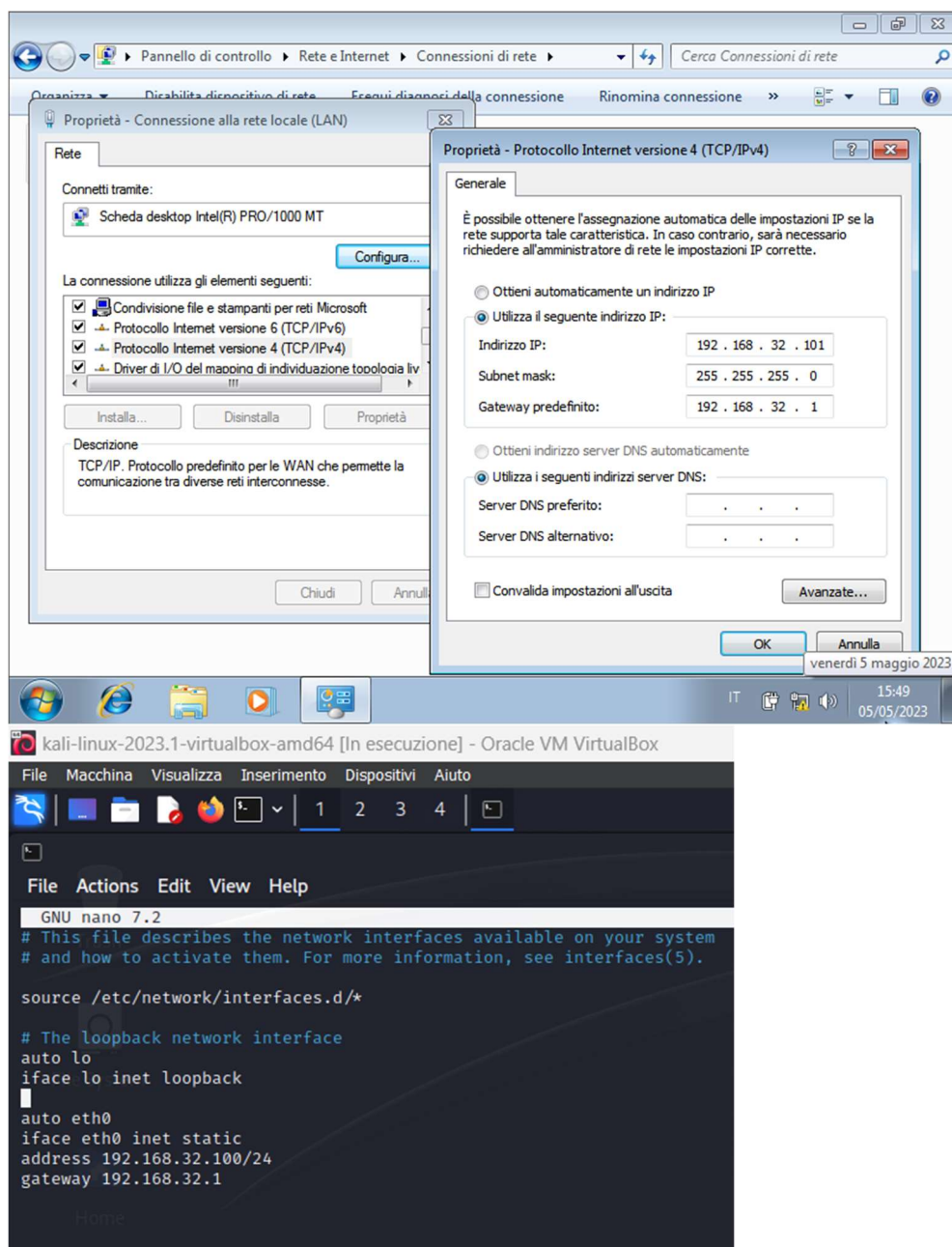


Pierluigi Amorese

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
419 #####
```

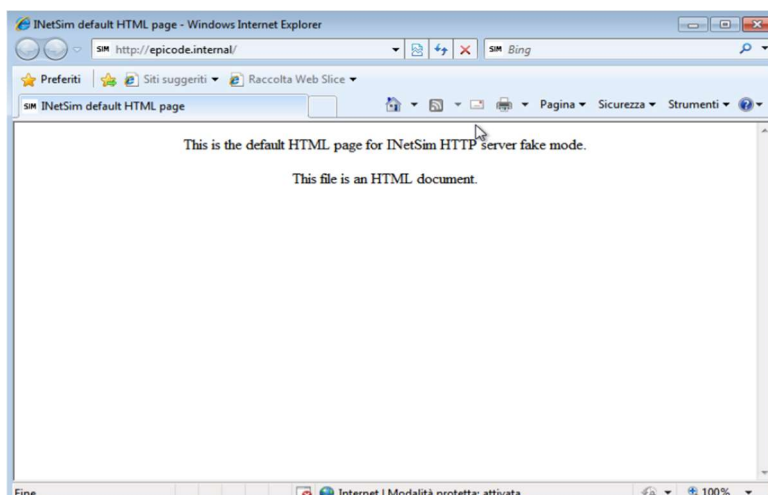
4. Con il comando “sudo cp” ho sostituito il file di configurazione modificato nella cartella di origine;

```
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:

Time	Source	Destination	Protocol	Length	Info
1 0.000000000	192.168.32.101	192.168.32.100	TCP	66	49164 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
2 0.000028208	192.168.32.100	192.168.32.101	TCP	66	80 → 49164 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3 0.000502310	192.168.32.101	192.168.32.100	TCP	60	49164 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4 0.000576752	192.168.32.101	192.168.32.100	HTTP	472	GET / HTTP/1.1
5 0.000584277	192.168.32.100	192.168.32.101	TCP	54	80 → 49164 [ACK] Seq=1 Ack=419 Win=64128 Len=0
6 0.013796703	192.168.32.100	192.168.32.101	TCP	204	80 → 49164 [PSH, ACK] Seq=1 Ack=419 Win=64128 Len=150 [TCP segment of a reassembled PDU]
7 0.015712041	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
8 0.016072646	192.168.32.101	192.168.32.100	TCP	60	49164 → 80 [ACK] Seq=419 Ack=410 Win=65292 Len=0
9 0.016762373	192.168.32.101	192.168.32.100	TCP	60	49164 → 80 [FIN, ACK] Seq=419 Ack=410 Win=65292 Len=0
10 0.016774639	192.168.32.100	192.168.32.101	TCP	54	80 → 49164 [ACK] Seq=410 Ack=420 Win=64128 Len=0
11 0.055979202	192.168.32.101	192.168.32.100	DNS	77	Standard query 0x966b A urs.microsoft.com
12 0.061516762	192.168.32.100	192.168.32.101	DNS	93	Standard query response 0x966b A urs.microsoft.com A 192.168.32.100
13 0.062322952	192.168.32.101	192.168.32.100	TCP	66	49165 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
14 0.062323265	192.168.32.101	192.168.32.100	TCP	66	49166 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
15 0.062350608	192.168.32.100	192.168.32.101	TCP	66	443 → 49165 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
16 0.062363637	192.168.32.100	192.168.32.101	TCP	66	443 → 49166 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
17 0.062669923	192.168.32.101	192.168.32.100	TCP	60	49165 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
18 0.062670003	192.168.32.101	192.168.32.100	TCP	60	49166 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
19 0.066463353	192.168.32.101	192.168.32.100	TLSv1	179	Client Hello
20 0.066479046	192.168.32.100	192.168.32.101	TCP	54	443 → 49166 [ACK] Seq=1 Ack=126 Win=64128 Len=0
21 0.066991461	192.168.32.101	192.168.32.100	TLSv1	170	Client Hello

Frame 4: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_1e:87:e2 (08:00:27:1e:87:e2), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)

Destination: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)

Source: PcsCompu_1e:87:e2 (08:00:27:1e:87:e2)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100

Transmission Control Protocol, Src Port: 49164, Dst Port: 80, Seq: 1, Ack: 1, Len: 418

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*\r\n

Accept-Language: it-IT\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\r\n

Accept-Encoding: gzip, deflate\r\n

Host: epicode.internal\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://epicode.internal/]

[HTTP request 1/1]

[Response in frame: 7]

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

```
301 # http_fakemode
302 #
303 # Turn HTTP fake mode on or off
304 #
305 # Syntax: http_fakemode [yes|no]
306 #
307 # Default: yes
308 #
309 #http_fakemode yes
310
311
```


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

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.101	192.168.32.100	DNS	76	Standard query 0x7265 A epicode.internal
2	0.005453246	192.168.32.100	192.168.32.101	DNS	92	Standard query response 0x7265 A epicode.internal A 192.168.32.100
3	0.006280748	192.168.32.101	192.168.32.100	TCP	66	49162 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.006295473	192.168.32.100	192.168.32.101	TCP	66	80 → 49162 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.006707892	192.168.32.101	192.168.32.100	TCP	60	49162 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.006707963	192.168.32.101	192.168.32.100	HTTP	472	GET / HTTP/1.1
7	0.006730684	192.168.32.100	192.168.32.101	TCP	54	80 → 49162 [ACK] Seq=1 Ack=419 Win=64128 Len=0
8	0.022098106	192.168.32.100	192.168.32.101	TCP	204	80 → 49162 [PSH, ACK] Seq=1 Ack=419 Win=64128 Len=150 [TCP segment of a reassembled PDU]
9	0.023820141	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
10	0.024346663	192.168.32.101	192.168.32.100	TCP	60	49162 → 80 [ACK] Seq=419 Ack=410 Win=65292 Len=0
11	0.024695732	192.168.32.101	192.168.32.100	TCP	60	49162 → 80 [FIN, ACK] Seq=419 Ack=410 Win=65292 Len=0
12	0.024714279	192.168.32.100	192.168.32.101	TCP	54	80 → 49162 [ACK] Seq=410 Ack=420 Win=64128 Len=0
13	0.062696584	192.168.32.101	192.168.32.100	DNS	77	Standard query 0xd7d9 A urs.microsoft.com
14	0.067888119	192.168.32.100	192.168.32.101	DNS	93	Standard query response 0xd7d9 A urs.microsoft.com A 192.168.32.100
15	0.068723890	192.168.32.101	192.168.32.100	TCP	66	49164 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
16	0.068724269	192.168.32.101	192.168.32.100	TCP	66	49163 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
17	0.068740760	192.168.32.100	192.168.32.101	TCP	66	443 → 49164 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
18	0.068750360	192.168.32.100	192.168.32.101	TCP	66	443 → 49163 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
19	0.069336229	192.168.32.101	192.168.32.100	TCP	60	49164 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
20	0.069336351	192.168.32.101	192.168.32.100	TCP	60	49163 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
21	0.086493513	192.168.32.101	192.168.32.100	TLSv1	179	Client Hello
22	0.086529600	192.168.32.100	192.168.32.101	TCP	54	443 → 49163 [ACK] Seq=1 Ack=126 Win=64128 Len=0

Frame 6: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_1e:87:e2 (08:00:27:1e:87:e2), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)

Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100

Transmission Control Protocol, Src Port: 49162, Dst Port: 80, Seq: 1, Ack: 1, Len: 418

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*\r\n

Accept-Language: it-IT\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\r\n

Accept-Encoding: gzip, deflate\r\n

Host: epicode.internal\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://epicode.internal/]

[HTTP request 1/1]

[Response in frame: 9]