Simulazione architettura client-server

ERNESTO ROBLES

Dispositivi coinvolti:

Kali Linux (dns server) - IP 192.168.32.100/24
Il Dns server Kali Linux ha come servizi attivi DNS, Http e Https.

Windows pc (client) - IP 192.168.32.101/24

Software WireShark utilizza lo stesso canale di comunicazione condiviso tra più utenti consentendo di esaminare il contenuto di tutti i pacchetti dati in transito.

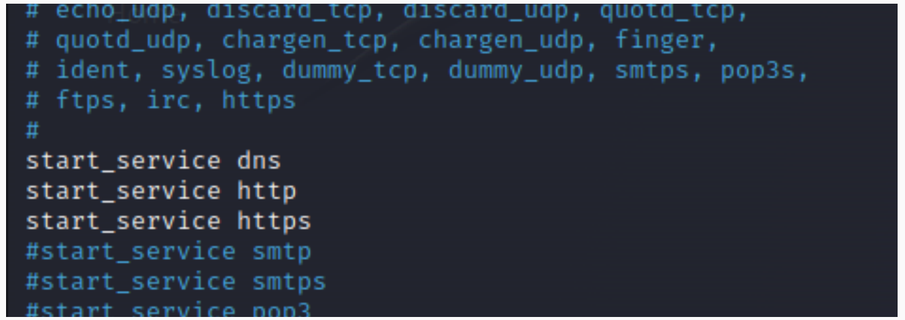
Scopo della simulazione:

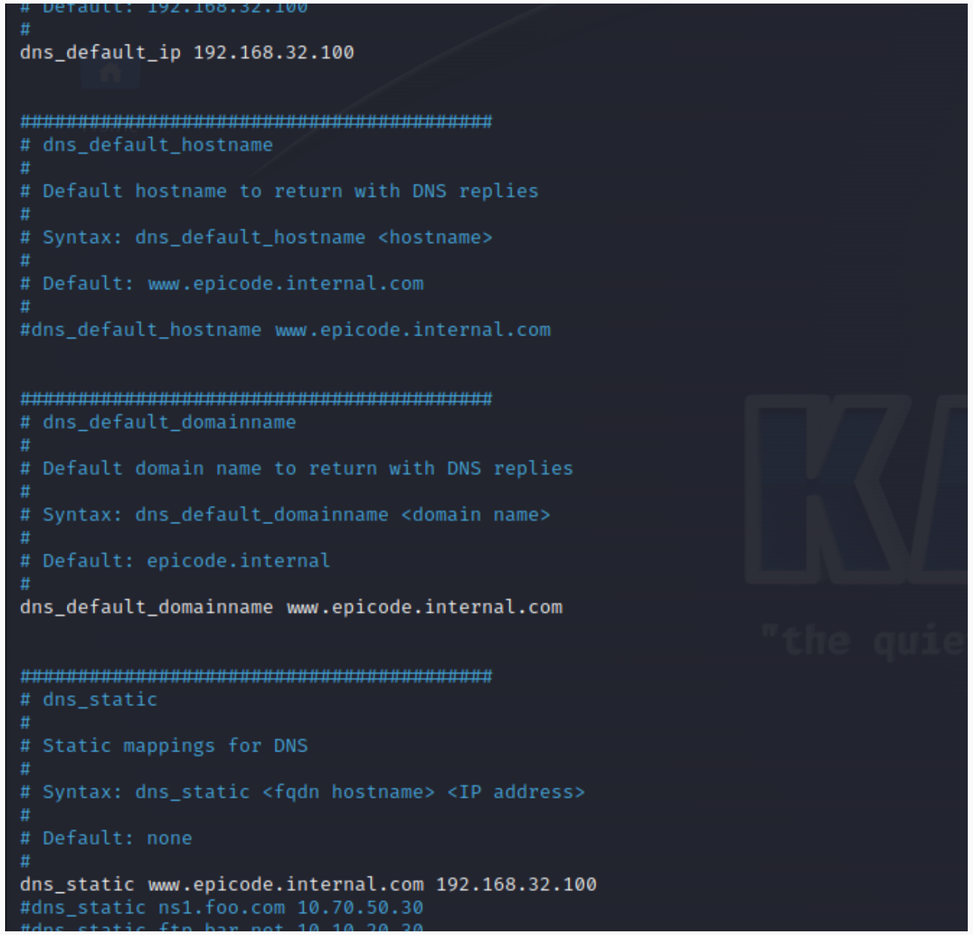
Data una richiesta di una specifico servizio internet es: sito web (www.epicode.internal.com), dal client ad un server quest'ultimo risponderà al client mediante l'uso del servizio DNS il quale associa ad un nome ovvero un dominio un indirizzo IP che risponde al servizio richiesto, in questo caso la pagina web.

LABORATORIO VM

NEL LABORATORIO VM
ATTIVIAMO ALL'INTERNO DELLA MACCHINA KALI I SERVIZI DNS, HTTP E HTTPS AVVALENDOCI DI INETSIM CHE È UN SOFTWARE CHE PERMETTE DI EMULARE SERVIZI INTERNET.

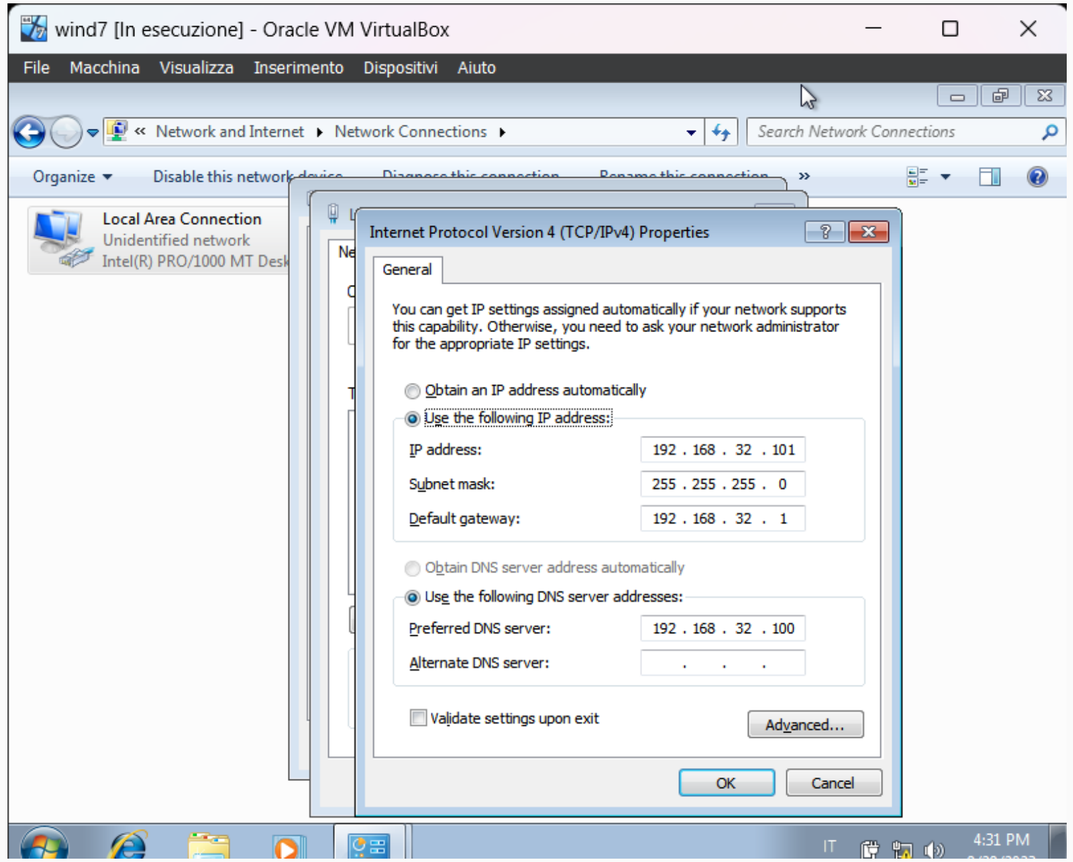
CON IL COMANDO "SUDO NANO /ETC/INETSIM/INETSIM.CONF"
ACCEDIAMO ALL'INTERFACCIA DEI SERVIZI NELLA QUALE ATTIVIAMO I SERVIZI DESIDERATI SOPRACITATI
NELLE IMPOSTAZIONI DEL SERVIZIO DNS
MODIFICHIAMO LE VOCI:
DNS DEFAULTIP INSERENDO 192.168.32.100
DNS DEFAULT INSERENDONAME WWW.EPICODE.INTERNAL
DNS STATIC INSERENDO WWW.EPICODE.INTERNAL.COM 192.162.32.100





LABORATORIO VM

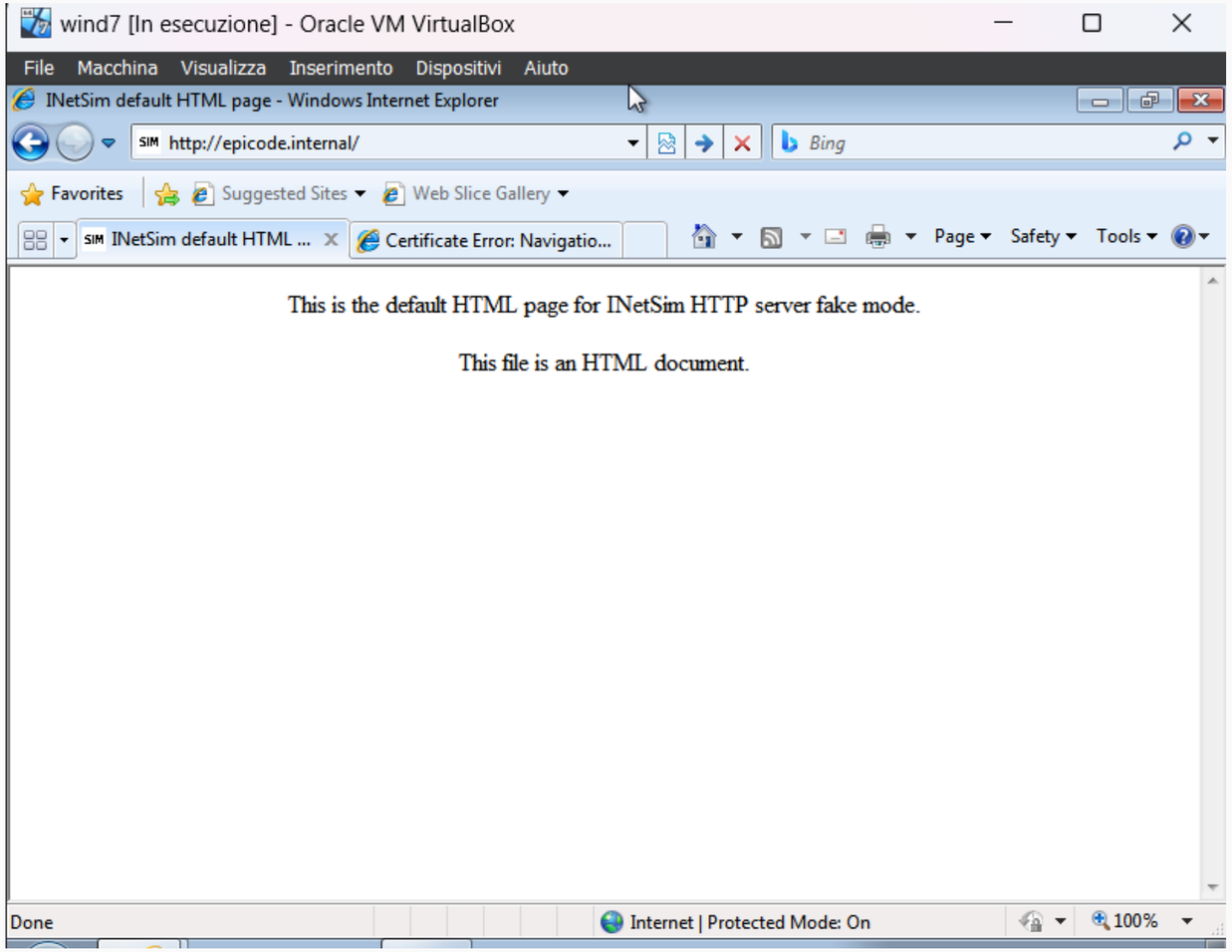
INSERIAMO ALL'INTERNO DELLA MACCHINA WINDOWS L'IP DNS 192.168.32.100 IL QUALE CORRISPONDE AL SERVER DNS KALI



LABORATORIO VM

UNA VOLTA AVVIATO IL SERVIZIO INETSIM NELLA MACCHINA KALI TRAMITE IL COMANDO “SUDO INETSIM”

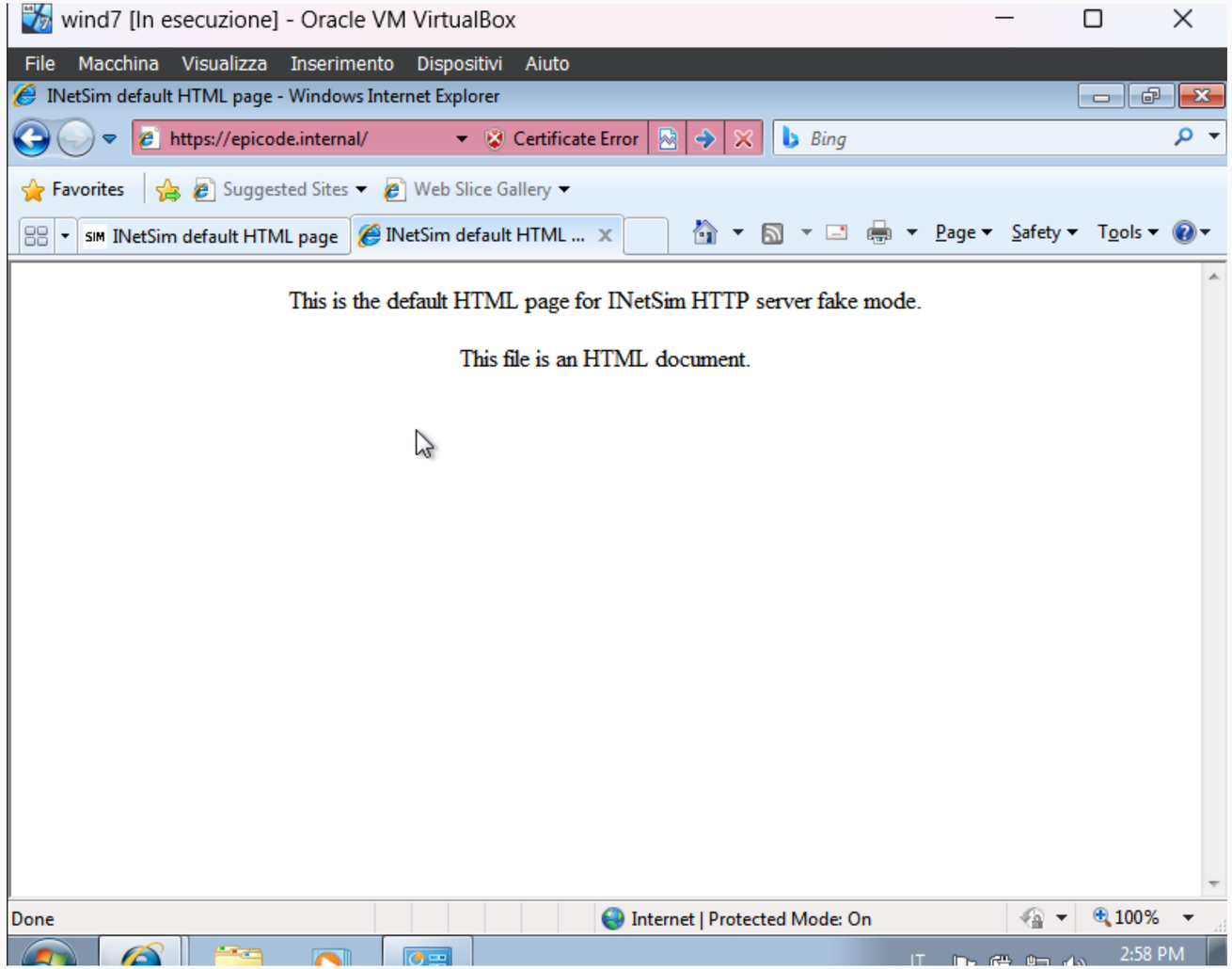
AVVALENDOCI DEL BROWSER DELLA MACCHINA WINDOWS CERCHIAMO IL SITO D’INTERESSE INSERENDO IL SUO DOMINIO NELLA BARRA DELL’URL TRAMITE UNA RICHIESTA HTTP, VISUALIZZANDO COSÌ LA RISPOSTA DEL DNS SERVER.



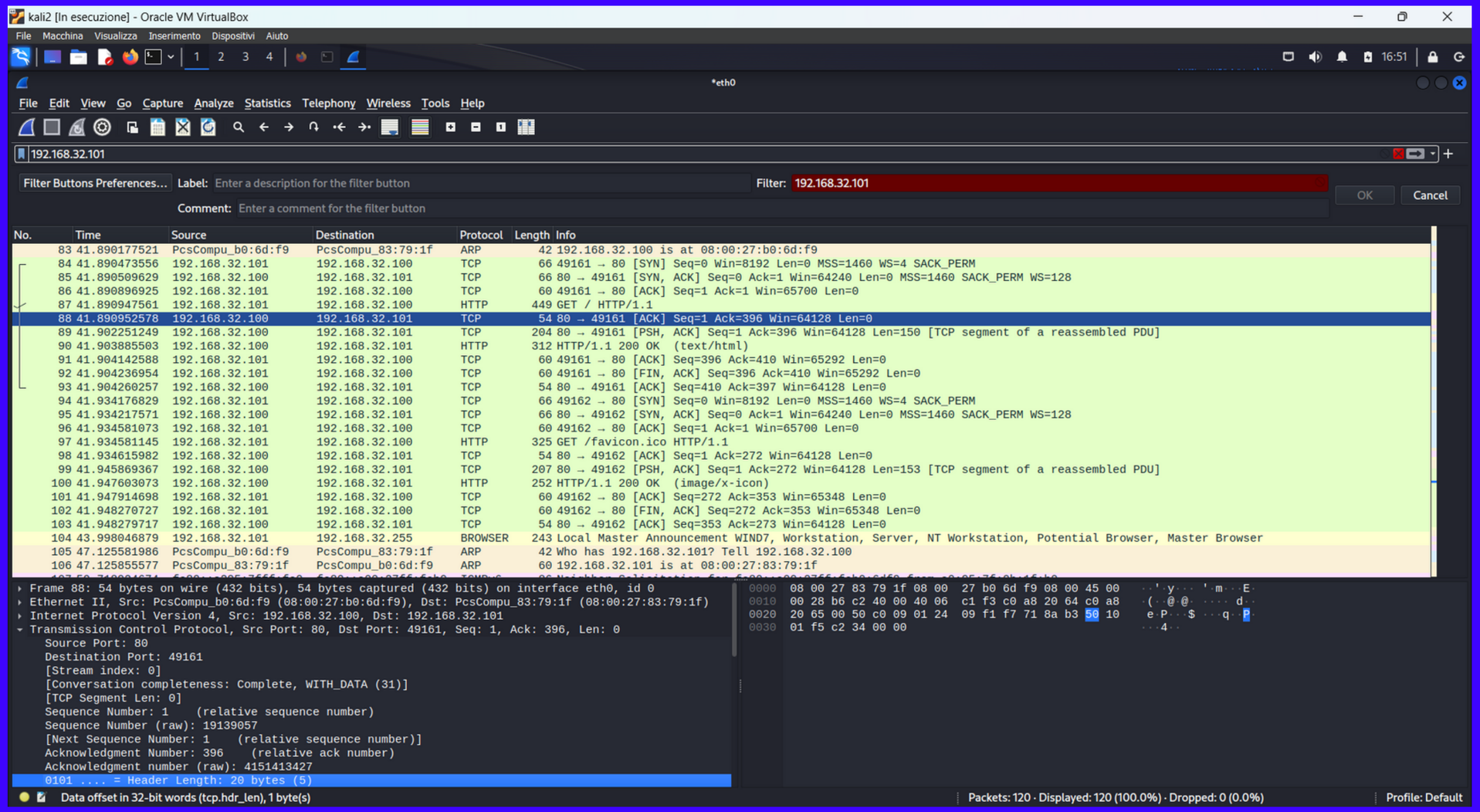
LABORATORIO VM

UNA VOLTA AVVIATO IL SERVIZIO INETSIM NELLA MACCHINA KALI TRAMITE IL COMANDO “SUDO INETSIM”

AVVALENDOCI DEL BROWSER DELLA MACCHINA WINDOWS CERCHIAMO IL SITO D’INTERESSE INSERENDO IL SUO DOMINIO NELLA BARRA DELL’URL TRAMITE UNA RICHIESTA HTTPS, VISUALIZZANDO COSÌ LA RISPOSTA DEL DNS SERVER



TRAMITE L'USO DI WIRESHARK
SI EVIDENZIA COME CON IL SOLO HTTP SI EFFETTUA SOLO LA CONESSIONE POICHE' TCP/ DI INTERNET NON PREVEDE FUNZIONALITÀ DI SICUREZZA ALL'USO PRINCIPALE DELLA RETE



TRAMITE L'USO DI WIRESHARK
MENTRE L'USO DI HTTPS PERMETTE UNA COMUNICAZIONE SICURA DALLA SORGENTE AL DESTINATARIO (END-TO-END) FORNENDO AUTENTICAZIONE, CONFIDENZIALITÀ E INTEGRITÀ DEI DATI POICHÈ LAVORA AL DI SOPRA DEL LIVELLO DI TRASPORTO