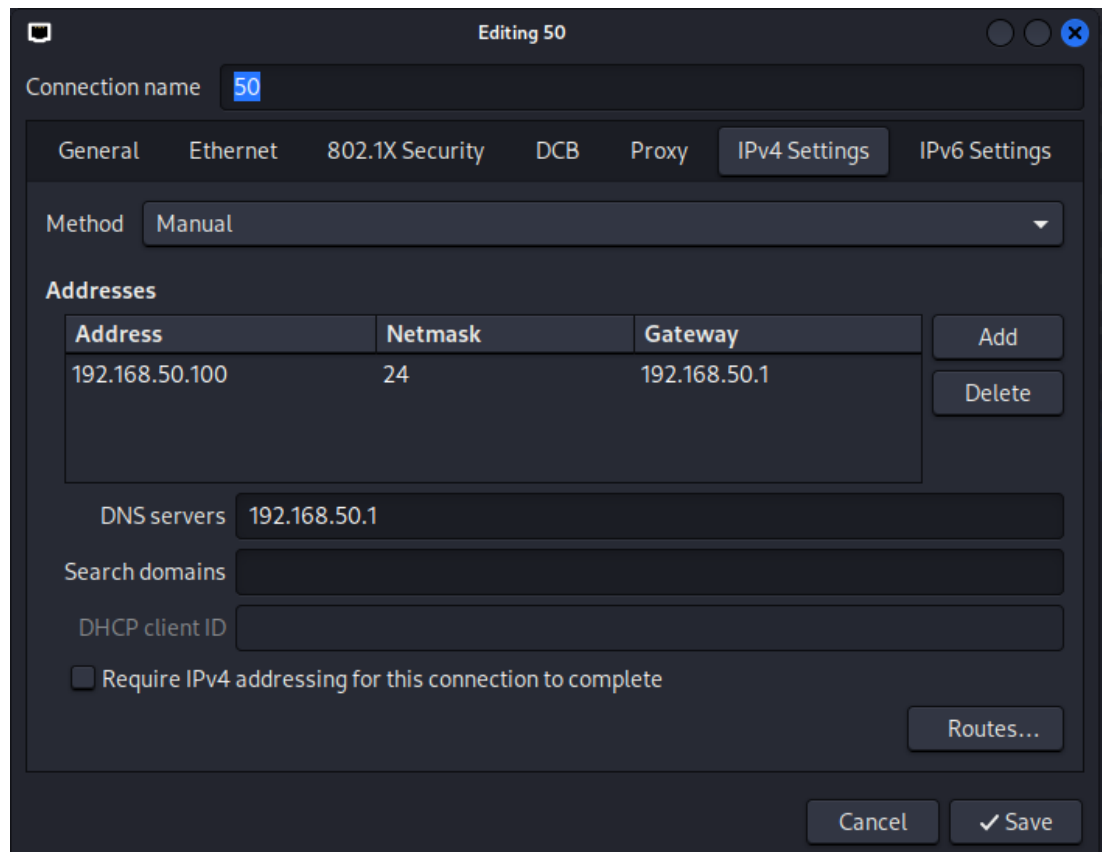




## Progetto finale M1

### CONFIGURAZIONE MACCHINE

Kali

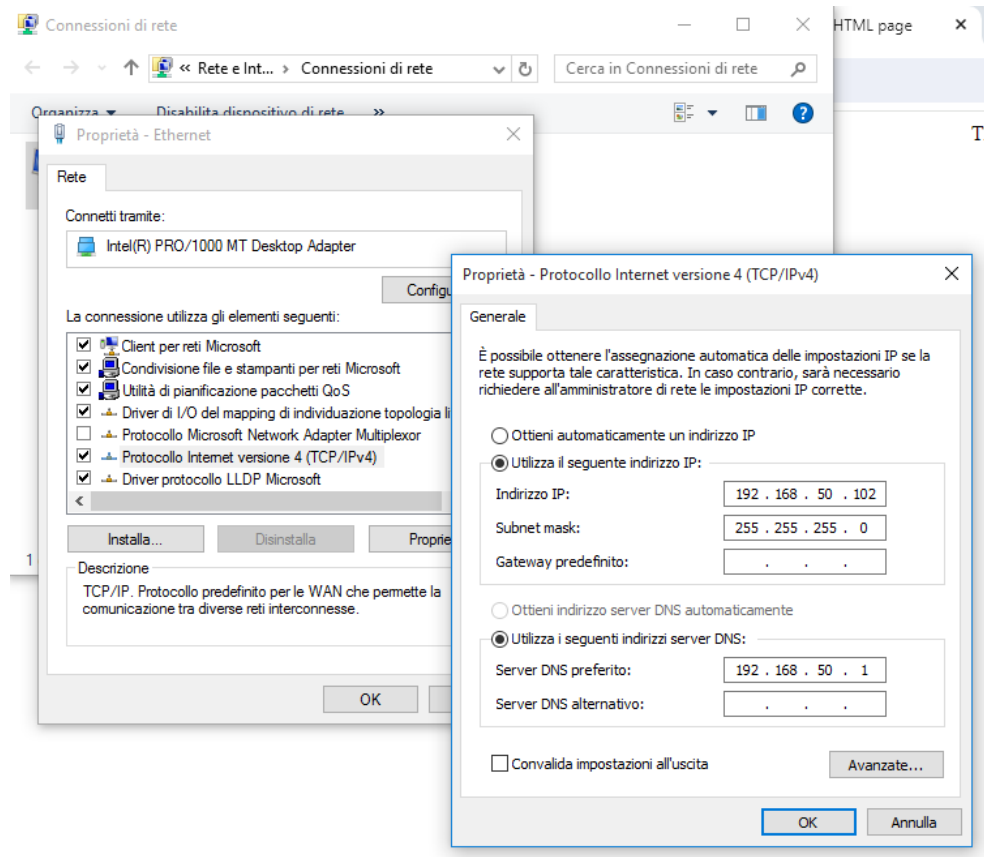


The image shows a network configuration window titled "Editing 50". The "Connection name" field contains "50". The "IPv4 Settings" tab is selected, showing a "Method" of "Manual". Below this is a table of IP addresses:

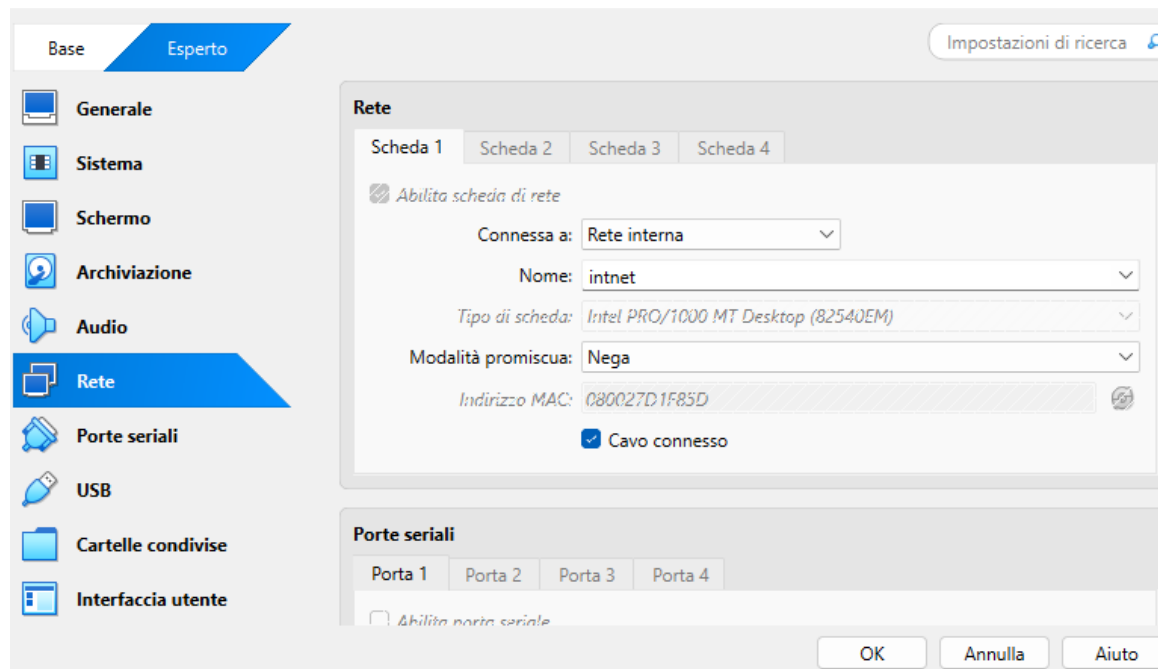
Address	Netmask	Gateway
192.168.50.100	24	192.168.50.1

Buttons "Add" and "Delete" are next to the table. Below the table, the "DNS servers" field contains "192.168.50.1". The "Search domains" and "DHCP client ID" fields are empty. A checkbox "Require IPv4 addressing for this connection to complete" is unchecked. A "Routes..." button is at the bottom right. At the very bottom are "Cancel" and "Save" buttons.

## Windows



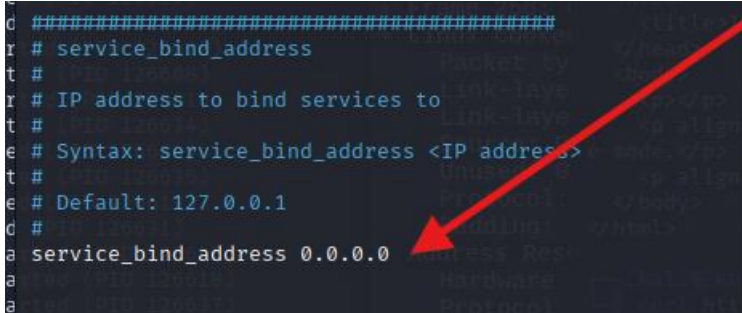
Entrambe le macchine si trovano sulla rete interna, quindi possono comunicare tra loro ma non con l'host



## CONFIGURAZIONE INetSim

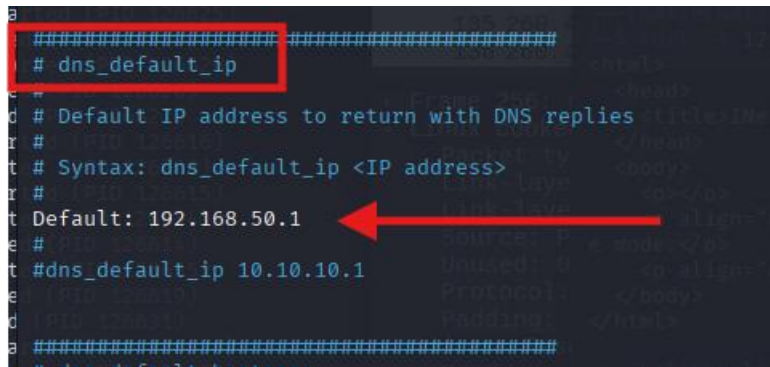
Avvio la configurazione tramite comando **sudo nano /etc/inetsim/inetsim.conf**

Tolgo il # che precede **service\_bind\_address**, per abilitarlo e lo imposto su 0.0.0.0 per fare in modo che le macchine comunichino



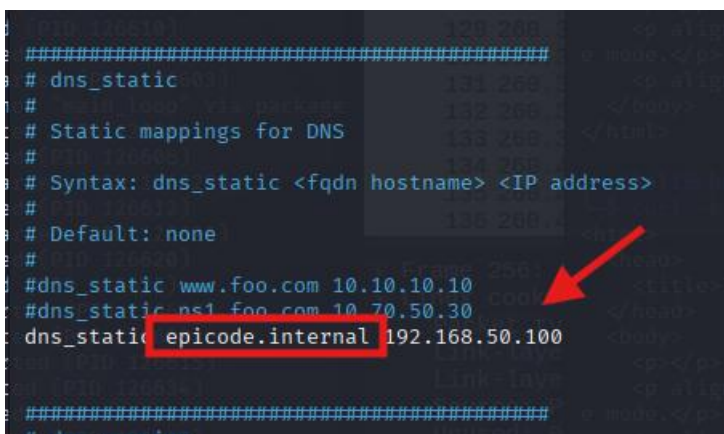
A screenshot of a terminal window showing the configuration file `/etc/inetsim/inetsim.conf` in nano editor. The file is dark-themed. A red arrow points from the top right towards the line `service_bind_address 0.0.0.0`, which has been uncommented (the '#' has been removed). The surrounding text includes comments about the syntax and default value (127.0.0.1).

Abilito il DNS e lo imposto con lo stesso IP configurato su Kali e Windows



A screenshot of a terminal window showing the configuration file `/etc/inetsim/inetsim.conf` in nano editor. A red box highlights the line `# dns_default_ip`, which has been uncommented. A red arrow points from the right towards the line `dns_default_ip 10.10.10.1`, which has been added below the default value of 192.168.50.1.

Abilito l'host name del DNS e lo imposto su **epicode.internal** associandolo all'IP della macchina Kali per poterla interrogare dal browser windows



A screenshot of a terminal window showing the configuration file `/etc/inetsim/inetsim.conf` in nano editor. A red box highlights the line `dns_static epicode.internal 192.168.50.100`, which has been added. A red arrow points from the right towards this line. The surrounding text includes comments about the syntax and default value (none).

Avvio il simulatore INetSim per avviare i processi

```
(kali@kali)-[~]
$ sudo inetsim
[sudo] password for kali:
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.
Warning: Unknown option 'Default:' in configuration file '/etc/inetsim/inetsim.conf' line 205
Configuration file parsed successfully.
== INetSim main process started (PID 147530) ==
Session ID: 147530
Listening on: 0.0.0.0
Real Date/Time: 2025-07-18 15:22:50
Fake Date/Time: 2025-07-18 15:22:50 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 147532)
Can't locate object method "main_loop" via package "Net::DNS::Nameserver" at /usr/share/perl5/INetSim/DNS.pm line 69.
* https_443_tcp - started (PID 147534)
* ident_113_tcp - started (PID 147545)
* chargen_19_tcp - started (PID 147557)
* smtps_465_tcp - started (PID 147536)
* pop3s_995_tcp - started (PID 147538)
* syslog_514_udp - started (PID 147546)
* time_37_tcp - started (PID 147547)
* ftp_21_tcp - started (PID 147539)
* http_80_tcp - started (PID 147533)
* smtp_25_tcp - started (PID 147535)
* ftps_990_tcp - started (PID 147540)
* ntp_123_udp - started (PID 147543)
* irc_6667_tcp - started (PID 147542)
* discard_9_tcp - started (PID 147553)
* quotd_17_tcp - started (PID 147555)
* tftp_69_udp - started (PID 147541)
* finger_79_tcp - started (PID 147544)
* quotd_17_udp - started (PID 147556)
* pop3_110_tcp - started (PID 147537)
* time_37_udp - started (PID 147548)
* echo_7_udp - started (PID 147552)
* echo_7_tcp - started (PID 147551)
* chargen_19_udp - started (PID 147558)
* dummy_1_udp - started (PID 147560)
* daytime_13_tcp - started (PID 147549)
* discard_9_udp - started (PID 147554)
* daytime_13_udp - started (PID 147550)
* dummy_1_tcp - started (PID 147559)
done.
Simulation running.
```

Apro Wireshark per metterlo in ascolto, impostandolo sulla nostra rete et0 e invio la richiesta http dal browser Windows



Vedremo i pacchetti http transitare; tra i dati visualizzati possiamo notare gli indirizzi MAC, indirizzo sorgente, destinazione e la porta 80, su cui viaggiano i dati di default sul protocollo http.

No.	Time	Source	Destination	Protocol	Length	Info
208	855.598325877	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
209	856.599809811	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
210	858.802175817	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
211	859.600119986	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
212	860.599981241	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
213	862.802459915	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
214	863.598155002	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
215	864.599472734	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
216	865.870493415	192.168.50.102	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
217	866.879566231	192.168.50.102	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
218	867.880295914	192.168.50.102	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
219	868.895791313	192.168.50.102	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
220	985.871558544	192.168.50.102	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

▶ Frame 215: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0  
 ▶ Ethernet II, Src: PCSSystemtec\_ad:0a:b9 (08:00:27:ad:0a:b9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 ▶ Address Resolution Protocol (request)  
   Hardware type: Ethernet (1)  
   Protocol type: IPv4 (0x0800)  
   Hardware size: 6  
   Protocol size: 4  
   Opcode: request (1)  
   Sender MAC address: PCSSystemtec\_ad:0a:b9 (08:00:27:ad:0a:b9) ←  
   Sender IP address: 192.168.50.102  
   Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00) ←  
   Target IP address: 192.168.50.1

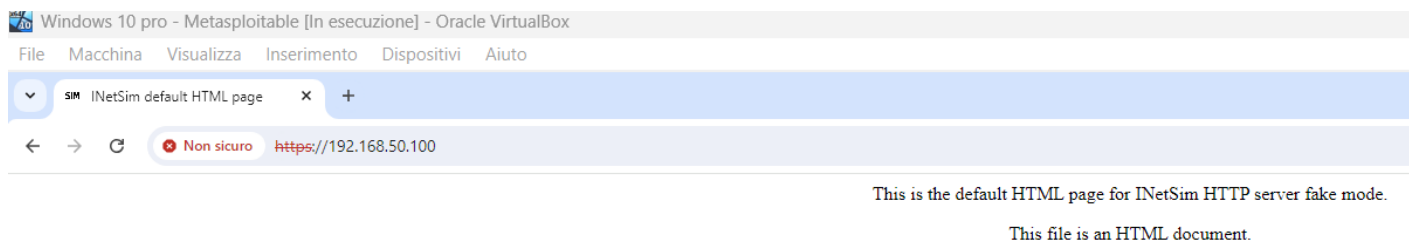
No.	Time	Source	Destination	Protocol	Length	Info
14	1.911915863	192.168.50.102	192.168.50.100	TCP	60	49541 → 80 [ACK] Seq
15	1.939068899	192.168.50.102	192.168.50.100	TCP	60	49541 → 80 [FIN, ACK
16	1.939105020	192.168.50.100	192.168.50.102	TCP	54	80 → 49541 [ACK] Seq
17	1.948555645	192.168.50.102	192.168.50.100	HTTP	447	GET /favicon.ico HT
18	1.948626163	192.168.50.100	192.168.50.102	TCP	54	80 → 49542 [ACK] Seq
19	1.966242779	192.168.50.100	192.168.50.102	TCP	207	80 → 49542 [PSH, ACK
20	1.970094329	192.168.50.100	192.168.50.102	HTTP	252	HTTP/1.1 200 OK (in
21	1.970876084	192.168.50.102	192.168.50.100	TCP	60	49542 → 80 [ACK] Seq
22	1.976389368	192.168.50.102	192.168.50.100	TCP	60	49542 → 80 [FIN, ACK
23	1.976424040	192.168.50.100	192.168.50.102	TCP	54	80 → 49542 [ACK] Seq
24	3.052868089	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1
25	3.597773141	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1
26	4.594922898	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.1

Time to Live: 128  
 Protocol: TCP (6)  
 Header Checksum: 0xb6bd [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 192.168.50.102  
 Destination Address: 192.168.50.100  
 [Stream index: 0]  
 ▶ Transmission Control Protocol, Src Port: 49542, Dst Port: 80, Seq: 1,  
   Source Port: 49542  
   Destination Port: 80 ←  
   [Stream index: 1]

Quindi azzero la schermata di Wireshark per visualizzare i soli pacchetti della prossima richiesta e lo metto in ascolto.

Sempre da browser, in Windows, invio una richiesta <https://192.168.50.100/>





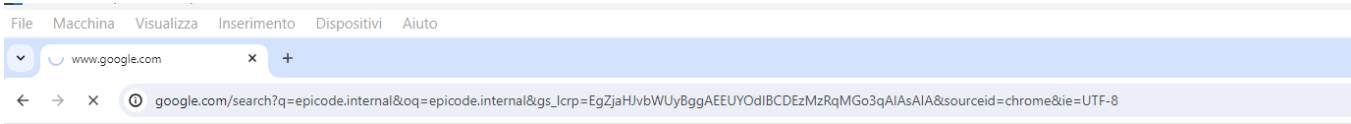
A questo punto vedremo transitare i pacchetti criptati HTTPS

No.	Time	Source	Destination	Protocol	Length	Info
40	3.353158579	192.168.50.102	192.168.50.100	TLSv1.3	2058	Client Hello
41	3.353186673	192.168.50.100	192.168.50.102	TCP	54	443 → 49549 [ACK] S
42	3.359648729	192.168.50.100	192.168.50.102	TLSv1.3	1497	Server Hello, Chang
43	3.361070885	192.168.50.102	192.168.50.100	TLSv1.3	84	Change Cipher Spec,
44	3.361071208	192.168.50.102	192.168.50.100	TCP	60	49549 → 443 [FIN, A
45	3.362632248	192.168.50.102	192.168.50.100	TCP	66	49550 → 443 [SYN] S
46	3.362657260	192.168.50.100	192.168.50.102	TCP	66	443 → 49550 [SYN, A
47	3.363635347	192.168.50.102	192.168.50.100	TCP	60	49550 → 443 [ACK] S
48	3.364188777	192.168.50.102	192.168.50.100	TLSv1.3	2026	Client Hello
49	3.364200953	192.168.50.100	192.168.50.102	TCP	54	443 → 49550 [ACK] S
50	3.366575082	192.168.50.100	192.168.50.102	TCP	54	443 → 49549 [FIN, A
51	3.367418375	192.168.50.102	192.168.50.100	TCP	60	49549 → 443 [ACK] S
52	3.382037636	192.168.50.100	192.168.50.102	TLSv1.3	1497	Server Hello, Chang
53	3.389717988	192.168.50.102	192.168.50.100	TLSv1.3	134	Change Cipher Spec,
54	3.390156975	192.168.50.102	192.168.50.100	TLSv1.3	687	Application Data
55	3.390453652	192.168.50.100	192.168.50.102	TLSv1.3	309	Application Data
56	3.412106891	192.168.50.100	192.168.50.102	TLSv1.3	729	Application Data, A
57	3.412811606	192.168.50.102	192.168.50.100	TCP	60	49550 → 443 [ACK] S
58	3.419775680	192.168.50.102	192.168.50.100	TCP	60	49550 → 443 [FIN, A
59	3.419806610	192.168.50.100	192.168.50.102	TCP	54	443 → 49550 [ACK] S
60	4.004188433	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.
61	4.826268176	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.
62	5.826691996	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.
63	8.403493684	PCSSystemtec_d1:f8:5d	PCSSystemtec_ad:0a:...	ARP	42	Who has 192.168.50.
64	8.405348984	PCSSystemtec_ad:0a:b9	PCSSystemtec_d1:f8:...	ARP	60	192.168.50.102 is a
65	11.172754097	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.
66	11.828129855	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.
67	12.826621267	PCSSystemtec_ad:0a:b9	Broadcast	ARP	60	Who has 192.168.50.

▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes cap	0000	ff ff ff ff ff ff	08 00 27 ad 0a b9	08 06 0
▶ Ethernet II, Src: PCSSystemtec_ad:0a:b9 (08:00:27	0010	08 00 06 04 00 01	08 00 27 ad 0a b9	c0 a8 3
▶ Address Resolution Protocol (request)	0020	00 00 00 00 00 00	c0 a8 32 01 00 00	00 00 0
Hardware type: Ethernet (1)	0030	00 00 00 00 00 00	00 00 00 00 00 00	

Successivamente, da browser invio una richiesta **epicode.internal**, in base a quanto impostato su INetSim.



## Impossibile raggiungere il sito

Impossibile trovare l'indirizzo DNS di [www.google.com](http://www.google.com). Stiamo analizzando il problema.

[Prova a eseguire lo strumento Diagnostica di rete Windows.](#)

DNS\_PROBE\_STARTED

Ricarica

La richiesta però non andrà a buon fine, a causa dell'errore restituito da INetSim in fase di lancio, evidenziato in rosso nell'immagine che segue.

```
(kali@kali)~$ sudo inetsim
[sudo] password for kali:
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.
Warning: Unknown option 'Default:' in configuration file '/etc/inetsim/inetsim.conf' line 205
Configuration file parsed successfully.
== INetSim main process started (PID 159884) ==
Session ID: 159884
Listening on: 0.0.0.0
Real Date/Time: 2025-07-18 15:48:08
Fake Date/Time: 2025-07-18 15:48:08 (Delta: 0 seconds)
Forking services ...
* dns_95_tcp_udp - started (PID 159894)
Can't locate object method "main_loop" via package "Net::DNS::Nameserver" at /usr/share/perl5/INetSim/DNS.pm line 69.
* daytime_13_tcp - started (PID 159911)
* http_80_tcp - started (PID 159895)
* finger_79_tcp - started (PID 159906)
* pop3_110_tcp - started (PID 159899)
* ftp_21_tcp - started (PID 159901)
* pop3s_995_tcp - started (PID 159900)
* time_37_tcp - started (PID 159909)
* syslog_514_udp - started (PID 159908)
* echo_7_tcp - started (PID 159913)
* smtp_25_tcp - started (PID 159897)
* tftp_69_udp - started (PID 159903)
* daytime_13_udp - started (PID 159912)
* discard_9_tcp - started (PID 159915)
* time_37_udp - started (PID 159910)
* smtps_465_tcp - started (PID 159898)
* ntp_123_udp - started (PID 159905)
* echo_7_udp - started (PID 159914)
* irc_6667_tcp - started (PID 159904)
* ftps_990_tcp - started (PID 159902)
* ident_113_tcp - started (PID 159907)
* https_443_tcp - started (PID 159896)
* quotd_17_udp - started (PID 159918)
* discard_9_udp - started (PID 159916)
* quotd_17_tcp - started (PID 159917)
* dummy_1_tcp - started (PID 159921)
* chargen_19_tcp - started (PID 159919)
* dummy_1_udp - started (PID 159922)
* chargen_19_udp - started (PID 159920)
done.
Simulation running.
```