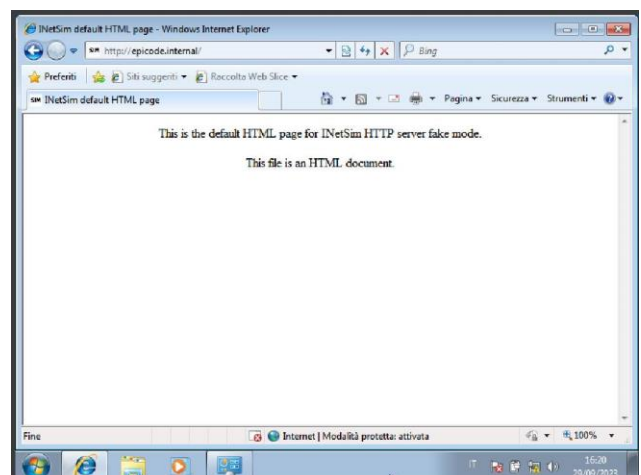
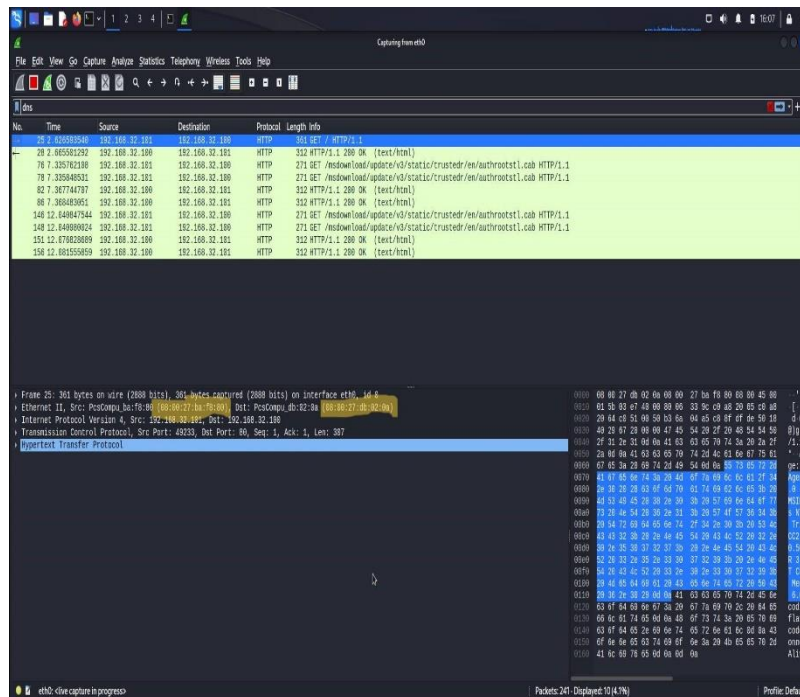


Figura 4

- E. 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;



F. 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.

