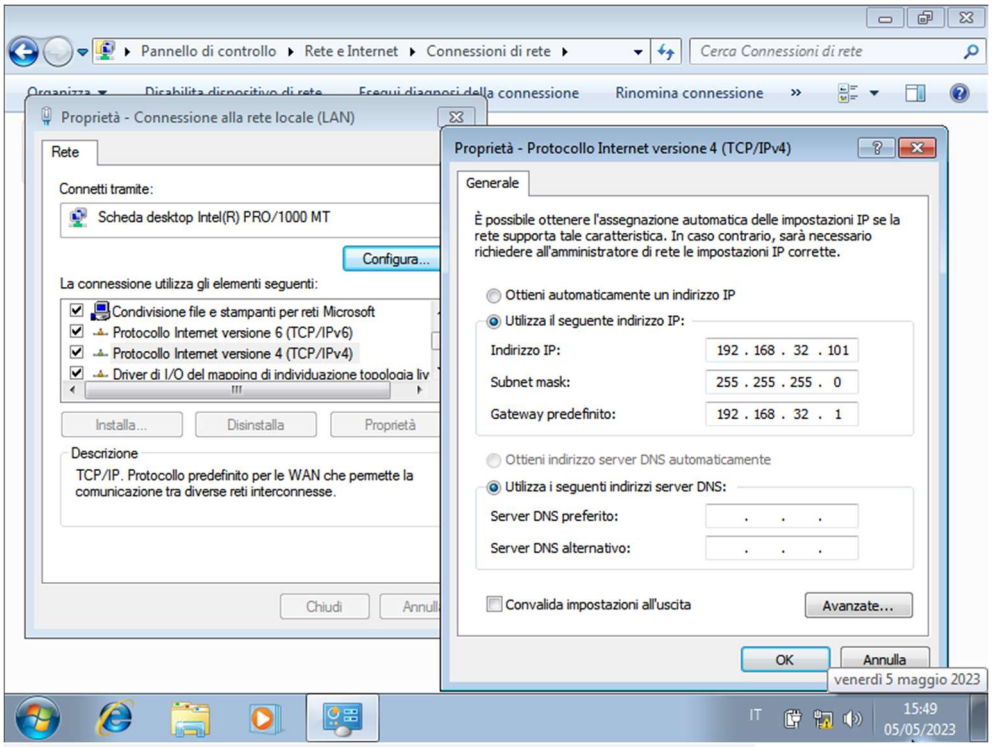
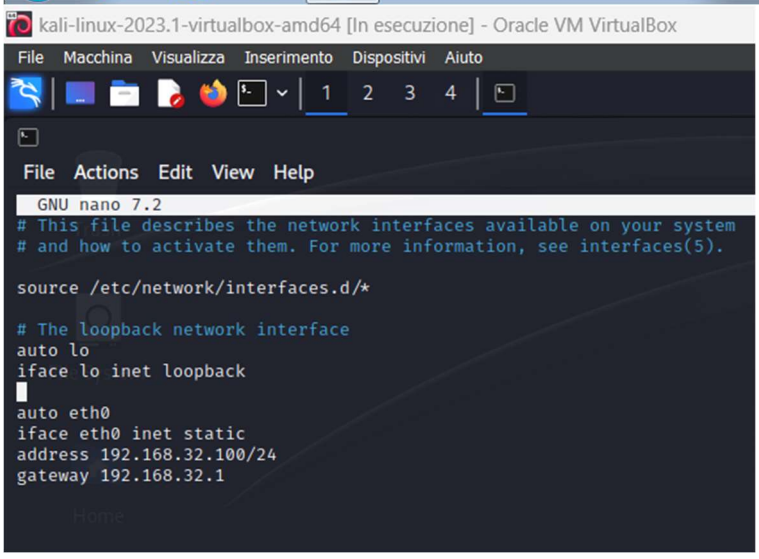
Pierluigi Amorese

Progetto:

Simulazione rete complessa

1. Come primo passo ho impostato gli indirizzi ip sulle macchine;





2. Qui ho configurato il DNS Server tramite il file inetsim.conf;

```
198 ##########################################
199 # dns_default_ip
200 #
201 # Default IP address to return with DNS replies
202 #
203 # Syntax: dns_default_ip <IP address>
204 #
205 # Default: 127.0.0.1
206 #
207 #dns_default_ip 10.10.10.1
208 dns_default_ip 192.168.32.100
209
210 ##########################################
211 # dns_default_hostname
212 #
213 # Default hostname to return with DNS replies
214 #
215 # Syntax: dns_default_hostname <hostname>
216 #
217 # Default: www
218 #
219 #dns_default_hostname epicode.internal
220
221
222 ##########################################
223 # dns_default_domainname
224 #
225 # Default domain name to return with DNS replies
226 #
227 # Syntax: dns_default_domainname <domain name>
228 #
229 # Default: inetsim.org
230 #
231 #dns_default_domainname epicode.internal
232
233
234 ##########################################
```

3. E ho configurato anche il server HTTPS;

```
407 ##########################################
408 # https_fakemode
409 #
410 # Turn HTTPS fake mode on or off
411 #
412 # Syntax: https_fakemode [yes|no]
413 #
414 # Default: yes
415 #
416 #https_fakemode yes
417
418
```

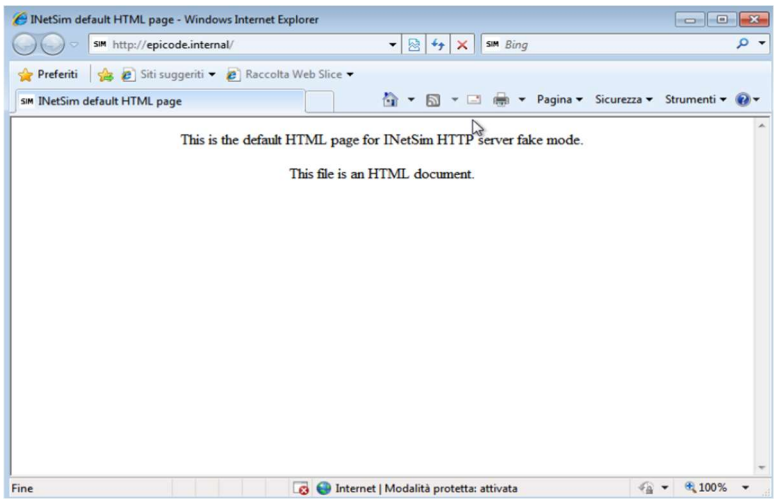
4. Con il comando “sudo cp” ho sostituito il file di configurazione modificato nella cartella di origine;

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ cd Desktop/

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo cp inetsim.conf /etc/inetsim/inetsim.conf
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop]
└─$
```

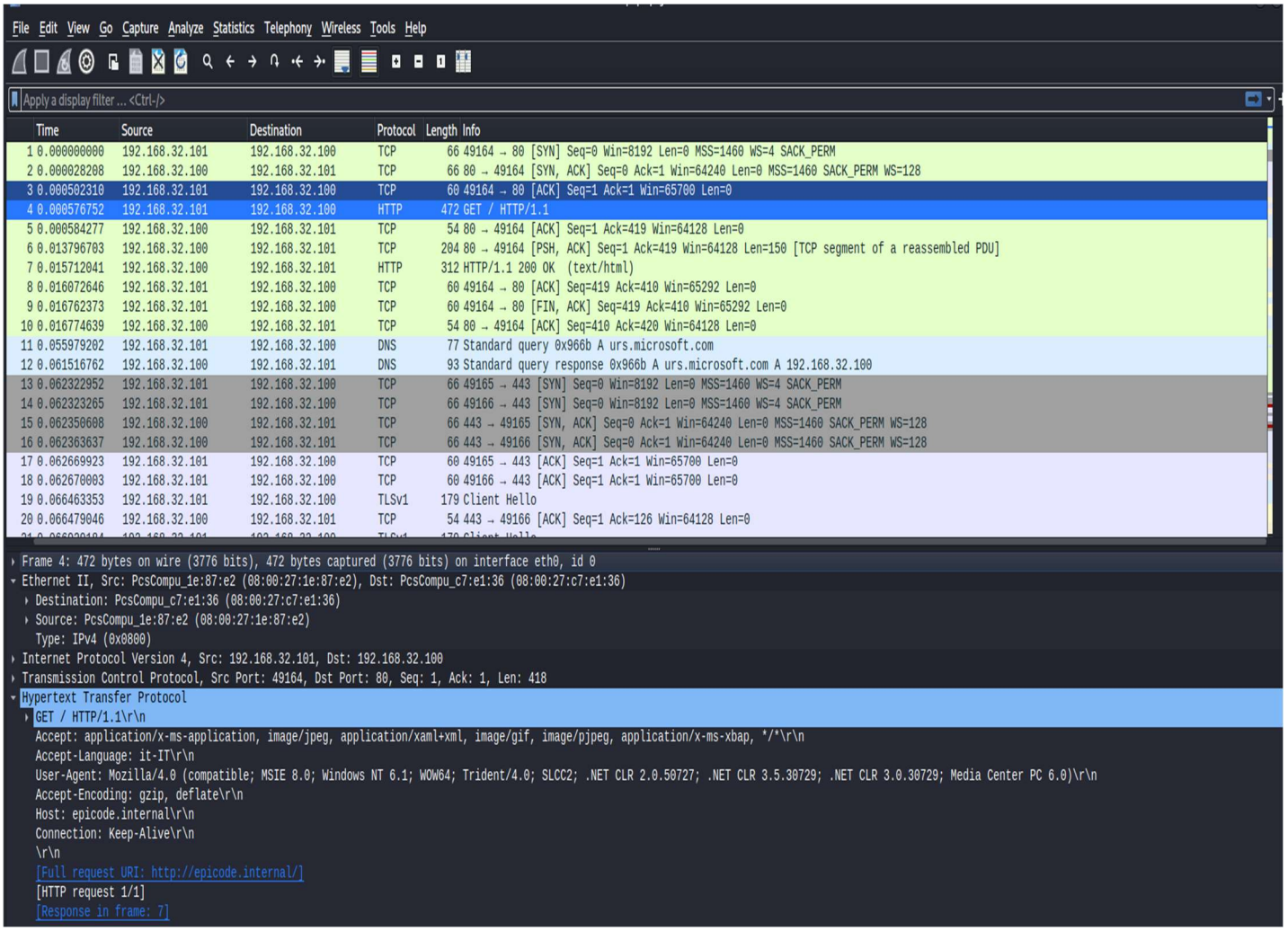
5. Ho avviato inetSim da terminale;

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 6330) ===
Session ID:     6330
Listening on:   192.168.32.100
Real Date/Time: 2023-05-07 06:02:47
Fake Date/Time: 2023-05-07 06:02:47 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 6332)
  * echo_7_tcp - started (PID 6351)
  * finger_79_tcp - started (PID 6344)
  * irc_6667_tcp - started (PID 6342)
  * ntp_123_udp - started (PID 6343)
  * tftp_69_udp - started (PID 6341)
  * daytime_13_udp - started (PID 6350)
  * https_443_tcp - started (PID 6334)
  * smtp_25_tcp - started (PID 6335)
  * ident_113_tcp - started (PID 6345)
  * time_37_udp - started (PID 6348)
  * smtps_465_tcp - started (PID 6336)
  * discard_9_tcp - started (PID 6353)
  * echo_7_udp - started (PID 6352)
  * dummy_1_tcp - started (PID 6359)
  * daytime_13_tcp - started (PID 6349)
  * quotd_17_tcp - started (PID 6355)
  * chargen_19_udp - started (PID 6358)
  * pop3_110_tcp - started (PID 6337)
  * http_80_tcp - started (PID 6333)
  * dummy_1_udp - started (PID 6360)
  * quotd_17_udp - started (PID 6356)
  * syslog_514_udp - started (PID 6346)
  * chargen_19_tcp - started (PID 6357)
  * discard_9_udp - started (PID 6354)
  * pop3s_995_tcp - started (PID 6338)
  * ftp_21_tcp - started (PID 6339)
  * time_37_tcp - started (PID 6347)
  * ftps_990_tcp - started (PID 6340)
 done.
Simulation running.
```

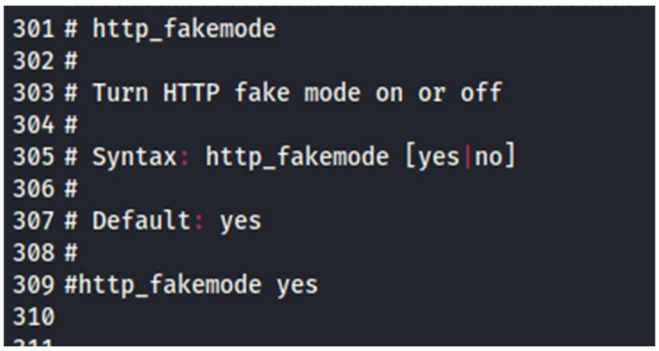
6. Da terminale Windows ho aperto il browser e ho digitato epicode.internal, con la seguente pagina come risultato:



7. nel frattempo su kali ho aperto wireshark e ho catturato i seguenti pacchetti:



8. Ho chiuso tutto e riconfigurato inetSim rimuovendo il server HTTPS e impostando il server HTTP nella stessa maniera di prima;



9. Ho ripetuto la simulazione con inetSim e su wireshark ho catturato i seguenti pacchetti: