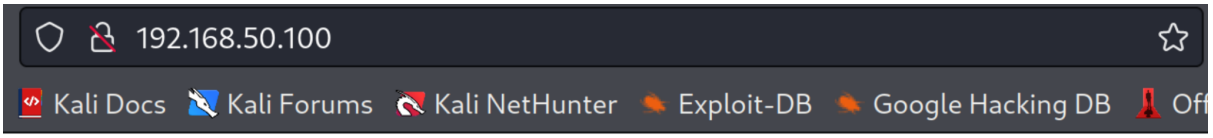
Windows firewall Inetsim e Wireshark

Iniziamo dalla rapida configurazione dell'applicazione Inetsim, aprendo il terminale(root) di Kali copiamo il nostro IP dopo aver eseguito un ifconfig(nel nostro caso essendo statico già lo conosciamo 192.168.50.100). Procediamo alla modifica del file di configurazione di Inetsim che si trova al percorso:
/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 192.168.50.100
```

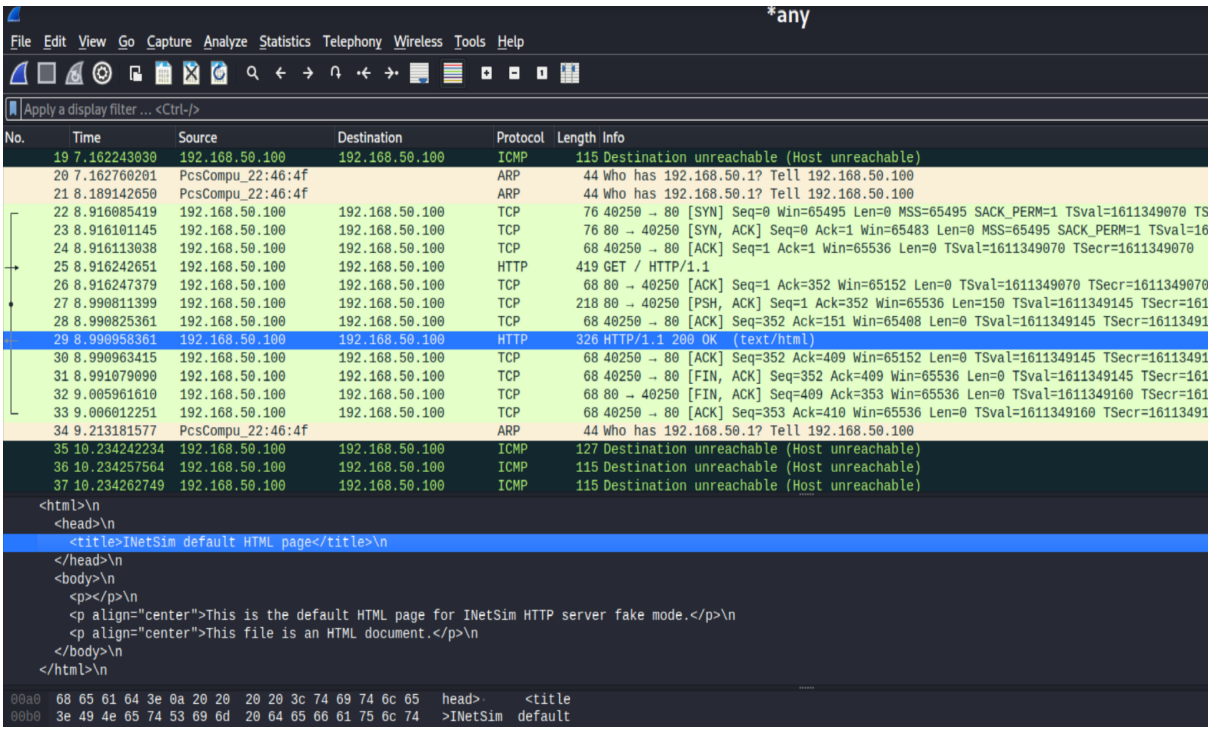
come da immagine andiamo a inserire il nostro IP come DNS (togliendo il # così da rendere effettiva la modifica). Effettuiamo la stessa modifica per la voce:
service_bind_address 192.168.50.100.
Dopo aver salvato il file Inetsim è pronto per essere avviato così da simulare una finta connessione ad una generica pagina HTML. Infatti aprendo il browser e recandosi all'indirizzo IP utilizzato otteniamo:



This is the default HTML page for INetSim HTTP server fake mode.

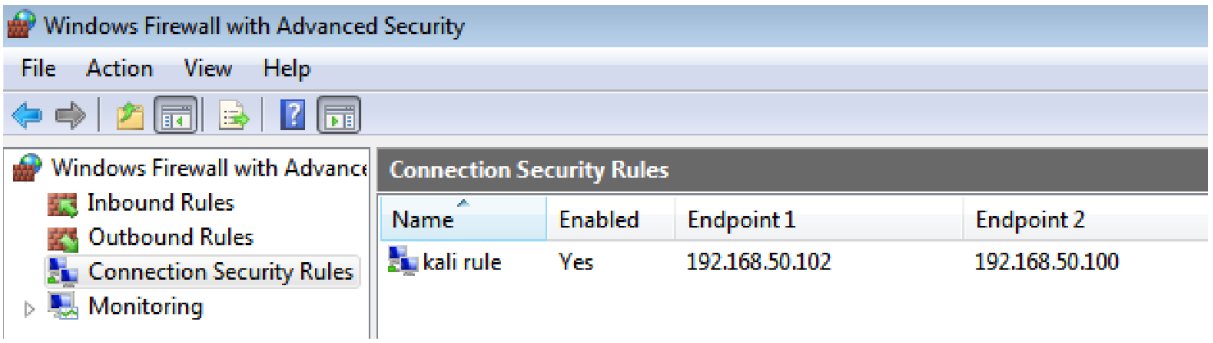
This file is an HTML document.

Alternativamente possiamo eseguire un ifconfig da terminale per ottenere lo stesso risultato. Adesso che abbiamo la conferma di funzionamento dell'applicazione possiamo andare a sniffare il traffico dati con l'utilizzo di wireshark. In pochi secondi avremo già catturato diversi pacchetti di diverso tipo. Soffermiamoci in particolare su quelli TCP che occupandosi della trasmissione dei dati utilizzano il Three-way-handshake, e su quelli di tipo HTTP che (come evidenziato in figura) trasmettono direttamente all'IP di destinazione il codice HTML della finta pagina generata da Inetsim.



Impostazione del Firewall di Windows 7: Aggiunta regola di connessione.

Per permettere al firewall di funzionare senza disturbare la connessione tra le nostre 2 macchine virtuali è sufficiente aggiungere una nuova regola alle Connection Security Rules del firewall stesso specificando l'indirizzo IP di entrambe le macchine da collegare.



Eseguiamo un test di ping per verificare che tutto funzioni.