

Simulazione architettura Cliente Server

Fernando Catrambone

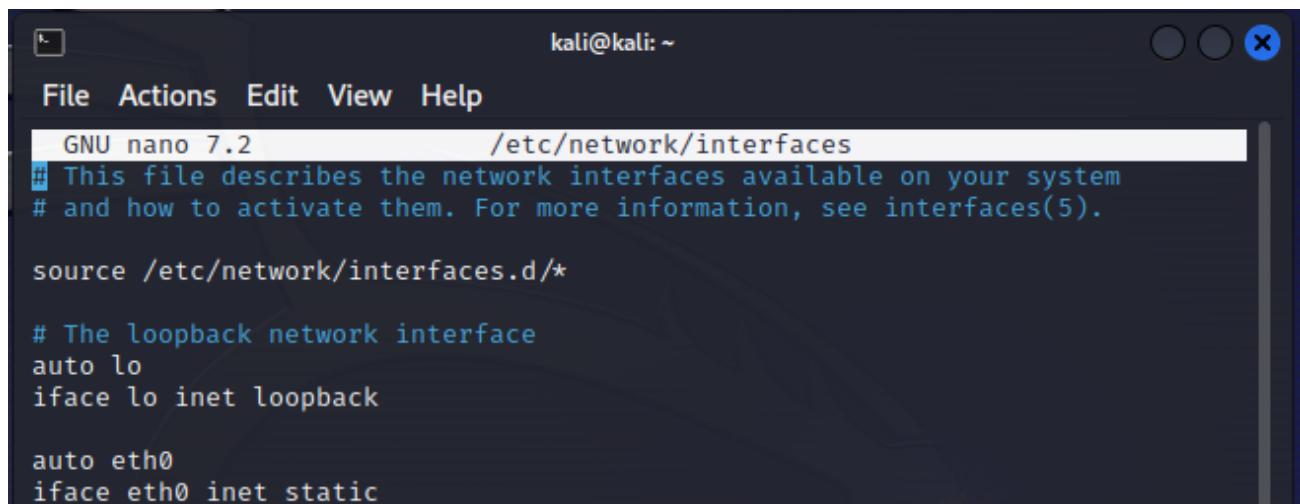
In questo progetto andrò a simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 richiede tramite web browser una risorsa all'hostname episode.internal che risponde all'indirizzo 192.168.32.100. Successivamente intercetterò la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS. Ripeterò la simulazione, sostituendo il server HTTPS, con un server HTTP. Intercettando nuovamente il traffico, evidenzierò le differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS.

Dettagli del progetto

Configurazione VM

-Ho configurato gli IP di Kali Linux e Windows

Su Kali ho modificato il file /etc/network/interfaces assegnando l'IP 192.168.32.100



```
File Actions Edit View Help
GNU nano 7.2          /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

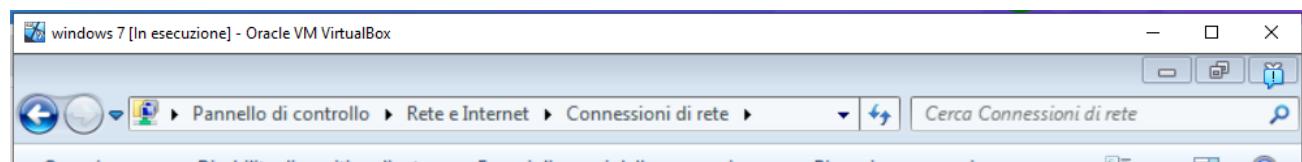
# The loopback network interface
auto lo
iface lo inet loopback

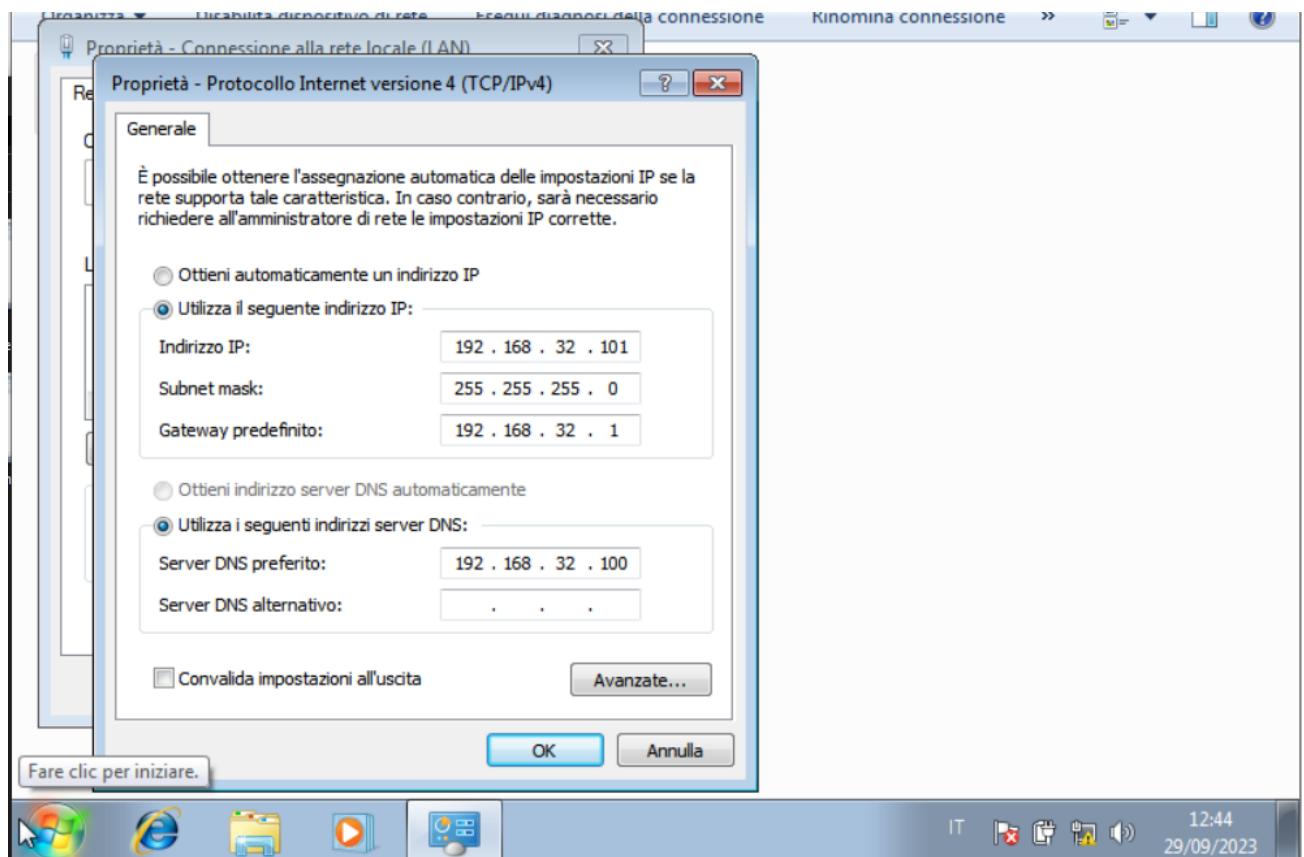
auto eth0
iface eth0 inet static
```

```
address 192.168.32.100  
netmask 255.255.255.0  
network 192.168.32.0  
broadcast 192.168.32.255  
gateway 192.168.32.1
```

```
[ Read 16 lines ]  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify  
kali@kali: ~  
File Actions Edit View Help  
└──(kali㉿kali)-[~]  
$ sudo nano /etc/network/interfaces  
└──(kali㉿kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255  
        inet6 fe80::a00:27ff:fedb:7ef5 prefixlen 64 scopeid 0x20<link>  
          ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)  
            RX packets 700 bytes 60521 (59.1 KiB)  
            RX errors 0 dropped 0 overruns 0 frame 0  
            TX packets 385 bytes 50529 (49.3 KiB)  
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
      inet 127.0.0.1 netmask 255.0.0.0  
        inet6 ::1 prefixlen 128 scopeid 0x10<host>  
          loop txqueuelen 1000 (Local Loopback)  
            RX packets 44 bytes 2240 (2.1 KiB)  
            RX errors 0 dropped 0 overruns 0 frame 0  
            TX packets 44 bytes 2240 (2.1 KiB)  
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
└──(kali㉿kali)-[~]  
$
```

Successivamente ho modificato l'IP di Windows 7 inserendo come indirizzo IP **192.168.32.101** e impostando come server DNS **192.168.32.100** ovvero l'indirizzo IP di Kali





Configurazione Inetsim

-Attivazione servizio HTTPS e DNS

```
kali㉿kali: ~
```

```
File Actions Edit View Help
GNU nano 7.2          /etc/inetsim/inetsim.conf
# Main configuration
#####
#
# start_service
#
# The services to start
#
# 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 https
```

```
*start_service https  
start_service https  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
```

-Configurazione bind address all'indirizzo 192.168.32.100

The screenshot shows a terminal window titled "kali@kali: ~". The window title bar includes standard keyboard shortcuts for help, exit, file operations, and text editing. The main content of the terminal is the configuration file "/etc/inetsim/inetsim.conf" displayed in the nano editor. The file contains the following configuration for the "service_bind_address" parameter:

```
GNU nano 7.2          /etc/inetsim/inetsim.conf  
#####  
# service_bind_address  
#  
# IP address to bind services to  
#  
# Syntax: service_bind_address <IP address>  
#  
# Default: 127.0.0.1  
#  
service_bind_address 192.168.32.100  
  
#####  
# service_run_as_user  
#  
# User to run services  
#  
# Syntax: service_run_as_user <username>  
#  
# Default: inetsim  
#  
#service_run_as_user nobody
```

The bottom of the terminal window also features a set of keyboard shortcuts for help, exit, file operations, and text editing.

-Configurazione server DNS all'indirizzo IP di Kali e il nome del dominio episode.internal

The screenshot shows a terminal window titled "kali@kali: ~". The window title bar includes standard keyboard shortcuts for help, exit, file operations, and text editing. The main content of the terminal is the configuration file "/etc/inetsim/inetsim.conf" displayed in the nano editor. The file contains the following configuration for the "dns_default_ip" parameter:

```
GNU nano 7.2          /etc/inetsim/inetsim.conf  
#####  
# dns_default_ip  
#  
# Default IP address to return with DNS replies  
#  
# Syntax: dns_default_ip <IP address>  
#  
# Default: 127.0.0.1  
#  
dns_default_ip 192.168.32.100
```

The bottom of the terminal window also features a set of keyboard shortcuts for help, exit, file operations, and text editing.

```
#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
#
#dns_default_hostname somehost
#
^G Help ^O Write Out ^W Where Is ^K Cut
^X Exit ^R Read File ^\ Replace ^U Paste ^T Execute
^J Justify
```

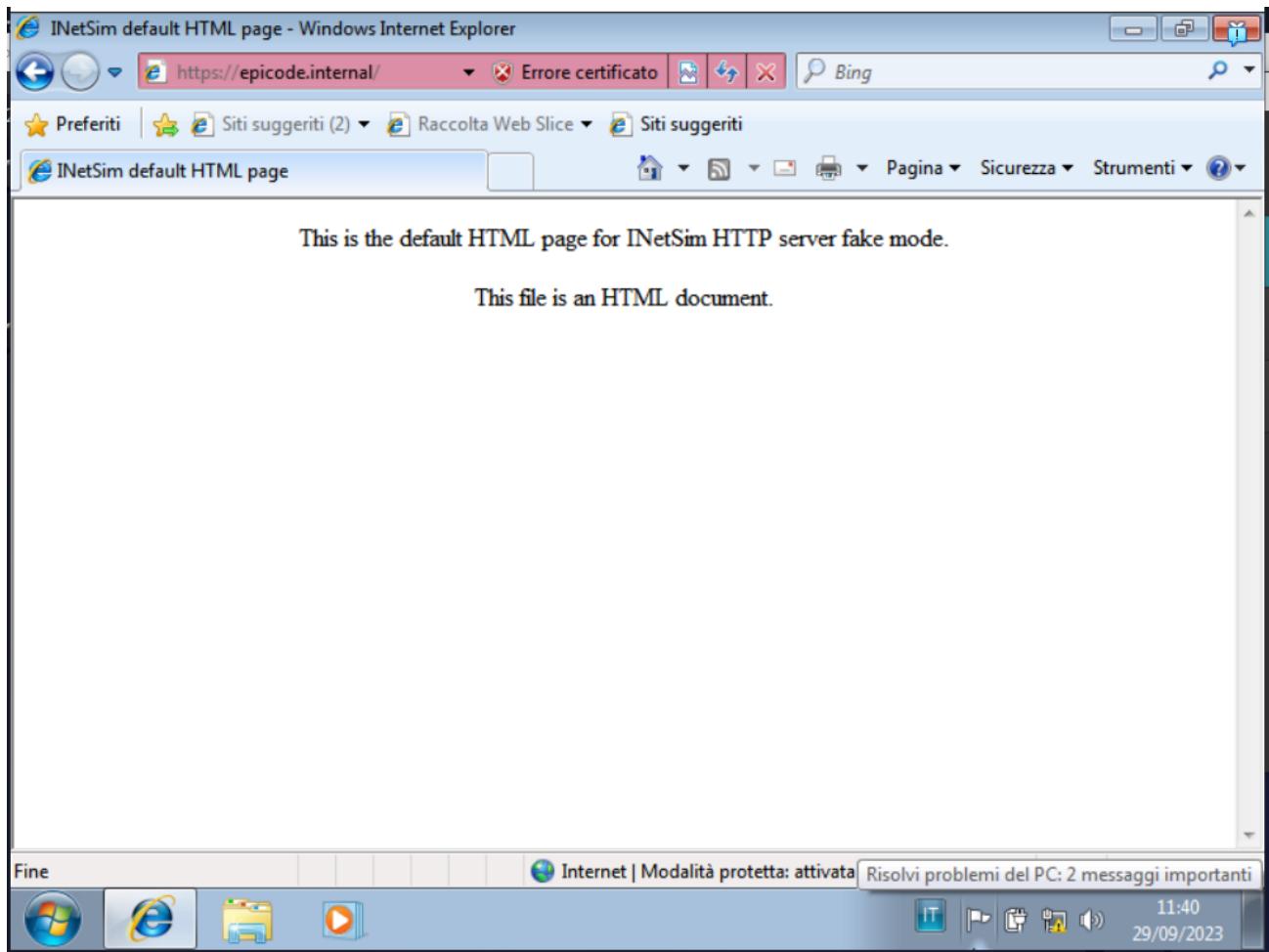
```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2          /etc/inetsim/inetsim.conf
#dns_default_hostname somehost

#####
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
dns_default_domainname episode.internal

#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
^G Help ^O Write Out ^W Where Is ^K Cut
^X Exit ^R Read File ^\ Replace ^U Paste ^T Execute
^J Justify
```

Richiesta tramite browser del dominio episode.internal

-Su Windows 7 ho dato il consenso all'utilizzo dei certificati TLS e SSL ed ho inserito nella barra degli indirizzi il nome del dominio che ho assegnato precedentemente



Il browser restituisce la pagina predefinita di Inetsim

-Intercetto con Wireshark la comunicazione tra Client e Server

Capturing from eth0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.37.101	192.168.32.100	TCP	66	49221 - 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
2	0.000019744	192.168.32.100	192.168.32.101	TCP	66	49221 - 49221 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	0.000268517	192.168.32.101	192.168.32.100	TCP	66	49221 - 443 [ACK] Seq=1 Ack=2 Win=65700 Len=0
4	0.000378292	192.168.32.101	192.168.32.100	TLSv1.2	248	Client Hello
5	0.000384202	192.168.32.100	192.168.32.101	TCP	54	443 - 49221 [ACK] Seq=1 Ack=195 Win=64128 Len=0
6	0.032837432	192.168.32.100	192.168.32.101	TLSv1.2	1370	Server Hello, Certificate, Server Key Exchange, Server Hello Done
7	0.037039685	192.168.32.101	192.168.32.100	TLSv1.2	220	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
8	0.037369957	192.168.32.100	192.168.32.101	TLSv1.2	145	Change Cipher Spec, Encrypted Handshake Message
9	0.040804266	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
10	0.246597549	192.168.32.100	192.168.32.101	TCP	145	[TCP Retransmission] 443 - 49221 [PSH, ACK] Seq=1317 Ack=361 Win=64128 Len=91
11	0.246732565	192.168.32.101	192.168.32.100	TCP	66	49221 - 443 [ACK] Seq=361 Ack=1408 Win=64292 Len=0 SLE=1317 SRE=1408
12	0.920550826	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
13	1.920975231	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
14	3.172328749	fe80::e8f3:0941:5f..	ff02::1:3	LLMNR	84	Standard query 0xafd8 A wpad
15	3.172427722	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xafd8 A wpad
16	3.281742323	fe80::e8f3:0941:5d..	ff02::1:3	LLMNR	84	Standard query 0xafd8 A wpad
17	3.281742505	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xafd8 A wpad
18	3.483533314	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
19	4.233236462	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
20	4.983124962	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
21	5.736644128	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
22	6.421206322	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
23	7.420487639	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_69:1c:5f (08:00:27:09:1c:5f), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49221, Dst Port: 443, Seq: 0, Len: 0

0000 08 00 27 cb 7e f5 08 00 27 69 1c 5f 08 00 45
0010 08 00 27 09 1c 5f 08 00 27 69 1c 5f 08 00 45
0020 20 64 c0 45 01 bb 02 c3 78 c0 00 00 00 00 00 80
0030 20 66 4f 72 00 00 02 04 05 b4 01 03 03 02 01
0040 04 02

Packets: 45 - Displayed: 45 (100.0%)

Capturing from eth0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.37.101	192.168.32.100	TCP	66	49221 - 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
2	0.000019744	192.168.32.100	192.168.32.101	TCP	66	49221 - 49221 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	0.000268517	192.168.32.101	192.168.32.100	TCP	66	49221 - 443 [ACK] Seq=1 Ack=2 Win=65700 Len=0
4	0.000378292	192.168.32.101	192.168.32.100	TLSv1.2	248	Client Hello
5	0.000384202	192.168.32.100	192.168.32.101	TCP	54	443 - 49221 [ACK] Seq=1 Ack=195 Win=64128 Len=0
6	0.032837432	192.168.32.100	192.168.32.101	TLSv1.2	1370	Server Hello, Certificate, Server Key Exchange, Server Hello Done
7	0.037039685	192.168.32.101	192.168.32.100	TLSv1.2	220	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
8	0.037369957	192.168.32.100	192.168.32.101	TLSv1.2	145	Change Cipher Spec, Encrypted Handshake Message
9	0.040804266	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
10	0.246597549	192.168.32.100	192.168.32.101	TCP	145	[TCP Retransmission] 443 - 49221 [PSH, ACK] Seq=1317 Ack=361 Win=64128 Len=91
11	0.246732565	192.168.32.101	192.168.32.100	TCP	66	49221 - 443 [ACK] Seq=361 Ack=1408 Win=64292 Len=0 SLE=1317 SRE=1408
12	0.920550826	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
13	1.920975231	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
14	3.172328749	fe80::e8f3:0941:5f..	ff02::1:3	LLMNR	84	Standard query 0xafd8 A wpad
15	3.172427722	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xafd8 A wpad
16	3.281742323	fe80::e8f3:0941:5d..	ff02::1:3	LLMNR	84	Standard query 0xafd8 A wpad
17	3.281742505	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xafd8 A wpad
18	3.483533314	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
19	4.233236462	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
20	4.983124962	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<00>
21	5.736644128	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
22	6.421206322	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101
23	7.420487639	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.17 Tell 192.168.32.101

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_69:1c:5f (08:00:27:09:1c:5f), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49221, Dst Port: 443, Seq: 0, Len: 0

0000 08 00 27 cb 7e f5 08 00 27 69 1c 5f 08 00 45
0010 08 00 27 09 1c 5f 08 00 27 69 1c 5f 08 00 45
0020 20 64 c0 45 01 bb 02 c3 78 c0 00 00 00 00 80
0030 20 66 4f 72 00 00 02 04 05 b4 01 03 03 02 01
0040 04 02

Packets: 45 - Displayed: 45 (100.0%)

No.	Time	Source	Destination	Protocol	Length Info
24	8.876187157	fe80::e8f3:d941:esd... ff02::1:3	LLMNR	84 Standard query 0x37d6 A wpad	
25	8.876303481	192.168.32.101	224.0.0.252	LLMNR	64 Standard query 0x37d6 A wpad
26	8.983436127	fe80::e8f3:d941:esd... ff02::1:3	LLMNR	84 Standard query 0x37d6 A wpad	
27	8.983436313	192.168.32.101	224.0.0.252	LLMNR	64 Standard query 0x37d6 A wpad
28	9.186772775	192.168.32.101	192.168.32.255	NBNS	92 Name query NB WPAD<00>
29	9.467704938	fe80::e8f3:d941:esd... ff02::1:2	DHCPv6	151 Solicit XID: 0x12019f CID: 000100012ca3470f080027691c5f	
30	9.936679033	192.168.32.101	192.168.32.255	NBNS	92 Name query NB WPAD<00>
31	10.686703672	192.168.32.101	192.168.32.255	NBNS	92 Name query NB WPAD<00>
32	11.436765979	192.168.32.101	192.168.32.100	DNS	90 Standard query 0xde66 A www.download.windowsupdate.com
33	11.449511091	192.168.32.100	192.168.32.101	DNS	106 Standard query response 0xde66 A www.download.windowsupdate.com A 192.168.32.100
34	11.450160200	192.168.32.101	192.168.32.100	TCP	66 49222 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
35	11.450170575	192.168.32.100	192.168.32.101	TCP	54 80 - 49222 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	11.967866678	192.168.32.101	192.168.32.100	TCP	66 [TCP Retransmission] 49222 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
37	11.967906995	192.168.32.100	192.168.32.101	TCP	54 80 - 49222 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	12.482821095	192.168.32.101	192.168.32.100	TCP	62 [TCP Retransmission] 49222 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM
39	12.482836744	192.168.32.100	192.168.32.101	TCP	54 80 - 49222 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	12.484164380	192.168.32.101	192.168.32.100	TLSv1.2	427 Application Data
41	12.493638017	192.168.32.100	192.168.32.101	TLSv1.2	267 Application Data
42	12.495288614	192.168.32.100	192.168.32.101	TLSv1.2	448 Application Data, Encrypted Alert
43	12.495550157	192.168.32.101	192.168.32.100	TCP	60 49221 - 443 [ACK] Seq=734 Ack=2016 Win=65700 Len=0
44	12.495694327	192.168.32.101	192.168.32.100	TCP	60 49221 - 443 [FIN, ACK] Seq=734 Ack=2016 Win=65700 Len=0
45	12.495703252	192.168.32.100	192.168.32.101	TCP	54 443 - 49221 [ACK] Seq=2016 Ack=735 Win=64128 Len=0

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_69:1c:5f (08:00:27:69:1c:5f), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49221, Dst Port: 443, Seq: 0, Len: 0

Packets: 45 - Displayed: 45 (100.0%) Profile: Default

Ecco i MAC Address dei due dispositivi

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_69:1c:5f (08:00:27:69:1c:5f), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49221, Dst Port: 443, Seq: 0, Len: 0

Nello screen si può notare che l'indirizzo sorgente è quello di Windows mentre il destinatario e Kali. Windows richiede i certificati TLS a Kali come da protocollo HTTPS affinchè la comunicazione tra i dispositivi sia sicura.

Richiesta tramite server HTTP

Ho attivato il servizio HTTP e disattivato quello HTTPS su Inetsim

```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf *
# Main configuration
#####
# start_service
#
# The services to start
#
# 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, quod_tcp,
# quod_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtsp, pop3s,
# ftns, irc, https
```

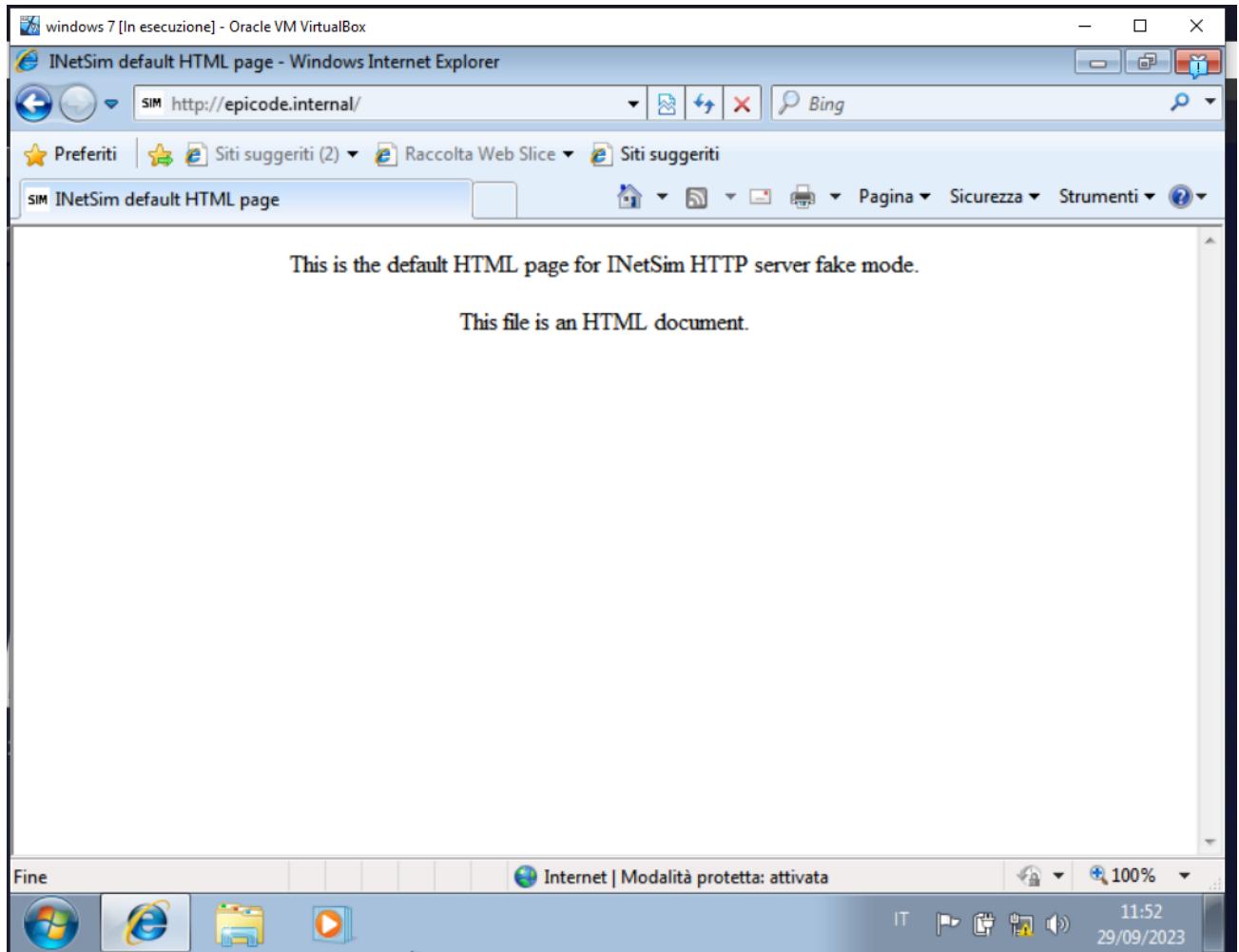
```

# http, https, https
#
start_service dns
start_service http
#start_service https

```

^{^G} Help ^{^O} Write Out ^{^W} Where Is ^{^K} Cut ^{^T} Execute
^{^X} Exit ^{^R} Read File ^{^V} Replace ^{^U} Paste ^{^J} Justify

Ho inserito il nome del dominio `epicode.internal` sul browser di windows



Come in precedenza il browser apre la pagina di default di Inetsim

-Analizzo il report di Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_69:1c:5f	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000018937	PcsCompu_cb:7e:f5	PcsCompu_69:1c:5f	ARP	42	192.168.32.100 is at 08:00:27:cb:7e:f5
3	0.0000264139	192.168.32.101	192.168.32.100	TCP	66	49219 → 80 [SYN] Seq=0 Win=6192 Len=0 MSS=1460 WS=4 SACK_PEE
4	0.0000279802	192.168.32.100	192.168.32.101	TCP	66	80 → 49219 [SYN, ACK] Seq=1 Ack=1 Win=64240 Len=0 MSS=1460
5	0.0000488794	192.168.32.101	192.168.32.100	TCP	60	49219 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.0000604339	192.168.32.101	192.168.32.100	HTTP	361	GET / HTTP/1.1
7	0.0000610609	192.168.32.100	192.168.32.101	TCP	54	80 → 49219 [ACK] Seq=1 Ack=308 Win=64128 Len=0
8	0.012745097	192.168.32.100	192.168.32.101	TCP	204	80 → 49219 [PSH, ACK] Seq=1 Ack=308 Win=64128 Len=150 [TCP
9	0.014411562	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
10	0.014657118	192.168.32.101	192.168.32.100	TCP	60	49219 → 80 [ACK] Seq=308 Ack=410 Win=65292 Len=0
11	0.014783646	192.168.32.101	192.168.32.100	TCP	60	49219 → 80 [FIN, ACK] Seq=308 Ack=410 Win=65292 Len=0
12	0.014810755	192.168.32.100	192.168.32.101	TCP	54	80 → 49219 [ACK] Seq=410 Ack=309 Win=64128 Len=0

13 5.210788371 PcsCompu_cb:7e:f5 PcsCompu_69:1c:5f ARP 42 Who has 192.168.32.101? Tell 192.168.32.100
14 5.212856756 PcsCompu_69:1c:5f PcsCompu_cb:7e:f5 ARP 60 192.168.32.101 is at 08:00:27:69:1c:5f

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_69:1c:5f (08:00:27:69:1c:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

Hex	Dec
0000	ff ff ff ff ff ff 08 00 27 69 1c 5f
0010	08 00 06 04 00 01 08 00 27 69 1c 5f
0020	00 00 00 00 00 00 c0 a8 20 64 00 00
0030	00 00 00 00 00 00 00 00 00 00 00 00

wireshark_eth0BABDC2.pcapng | Packets: 14 · Displayed: 14 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

In questo caso possiamo notare che a differenza del HTTPS non richiede nessun certificato TLS e i file non sono criptati.