

# CONFIGURAZIONE MACCHINA WINDOWS CON IP STATICO: (Client)

192.168.32.101

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright © 2009 Microsoft Corporation. All rights reserved.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . :
  IPv4 Address . . . . . : 192.168.32.101
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.32.1

Tunnel adapter isatap.{71178A4C-9E68-4AC0-A58D-F8A38143D72A}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : 

C:\>
```

# MACCHINA LINUX CON IP

## STATICO:

(Server)

192.168.32.100

```
michele@michele: ~
File Azioni Modifica Visualizza Aiuto
[michele@michele]-(~)
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host
        link-layer brd 00:00:00:00:00:00
        brd 00:00:00:00:00:00
        state UNKNOWN
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        link-layer brd 00:00:00:00:00:00
        brd 00:00:00:00:00:00
        state UNKNOWN
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7c:ab:6f brd ff:ff:ff:ff:ff:ff
    inet 192.168.32.100/24 brd 192.168.32.255 scope global eth0
        link-layer brd ff:ff:ff:ff:ff:ff
        brd ff:ff:ff:ff:ff:ff
        state UP
        valid_lft forever preferred_lft forever
        broadcast 192.168.32.255
        inet6 fe80::a00:27ff:fe7c:ab6f/64 scope link
            link-layer brd ff:ff:ff:ff:ff:ff
            brd ff:ff:ff:ff:ff:ff
            state UP
            valid_lft forever preferred_lft forever
michele@michele: ~
$ ping -c 1 192.168.32.100
PING 192.168.32.100 (192.168.32.100) 56(84) bytes from 192.168.32.100: icmp_seq=1 ttl=64 time=0.000 ms
Real Date/Time: 2023-05-08 00:08:38
Fake Date/Time: 2023-05-08 00:08:38 (Delta: 0 seconds)
Forking services...
  * dns_53_tcp_udp - started (PID 1557)
  * ntp_123_udp - started (PID 1568)
  * finger_79_tcp - started (PID 1569)
  * ident_113_tcp - started (PID 1570)
```

# SERVIZIO DNS IMPOSTATO DALLA MACCHINA LINUX:

Sono stati tolti gli asterischi dalle seguenti categorie "service\_bind\_address", "dns\_default\_ip" con l'ip della macchina Linux, faremo la stessa cosa per il "dns\_static" ma aggiungeremo il nome episode.internal. Una volta

impostato il server in questo modo:

```
File Azioni Modifica Visualizza Aiuto
GNU nano 7.2 /etc/inetsim/inetsim.conf
[sudo] password di michele:
#####
# service_bind_addresshele:
#NetSim 1.3.2 (2020-05-19) by Matthias Eckert & Ti
#IPaddress to bind services to log/inetsim/
#sing data directory: /var/lib/inetsim/
## Syntax: service_bind_address <IP/Address> report/
#sing configuration file: /etc/inetsim/inetsim.conf
#aDefault: 127.0.0.1n file.
#se of uninitialized value $args[1] in lc at /usr/
service_bind_address 192.168.32.100
Warning: Unknown service name '' in configuration
conf' line 13
#####
# service_run_as_useress started (PID 1547) ===
#session ID: 1547
# User to run services 8.32.100
#real Date/Time: 2023-05-08 00:08:38
# Syntax: /service_run_as_user: <username>ta: 0 seco
#Forking services ...
# Default: inetsim - started (PID 1557)
# * ntp_123_udp - started (PID 1568)
# * finger_79_tcp - started (PID 1569)
^G Guida _113_t^O Salva rted (P^W Cerca
^X Escicard_9_u^R Inserisci (P^Sostituisci ^K Taglia
^U Incolla
```

"the quiet"

```
michele@michele: ~
File Azioni Modifica Visualizza Aiuto
GNU nano 7.2 /etc/inetsim/inetsim.conf
[sudo] password di michele:
#####
# dns_default_ip
# Default IP address to return with DNS replies Thomas
# sing log directory: /var/log/inetsim/
# Syntax: dns_default_ip <IP/Address> etsim/
# sing report directory: /var/log/inetsim/report/
# Default: i127.0.0.1file: /etc/inetsim/inetsim.conf
#arsing configuration file.
dns_default_ip 192.168.32.100rgs[1] in lc at /usr/share/
pm line 529, <$CONFIGFILE> line 13.
Warning: Unknown service name '' in configuration file '
#####
# dns_default_hostnameed successfully.
# InetSim main process started (PID 1547) ===
# Default hostname to return with DNS replies
# listening on: 192.168.32.100
# Syntax: /dns_default_hostname <hostname>
#ake Date/Time: 2023-05-08 00:08:38 (Delta: 0 seconds)
# Default: wwwces ...
# * dns_53_tcp_udp - started (PID 1557)
#dns_default_hostname somehost 1568)
# * finger_79_tcp - started (PID 1569)
^G Guida _113_t^O Salva rted (P^W Cerca
^X Escicard_9_u^R Inserisci (P^Sostituisci ^K Taglia
^U Incolla
```

"the quiet"

michele@michele: ~

File Azioni Modifica Visualizza Aiuto

GNU nano 7.2 /etc/inetsim/inetsim.conf

```
[sudo] password di michele:  
#####
#dns_staticord di michele:  
#NetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungen  
# Static mappings for DNS /var/log/inetsim/  
# sing data directory: /var/lib/inetsim/  
# Syntax: dns_static <fqdn hostname> <IP:address>/  
# sing configuration file: /etc/inetsim/inetsim.conf  
# Default: none ration file.  
#se of uninitialized value $args[1] in lc at /usr/share/perl5/  
dns_static episode.internal 192.168.32.100  
#dns_static ns1.foo.com 10.70.50.30 configuration file '/etc/i  
#dns_static ftp.bar.net 10.10.20.30  
Configuration file parsed successfully.  
== INetSim main process started (PID 1547) ==  
#####
# dns_version 192.168.32.100  
#real Date/Time: 2023-05-08 00:08:38  
# DNS version: 2023-05-08 00:08:38 (Delta: 0 seconds)  
#Forking services ...  
# Syntax: dns_version <version> ID 1557)  
* ntp_123_udp - started (PID 1568)  
* finger_79_tcp - started (PID 1569)  
G Guida _113_ Salva Crea Cerca Taglia  
X Esci Card_9_ Inserisci Sostituisci Incolla
```

"the quiete

## ATTIVARE SERVER:

```
michele@michele: ~
```

esecuzione] - Oracle VM VirtualBox

Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

```
File Azioni Modifica Visualizza Aiuto  
* discard_9_udp - started (PID 1579) im/inetsim.conf  
* smtp_25_tcp - started (PID 1560)  
* ftp_21_tcp - started (PID 1564)  
* syslog_514_udp - started (PID 1571)  
* daytime_13_tcp - started (PID 1574)  
* irc_6667_tcp - started (PID 1567)  
* tftp_69_udp - started (PID 1566)  
* https_443_tcp - started (PID 1559)  
* echo_7_tcp - started (PID 1576) <IP:address>  
* pop3_110_tcp - started (PID 1562)  
* discard_9_tcp - started (PID 1578)  
* time_37_udp - started (PID 1573)  
* quotd_17_udp - started (PID 1581) 2.100  
* echo_7_udp - started (PID 1577)  
* chargen_19_tcp - started (PID 1582)  
* daytime_13_udp - started (PID 1575)  
* dummy_1_udp - started (PID 1585)  
* smtps_465_tcp - started (PID 1561) com  
* pop3s_995_tcp - started (PID 1563)  
* time_37_tcp - started (PID 1572)  
* quotd_17_tcp - started (PID 1580)  
* chargen_19_udp - started (PID 1583)  
* ftps_990_tcp - started (PID 1565)  
* http_80_tcp - started (PID 1558)  
* dummy_1_tcp - started (PID 1584)  
done.  
Simulation running.
```

Salva Cerca Taglia Esegui Giust

"the quiete yo

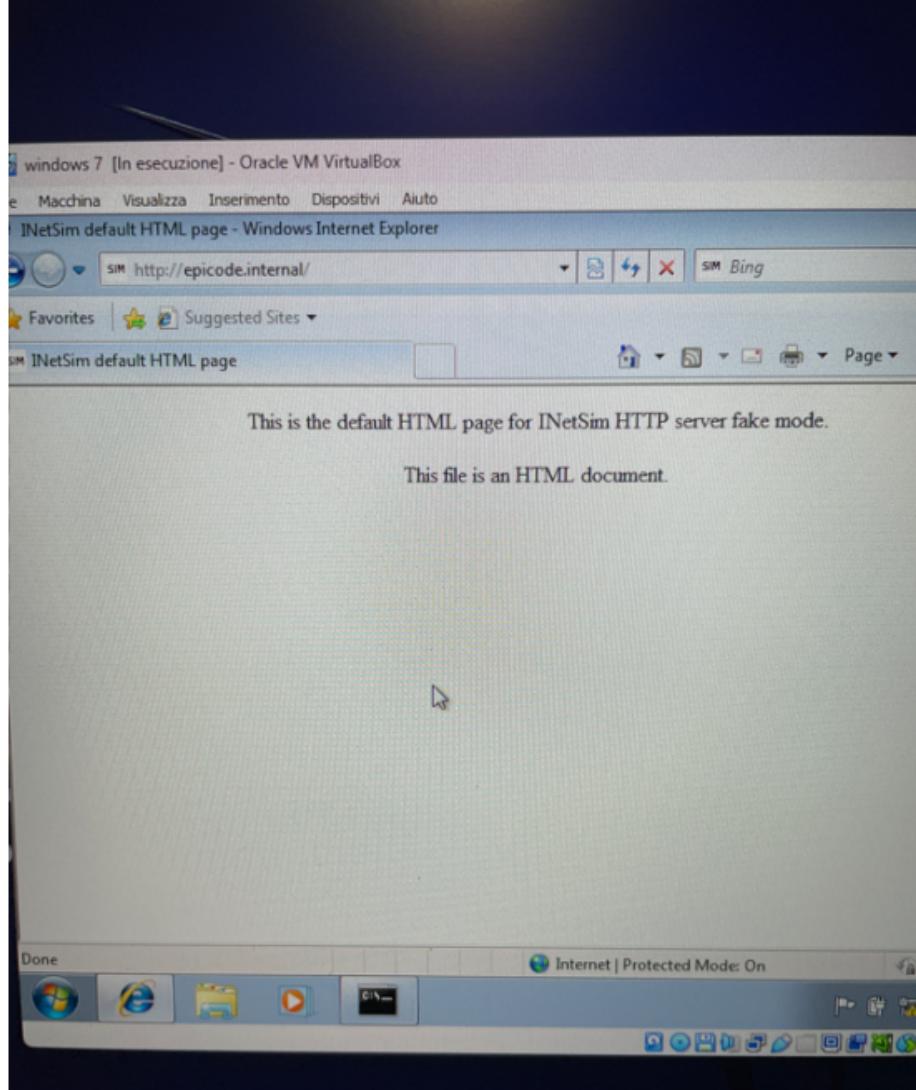
Una volta arrivato il server tramite comando:

"nano sudo /etc/inetsim/inetsim.conf"

Andremo a stabilire una connessione tra il server e il nostro

client

## CHIAMATA DA WINDOWS:

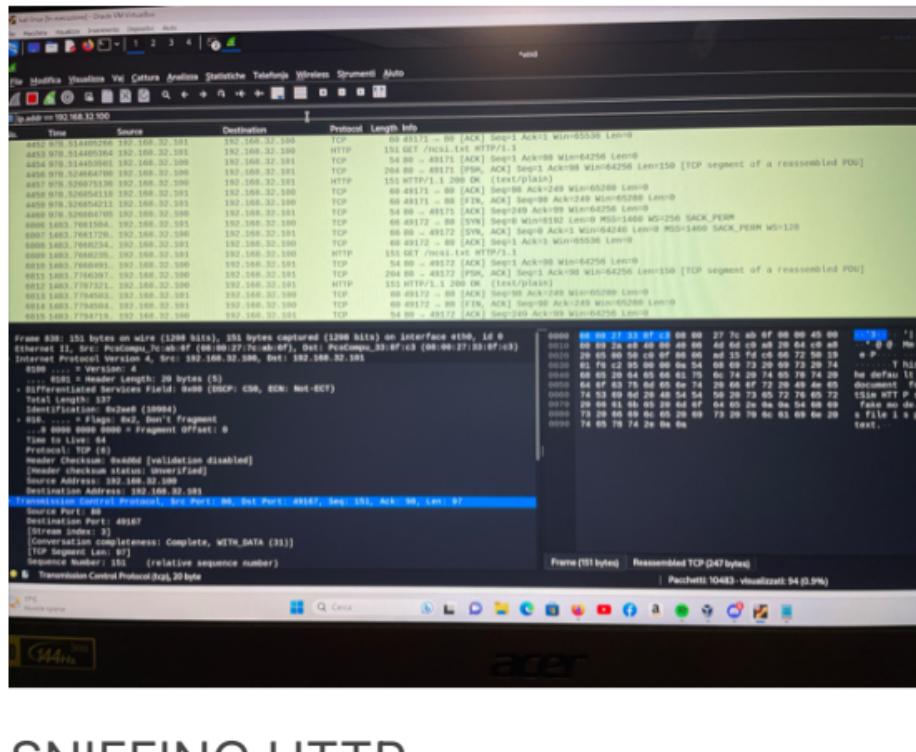


Una volta aver cercato sul motore di ricerca il nostro il nome del nostro server, tramite wireshark cerchiamo di capirne nel dettaglio lo scambio di pacchetti con uno “sniffing della rete”

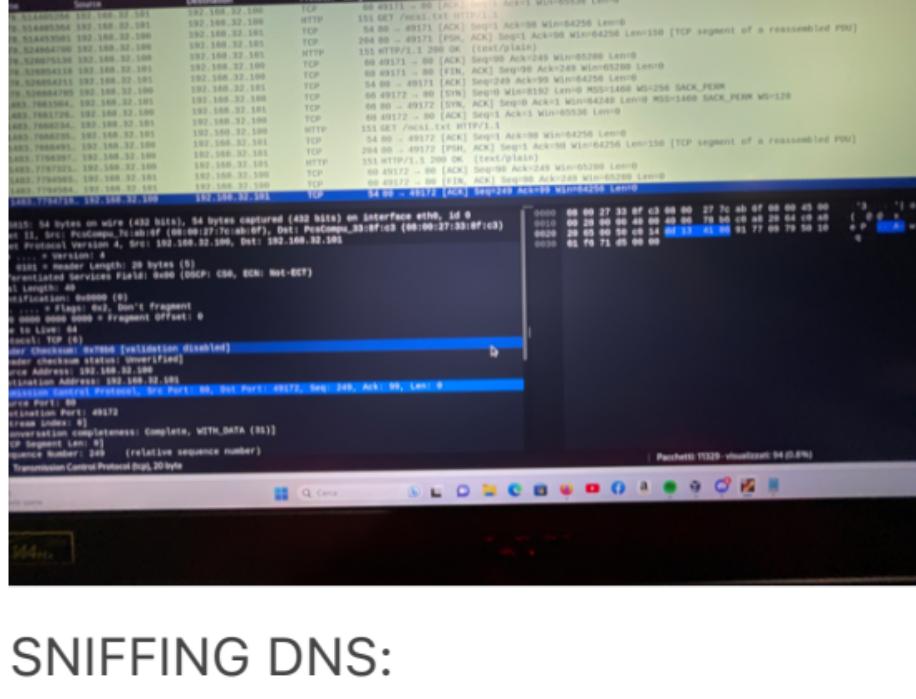
Sulla macchina Linux

## SNIFFING:

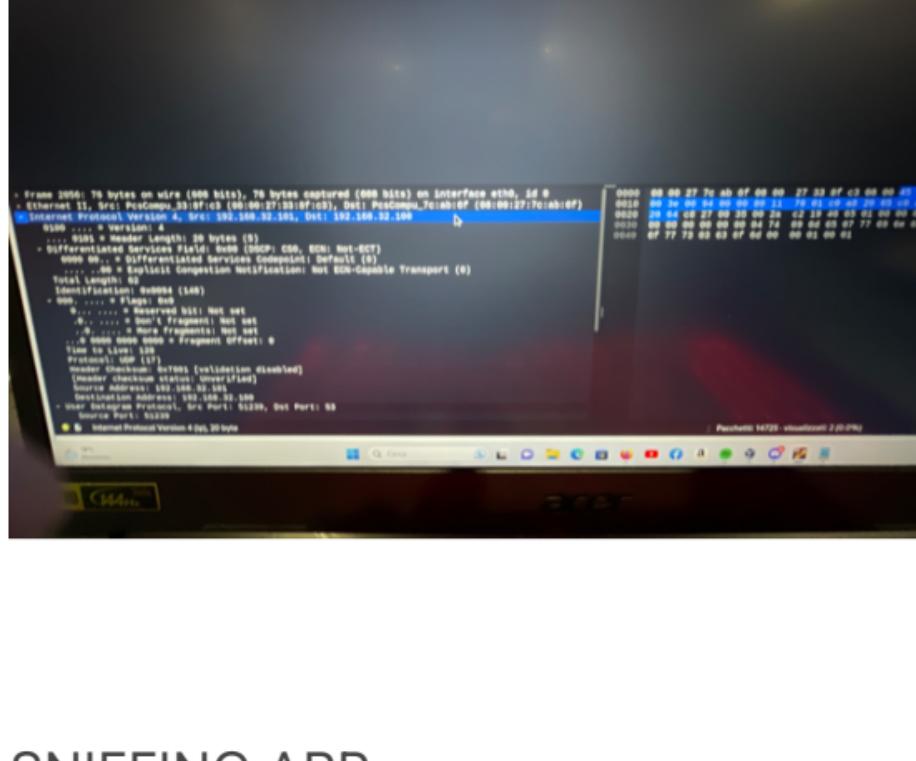
Metto nel filtro la priorità all'indirizzo 192.168.32.100 (ip server) tramite il filtro ip.addr== ipserver



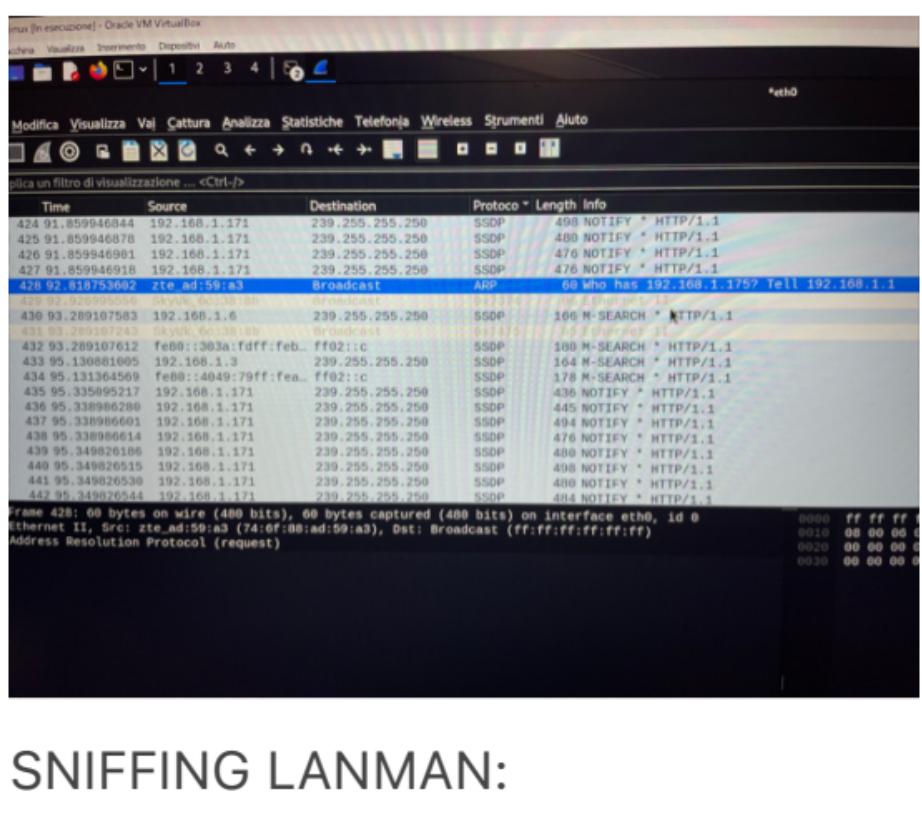
## SNIFFING HTTP:



## SNIFFING DNS:



## SNIFFING ARP:



## SNIFFING LANMAN:

