W3D4 - Pratica

EPICODE

W3D4 - Pratica PDF

Esercizio

L'esercizio di oggi mira a consolidare le conoscenze acquisite.

Vedremo due esercizi: I) la configurazione di una policy sul firewall windows; II) una packet capture con Wireshark.

Vedremo anche come simulare alcuni servizi di rete con un tool pre-installato su Kali Linux (InetSim)

Esercizio:

- Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall)
- Utilizzo dell'utility InetSim per l'emulazione di servizi Internet
- Cattura di pacchetti con Wireshark

Per permettere il ping da Linux a Win7 devo iniziare a fare un settaggio del Firewall di Win7.

Dal menu iniziale cerco Windows Firewall

- Impostazioni avanzate
- Regole connessioni in entrata
- Azione
- Nuova regola (scelgo una regola che permetterà il ping con kali)
- Personalizzata
- Tutti i programmi
- Tipo di protocollo ICMPv4
- Qualsiasi indirizzo IP
- Consenti la connessione
- "Allow_ping"

A questo punto il **ping tra kali e win7 verrà consentito**

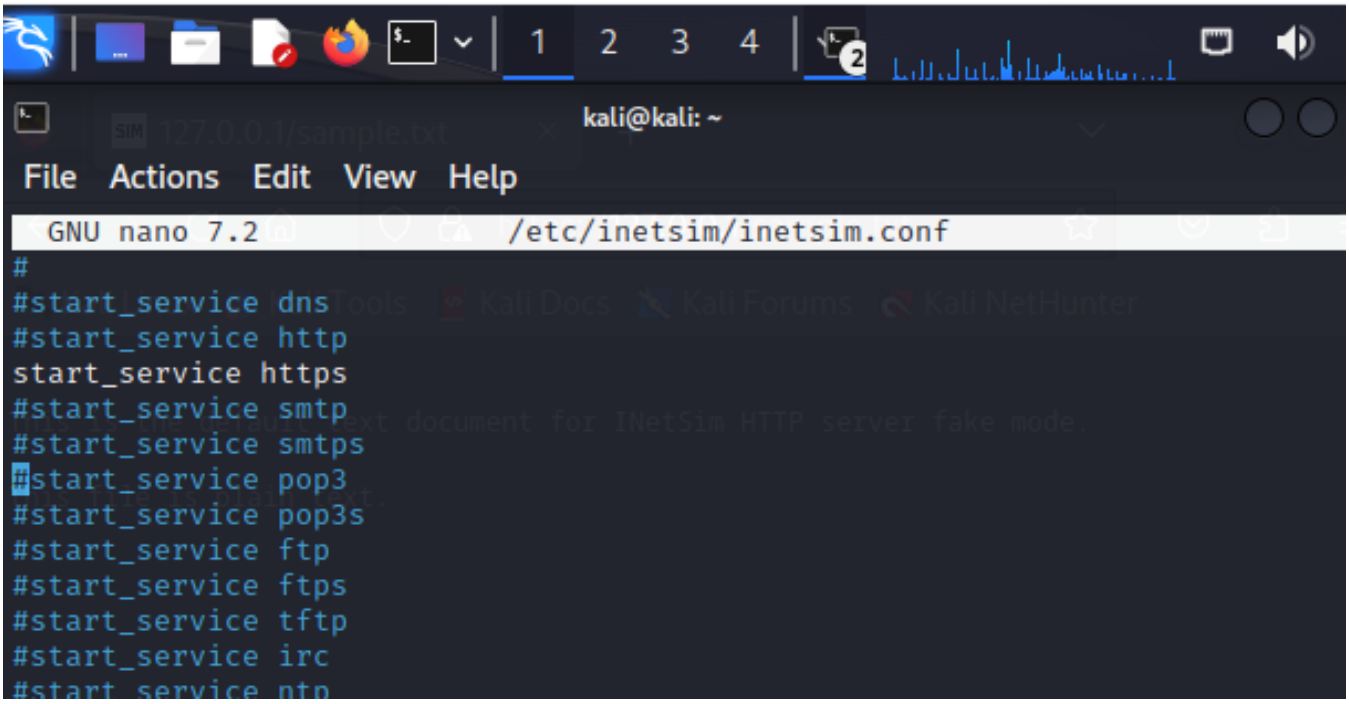
Ora utilizzerò un altro tool preinstallato su Kali, cioè **InetSim** che serve a simulare alcuni servizi internet per esempio HTTP e HTTPS. Verrà cosi emulata una connessione come fosse reale e la si vedrà nel dettaglio proprio per vedere la differenza tra HTTP e HTTPS.

Passo ora alla configurazione di InetSim tramite il file inetsim.conf al path

/etc/inetsim

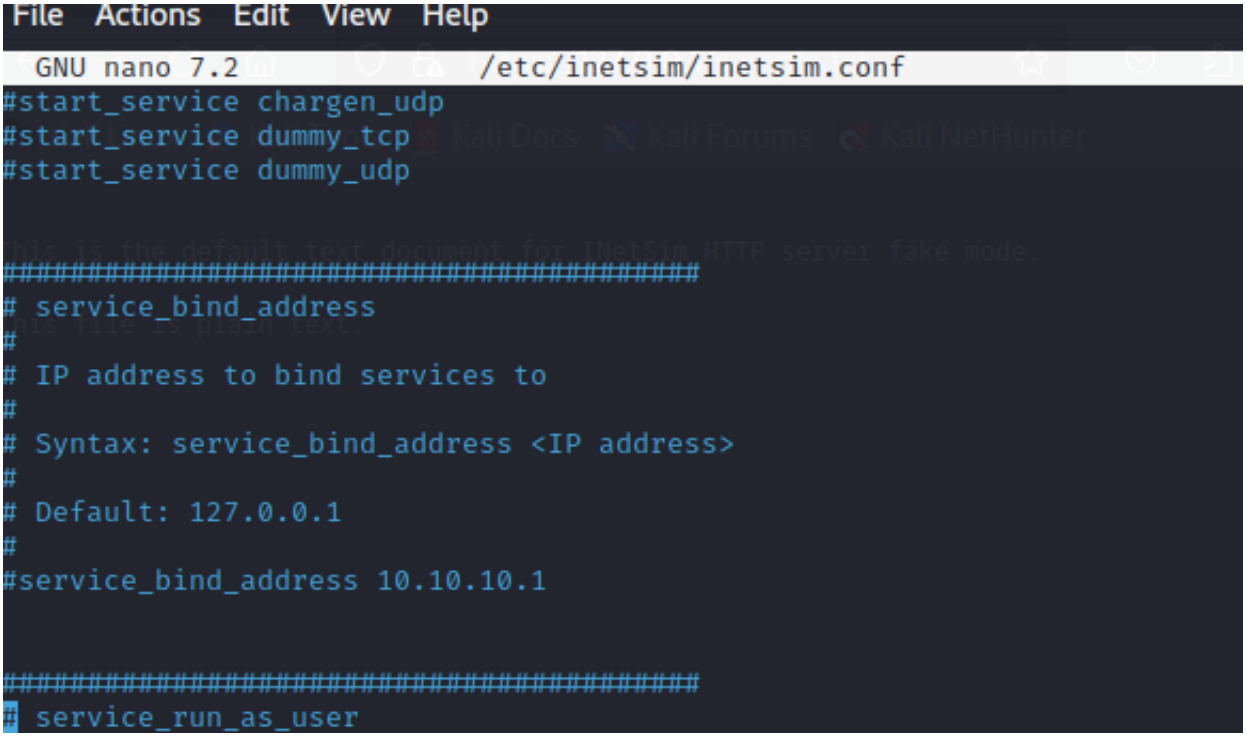
Si possono scegliere quali servizi avviare e su quale porta avviarli.

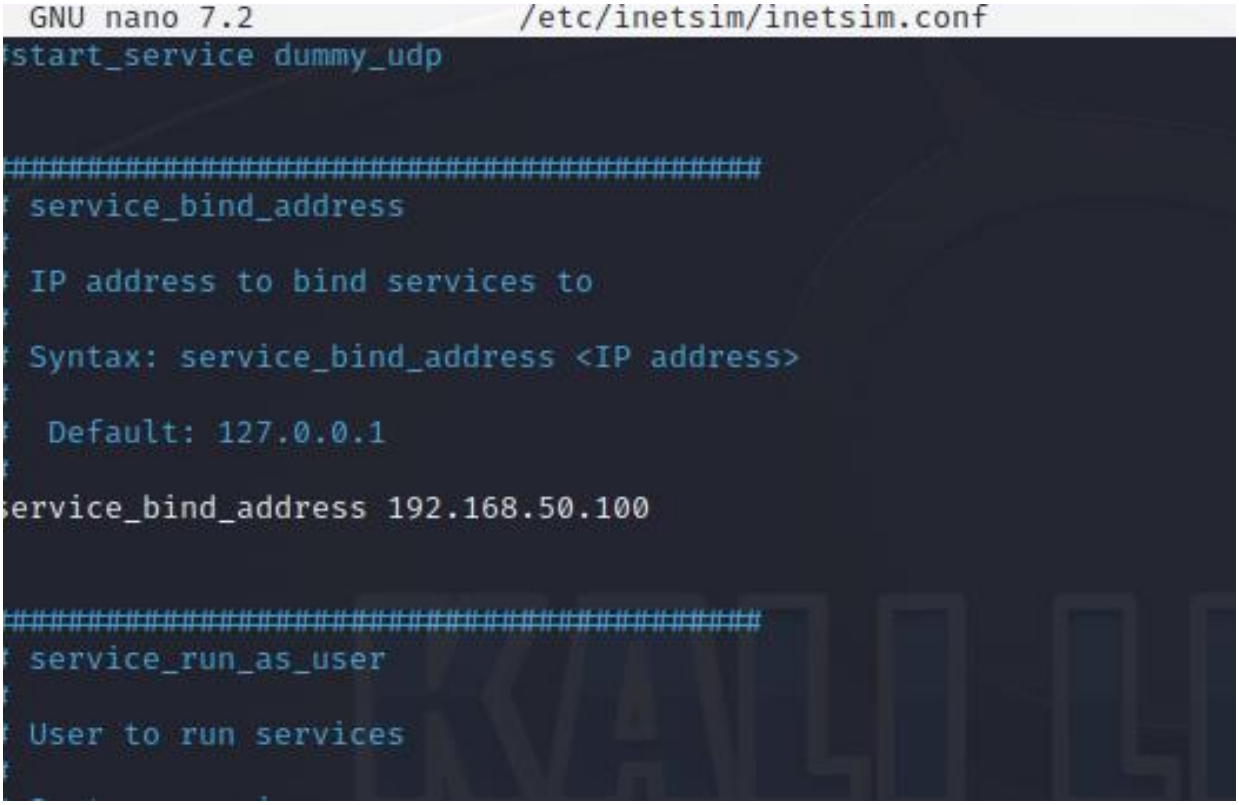
Avvio Kali ed eseguo il comando sudo nano /etc/inetsim/inetsim.conf



Ora attivo solo il servizio HTTPS quindi aggiungo un # prima di ogni riga lasciando scoperto appunto HTTPS cosi da analizzare il traffico dell'HTTPS

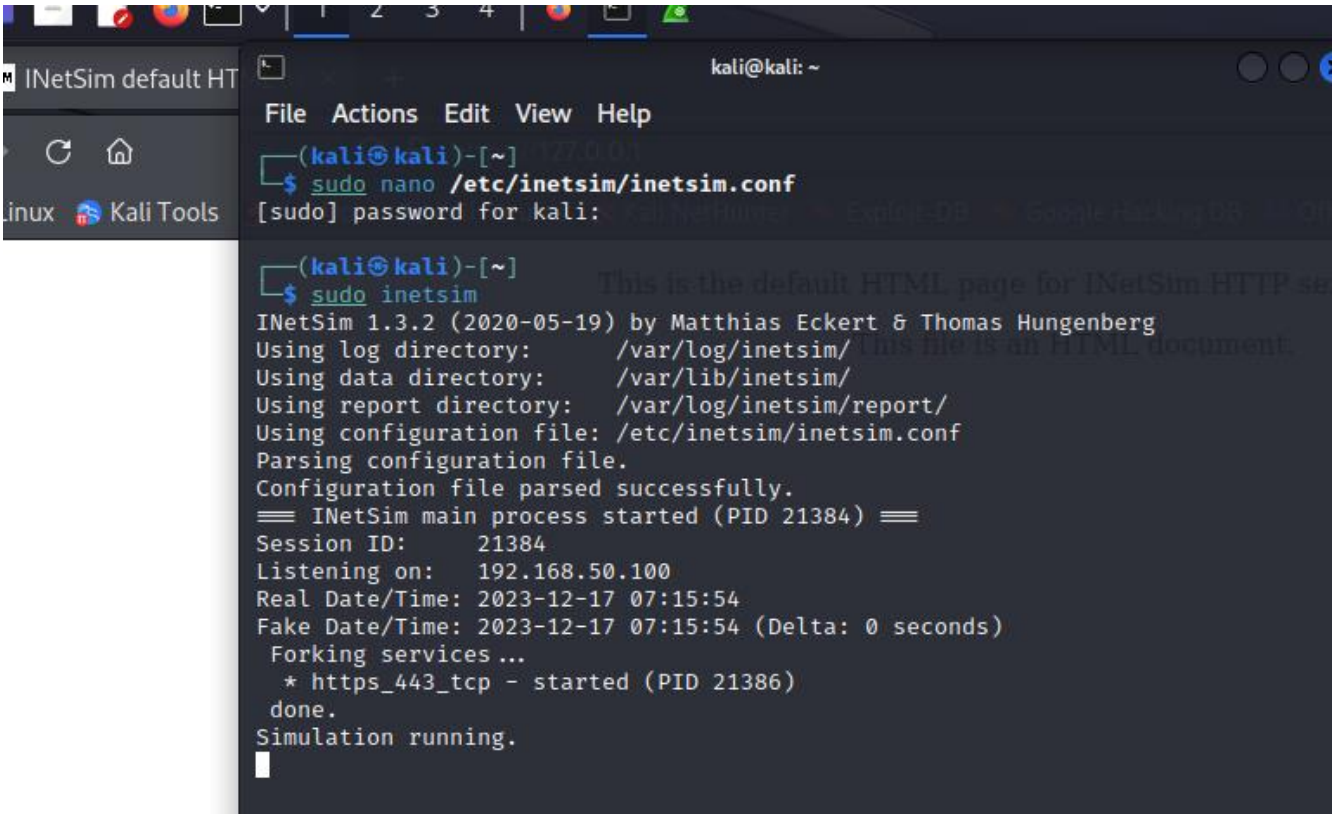
Nella sezione successiva possiamo decidere l'IP dove avviare il servizio; quindi, il service_bind_address e di default viene proposto 127.0.0.1, ma lo modifichiamo con il numero IP 192.168.50.100 (kali) perché il servizio deve avvenire tra Kali e Win7





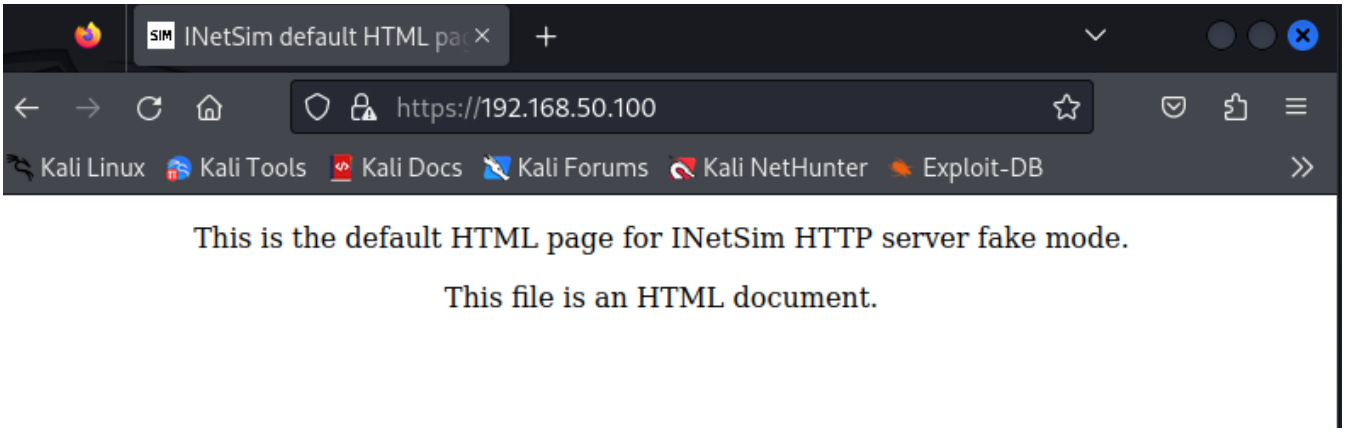
Ora, per simulare uno scenario reale, InetSim ci mette a disposizione dei **FAKE files** ovvero dei file vuoti con un'estensione che possiamo richiedere come se fossero delle risorse reali

Scriviamo sudo inetsim



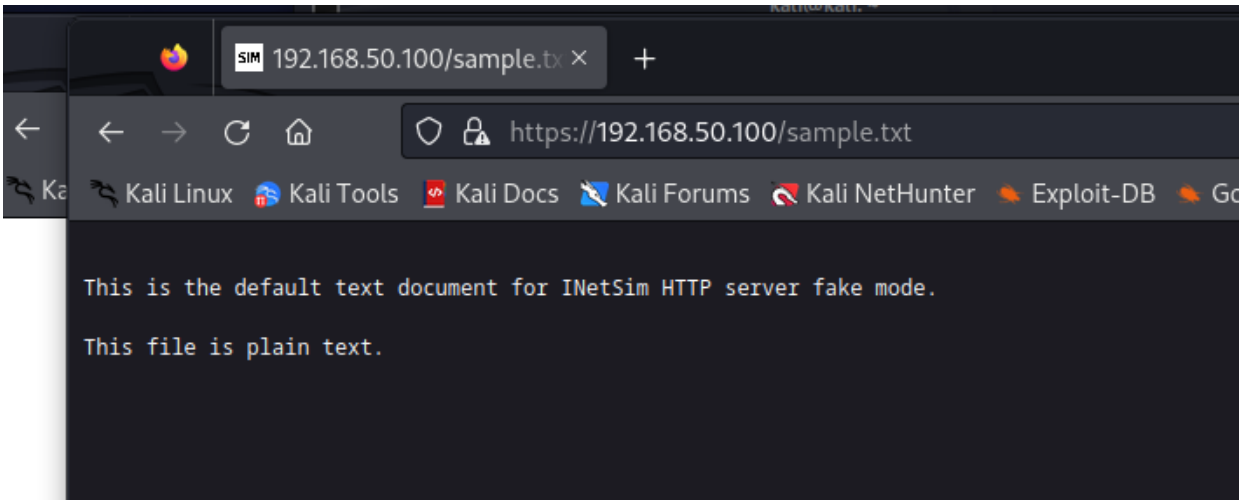
Il servizio HTTPS deve essere in ascolto sulla porta 443 del Local Host; quindi, proviamo a connetterci alla porta 443 del local host da un web browser su Kali

Andiamo su browser di kali e digitiamo HTTP://192.168.50.100 e accettiamo il WARNING di sicurezza

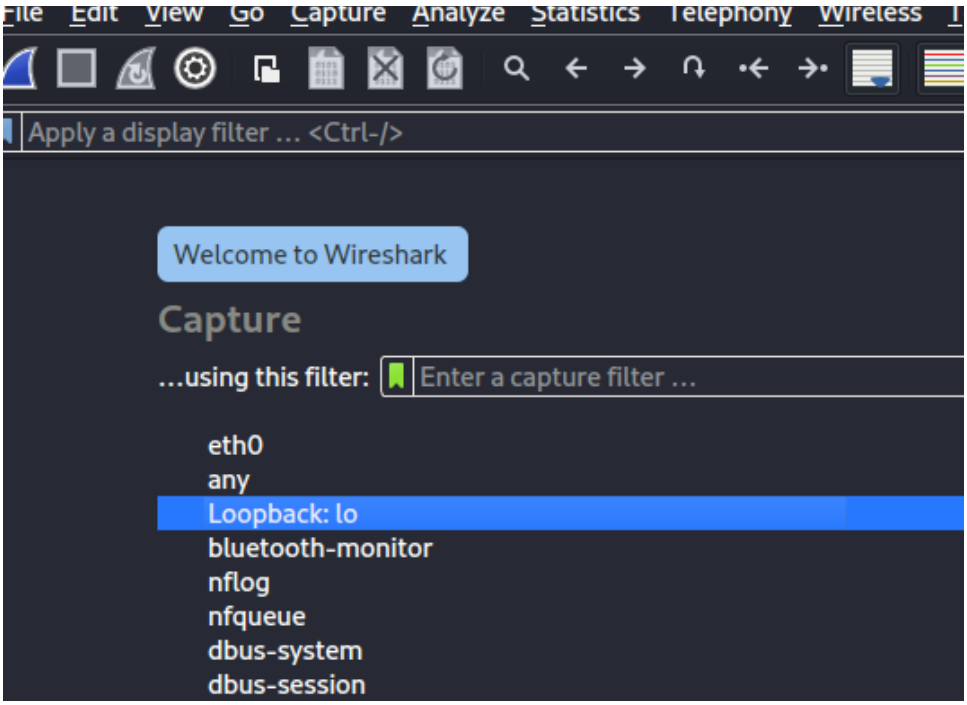


Dopodiché richiediamo

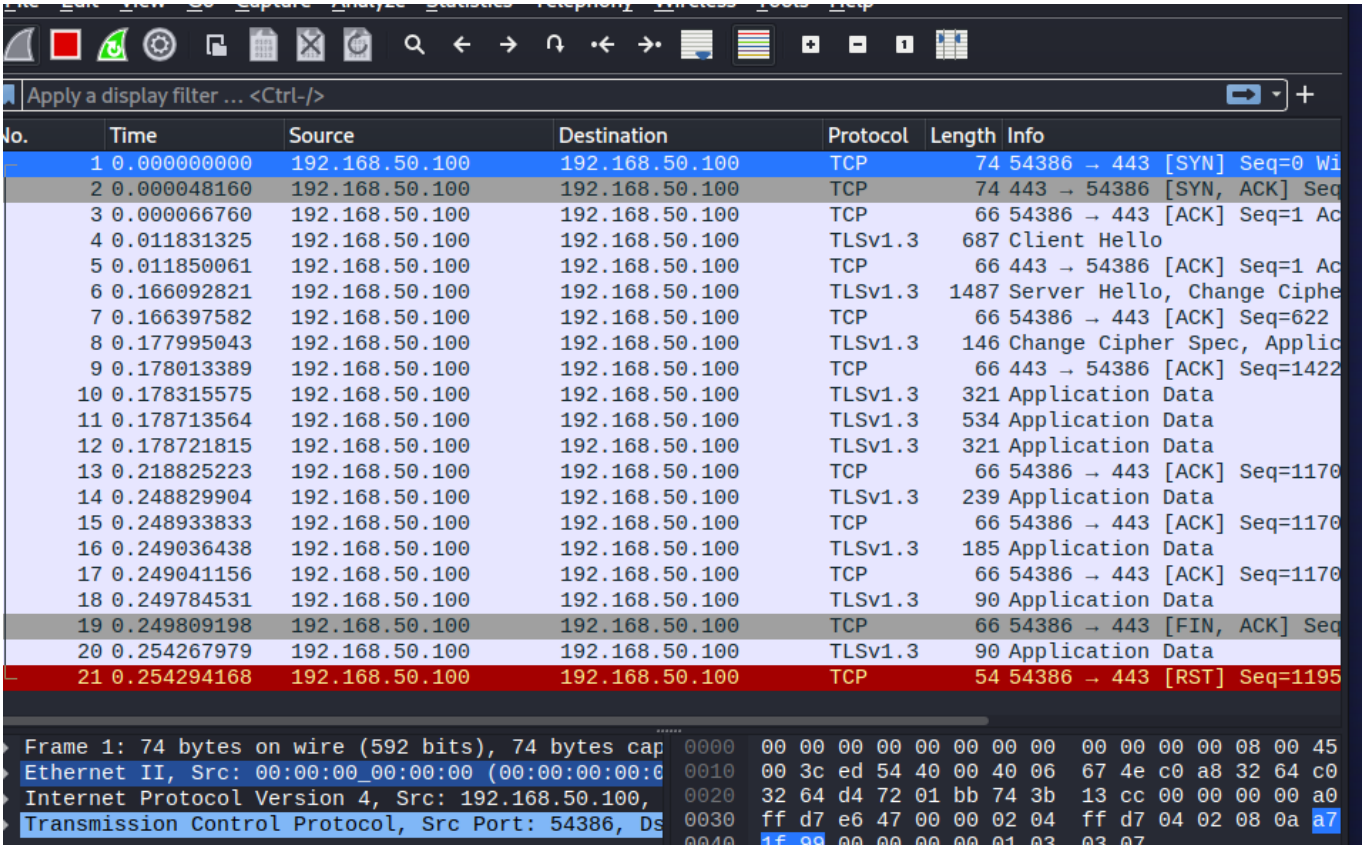
Uno dei file fittizi messi a disposizione da Inetsim andando sulla barra di ricerca del browser e digitando HTTPS://192.168.50.100/sample.txt



A questo punto avviamo WIRESHARK che si metterà in ascolto sull'interfaccia di LOOPBACK e ci connettiamo al local Host facendo una richiesta file.txt. Si analizzerà quindi la comunicazione tra le parti e noteremo come viene instaurata la sessione TCP tra le parti (la sequenza **SYN, SYN ACK, ACK**)

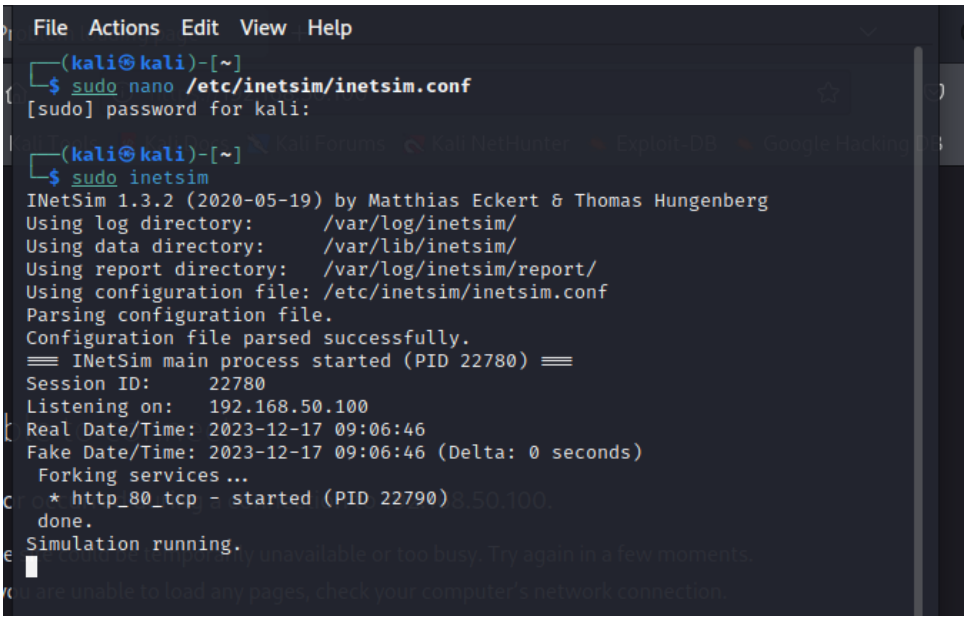


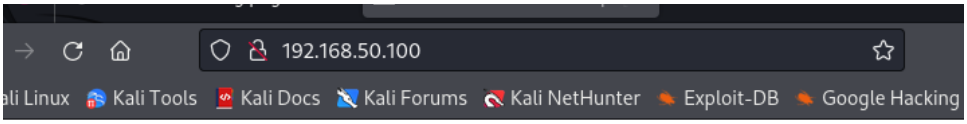
Clicco REFRESH sul browser e ottengo



Le prime 3 sequenze [SYN], [SYN ACK], [ACK] sono quelle di creazione della comunicazione.

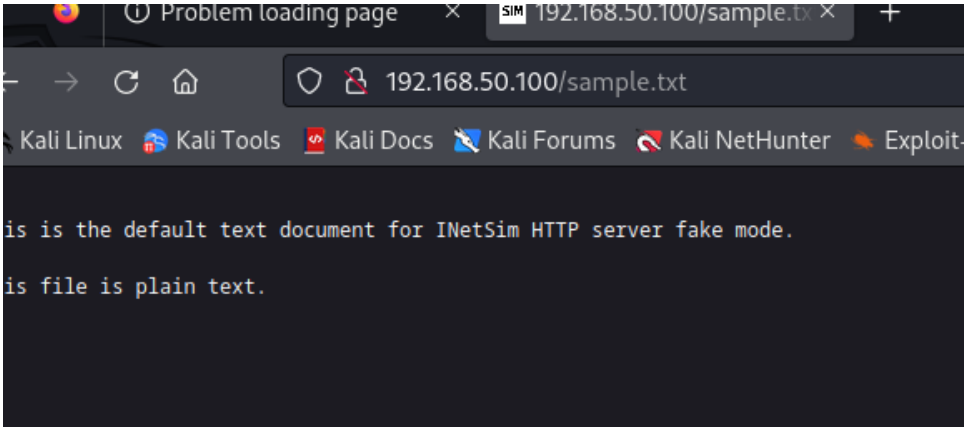
Ora effettuiamo lo stesso procedimento ma attraverso il servizio **HTTP** e la **porta 80**



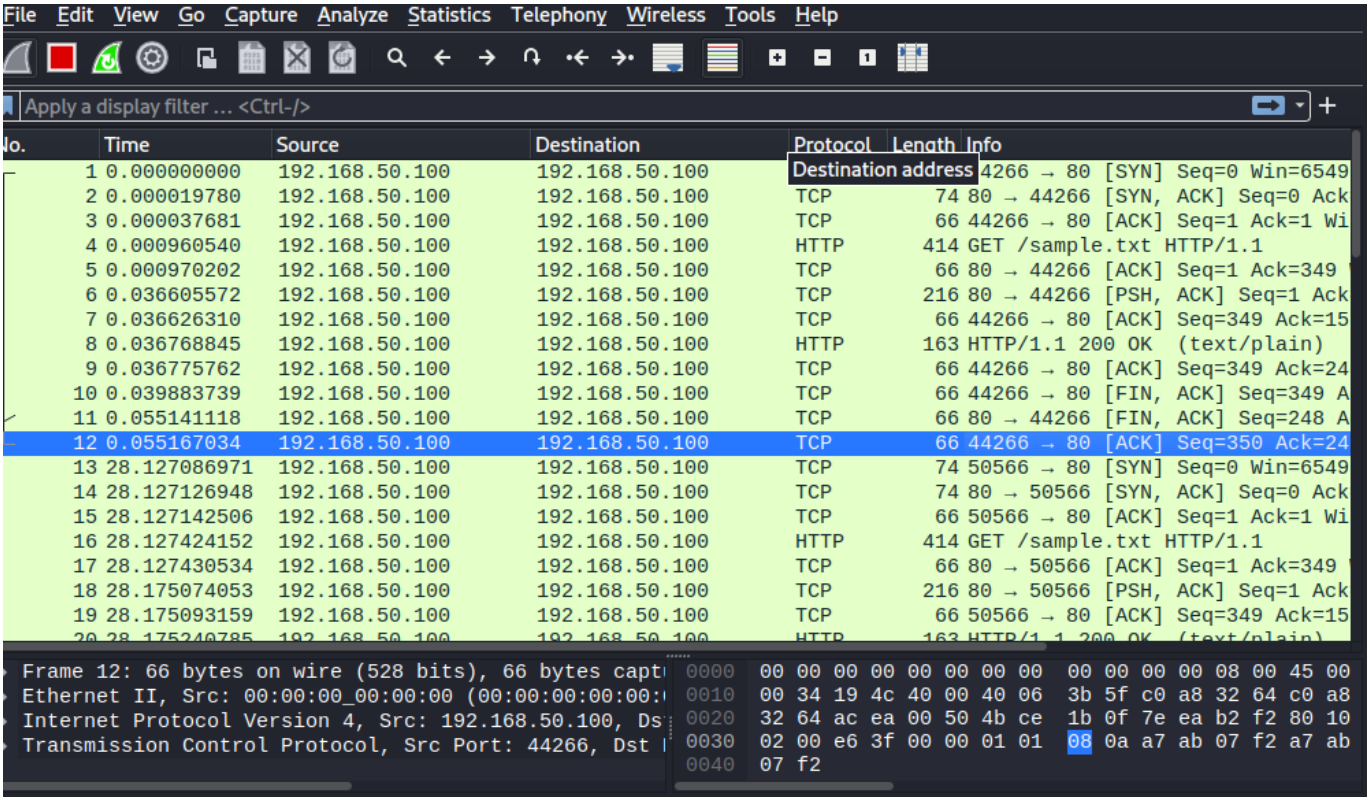


This is the default HTML page for INetSim HTTP server fake mode.

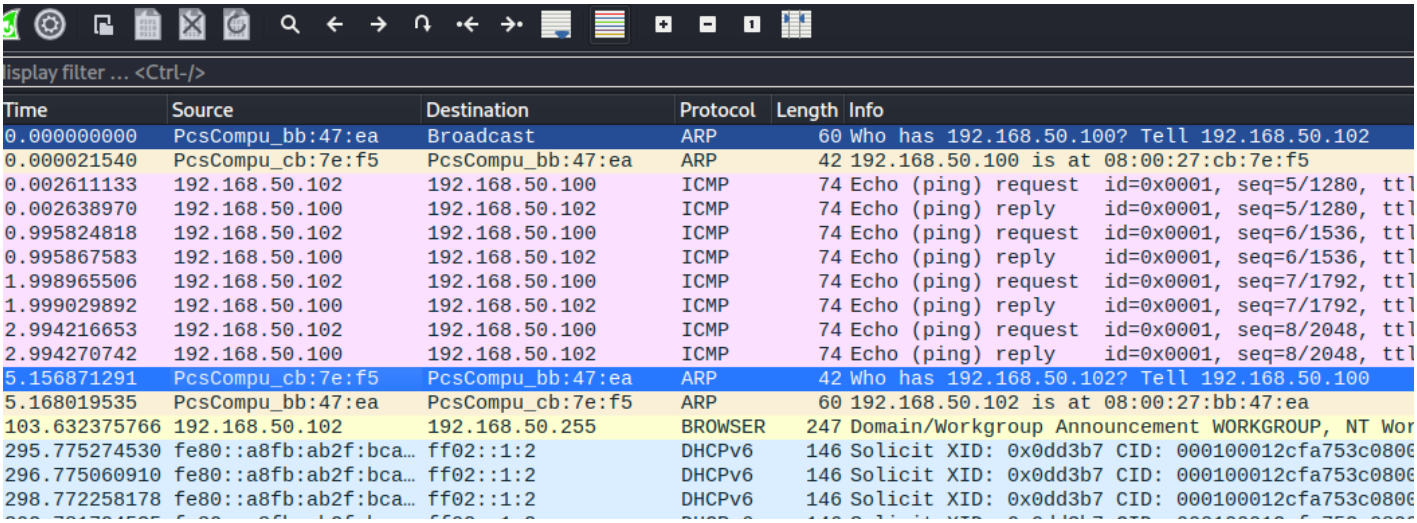
This file is an HTML document.



Sessione TCP su **HTTP**



Ora ho aperto il command su WIN7 e digitato ping 192.168.50.100 (kali) e aperto successivamente Wireshark su ETH0. È partita la richiesta ARP, le macchine pingano.



****