

Comunicazione tra client e host

Con questa simulazione metteremo in contatto due macchine virtuali con le seguenti caratteristiche:

- VM Kali con indirizzo ip statico 192.168.32.101 e MAC address 08002738BAF3;
- VM Windows con indirizzo ip statico 192.168.32.101 e MAC address 080027603D01.
- Server DNS attivo con indirizzo ip 192.168.32.100.

Comunicazione tra macchine virtuali e ricerca tramite web browser

Con la simulazione andremo a richiedere tramite il web browser una risorsa all' hostname **epicode.internal**.

Avendo impostato le macchine virtuali con ip statico andremo ad attivare il nostro **DNS server** (viene impiegato dai dispositivi per tradurre gli indirizzi URL per la macchina rendendoli leggibili all'uomo).

Accedendo alla vm di kali e tramite il terminale sarà possibile attivare il tool **inetsim** (permette di simulare i servizi internet comuni in un ambiente isolato).

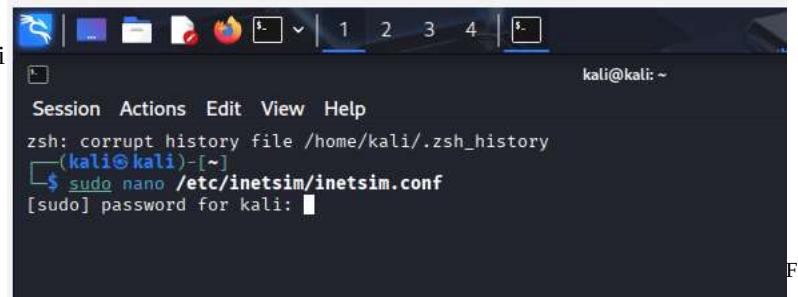
Attivazione e programmazione di “inetsim”

Fig 1

Andiamo a ricercare la pagina per la configurazione dei parametri del tool inetsim.

Utilizzando il comando “`sudo nano`

`/etc/inetsim/inetsim.conf`



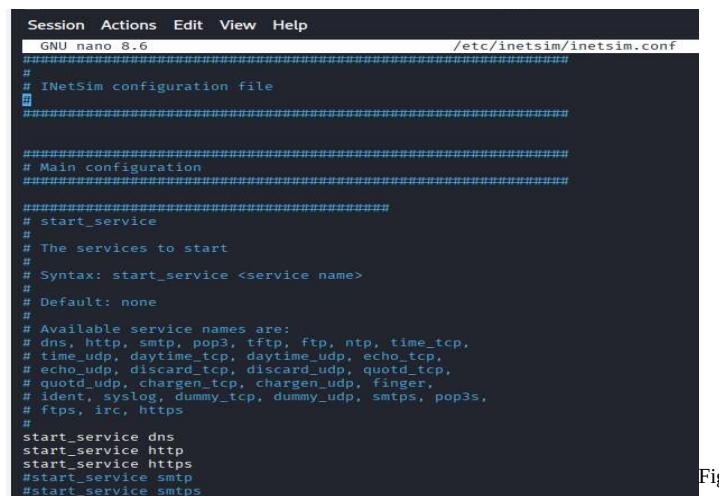
The screenshot shows a terminal window titled 'Session Actions Edit View Help'. The command `sudo nano /etc/inetsim/inetsim.conf` is being typed into the terminal. The terminal prompt is `(kali㉿kali)-[~]`. The background shows a desktop environment with icons for various applications like a browser and file manager.

Fig 1

Fig 2

Attiveremo il tool sui protocolli HTTPs, HTTP e DNS.

All' apertura della pagina tutte le righe saranno precedute da un “#”, questo fa sì che il terminale legga tutto come un commento. Andandolo a cancellare il cancelletto all'inizio della riga, come possiamo vedere in foto, il colore della riga diventa bianco e il Pc le leggerà come dei comandi, in questo caso le tre righe rappresentano i comandi di attivazione dei tre protocolli su indicati.



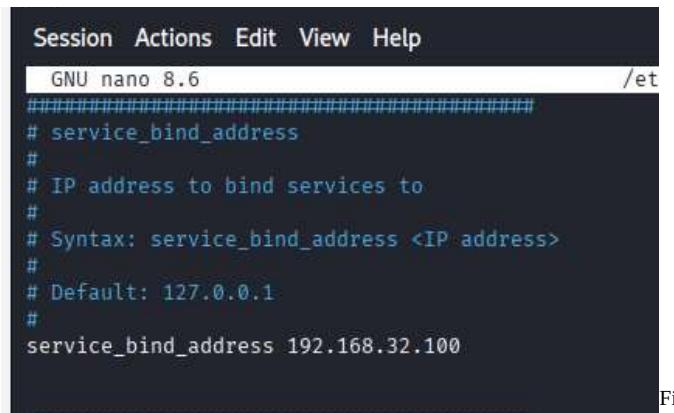
The screenshot shows a terminal window titled 'Session Actions Edit View Help' with the file `/etc/inetsim/inetsim.conf` open in 'GNU nano 8.6'. The file contains several lines of configuration comments starting with '#'. The lines are:
InetSim configuration file
Main configuration
start_service
The 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 http
start_service https
#start_service smtp
#start_service smtps

Fig 2

Entrando più nello specifico andiamo a modificare i parametri del DNS

Fig 3

Con il primo parametro andiamo a definire su quale interfaccia di rete e indirizzo ip inetsim deve "ascoltare" le connessioni in entrata.

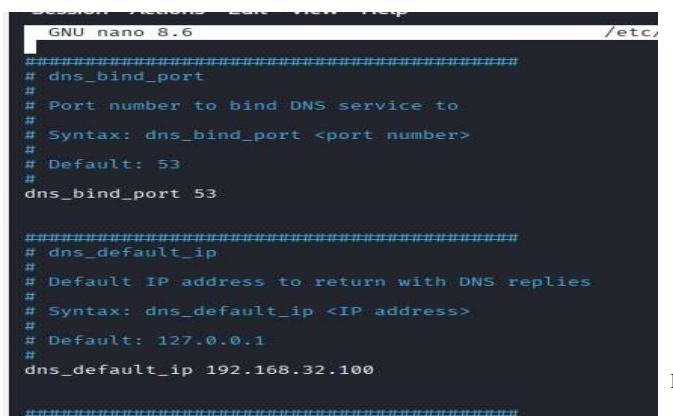


```
Session Actions Edit View Help
GNU nano 8.6
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100
```

Fig 3

Fig 4

Andiamo a definire per prima cosa la porta su cui è impostato il DNS, di default è già sulla porta 53, ma per una maggiore sicurezza gliela definiamo con un comando. In secondo luogo andiamo a dare un indirizzo ip al server.



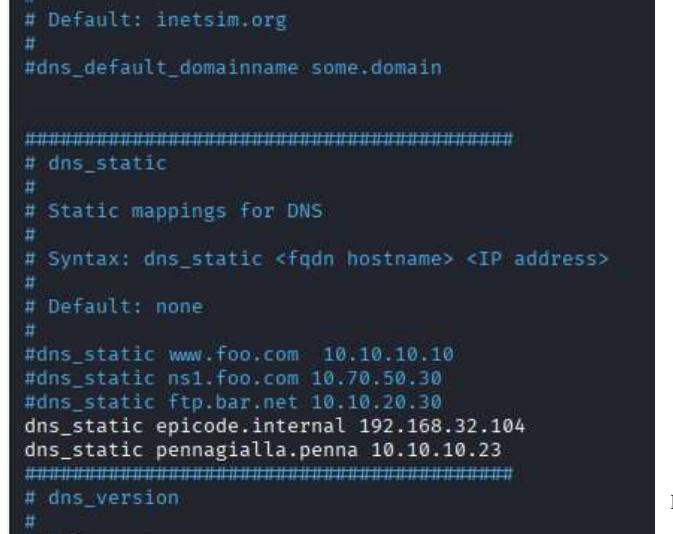
```
Session Actions Edit View Help
GNU nano 8.6
#####
# dns_bind_port
#
# Port number to bind DNS service to
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
dns_bind_port 53

#####
# 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
```

Fig 4

Fig 5

Con l'ultima impostazione definiamo l' hostname della risorsa che andremo a ricercare, in questo caso "**epicode.internal**".



```
#####
# Default: inetsim.org
#
#dns_default_domainname some.domain

#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
#dns_static www.foo.com 10.10.10.10
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
dns_static epicode.internal 192.168.32.104
dns_static pennajialla.penna 10.10.10.23
#####
# dns_version
#
```

Fig 5

Fig 6

Al termine della gestione dei parametri faremo partire inetsim con autorizzazioni da amministratore col comando “**sudo inetsim**”. Avremo la certezza che il programma sia in esecuzione nel momento in cui potremo leggere sul terminale “**Simulation Running**”

```
slide@vm:~$ sudo inetsim
[sudo] password for slide:
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 2382) ==
Session ID: 2382
Listening on: 192.168.50.100
Real Date/Time: 2026-01-16 12:16:27
Fake Date/Time: 2026-01-16 12:16:27 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 2384)
* http_80_tcp - started (PID 2385)
* https_443_tcp - started (PID 2386)
done.
Simulation running.
```

Fig 6

La prima parte del processo è terminata, i passaggi successivo saranno:

- Accensione della VM Windows;
- Ricercare tramite il web browser la pagina **epicode.internal**;
- Controllo del risultato della simulazione.

Controllo del risultato della simulazione

A questo punto andremo ad approfondire l’ultimo punto e quindi a controllare che tutto funzioni correttamente.

Nel nostro caso inizialmente avremo dei problemi in quanto il tool inetsim non ha gli aggiornamenti alle librerie (moduli per gestire i vari protocolli, necessari per farlo funzionare).

Per risolvere la problematica abbiamo dovuto ricercarle e scaricarle tramite il comando “force get NLNETLABS/Net-DNS-1.37.tar.gz” per poi installarle con il comando successivo “install NLNETLABS/Net-DNS-1.37”.

Risolta la problematica andiamo a ricercare la pagina web.

Fig 7

Dopo la risoluzione della problematica delle librerie possiamo vedere che la ricerca della pagina è andata a buon fine.

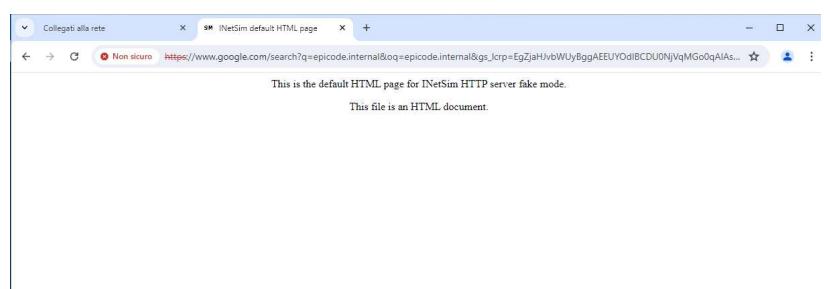


Fig 7

Fig 8

Per una maggiore sicurezza andiamo a controllare tramite terminale se il DNS riceve il collegamento da parte di windows, come da figura possiamo vedere che la simulazione è andata a buon fine.

```

nuovo Clone di di Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ping 192.168.32.100

Esecuzione di Ping a 192.168.32.100 con 32 byte di dati:
Risposta da 192.168.32.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.32.100:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 1ms, Medio = 0ms

C:\Users\user>ping epicode.internal

Esecuzione di Ping a epicode.internal [192.168.32.104] con 32 byte di dati:
Risposta da 192.168.32.101: Host di destinazione non raggiungibile.

Statistiche Ping per 192.168.32.104:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (% persi),

C:\Users\user>netcat

```

Fig 8

Lettura del traffico dati tramite Wireshark

Nell' ultima parte della simulazione dovremmo controllare il traffico dei pacchetti trasmessi tramite il programma “**wireshark**”, probabilmente per problemi di connessione o di macchine virtuali il risultato non è quello sperato, in quanto dal risultato, nonostante più tentativi dall'applicativo risultano solo alcuni pacchetti iniziali per provare a popolare la “**ARP Table**” (Tabella che contiene tutti gli indirizzi Mac travati sulla linea con cui la macchina entra in comunicazione) **Fig 9**.

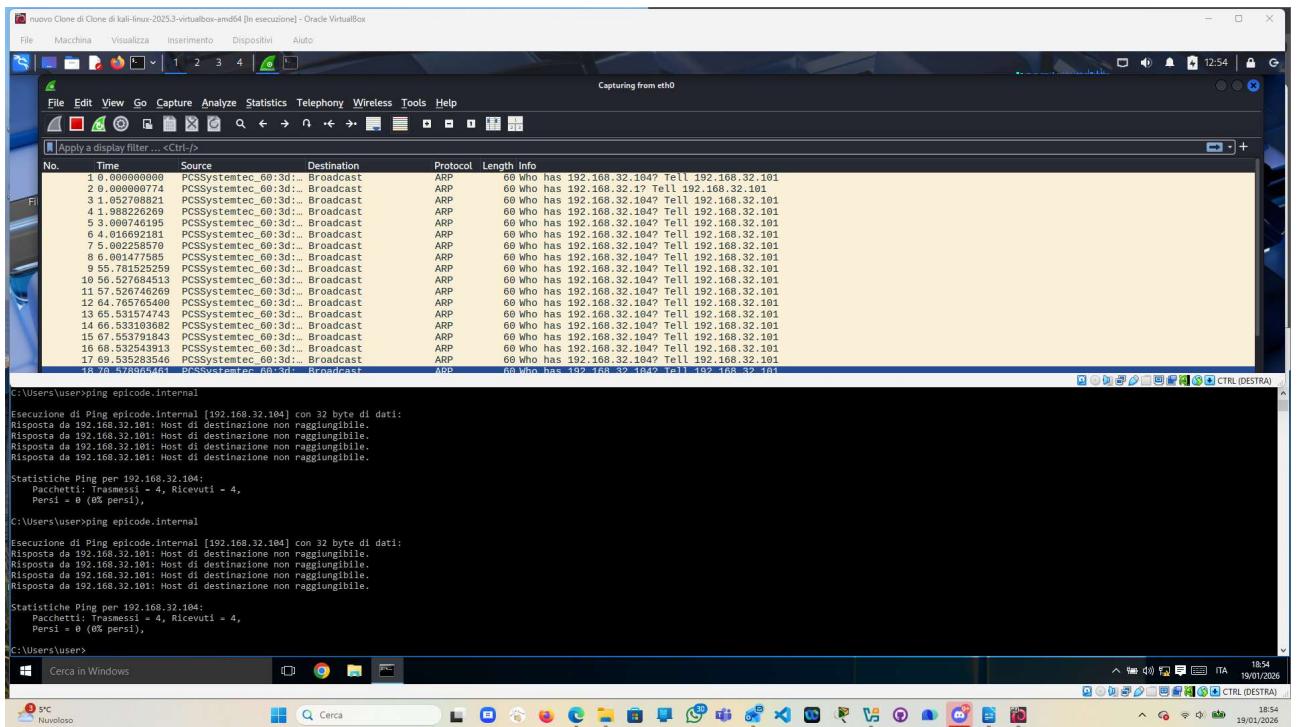


Fig 9