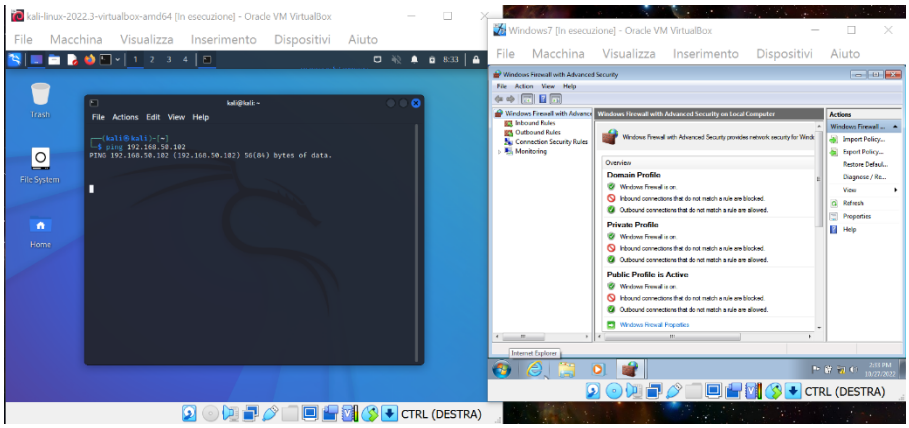
CONFIGURAZIONE POLICY SU FIREWALL WINDOWS

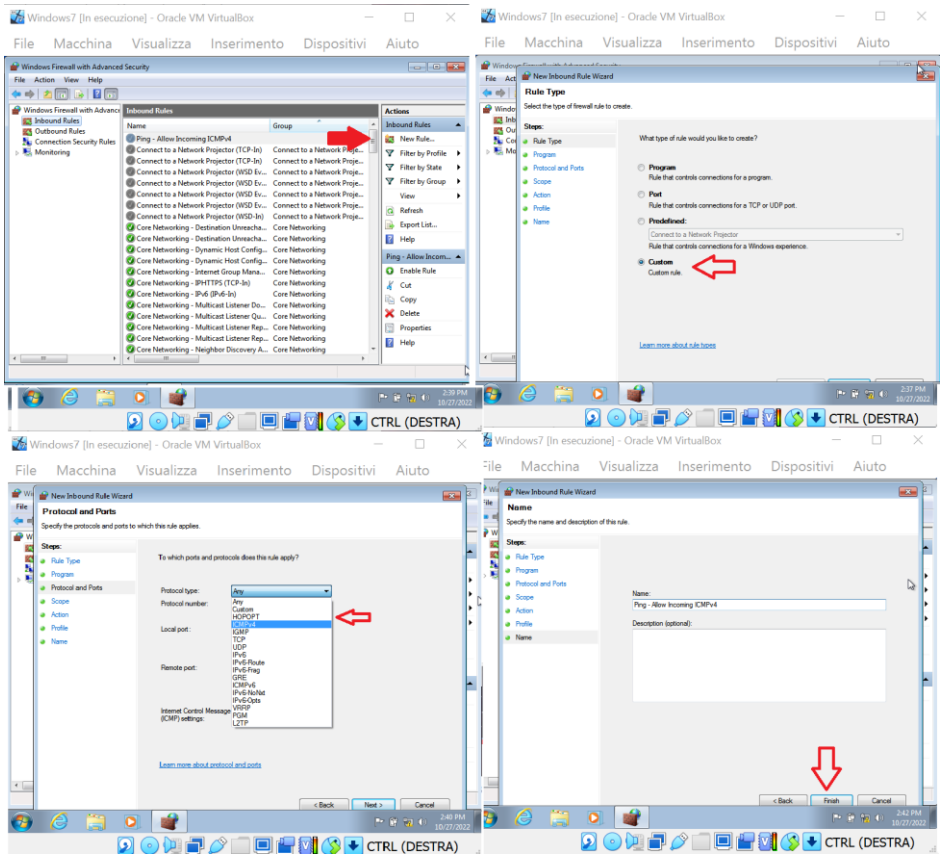
Nella prima parte dell'esercizio si dovrà configurare la policy sul Windows Firewall per permettere il ping dalla macchina Linux Kali alla macchina Windows in VirtualBox.

Con il Firewall Windows attivo e senza la policy configurata non sarà possibile pingare le due macchine:



come si può vedere dal terminal di Kali inserendo il comando del ping con IP della macchina Windows non è possibile pingare.

Sarà dunque necessario modificare la policy del Firewall per permettere il ping di ICMPv4 seguendo i passaggi illustrati in figura:



Sarà necessario aggiungere una nuova regola di policy su "New Rule";

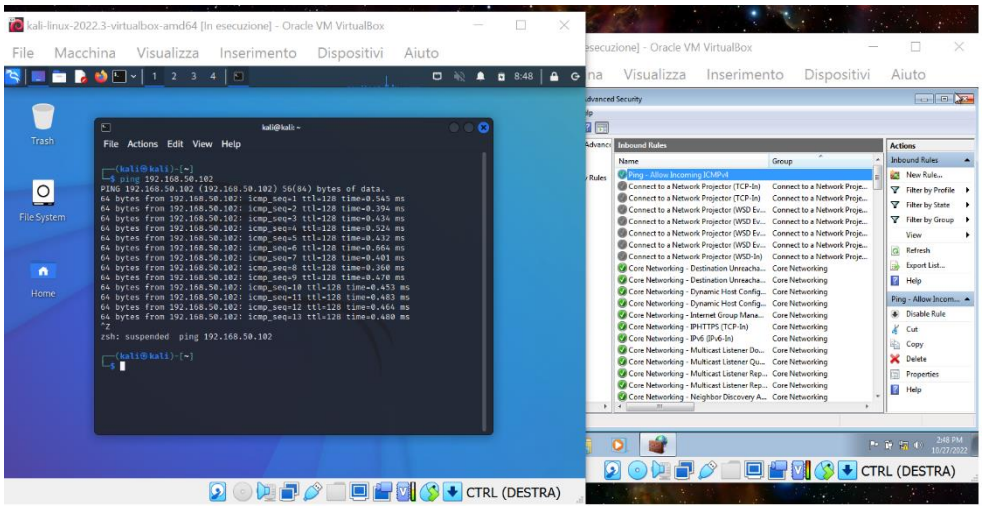
clickeremo su "Custom rule";

abiliteremo il protocollo per le ICMPv4;

andremo avanti fino alla denominazione della nuova regola di policy per poi clickare su "Finish".

Ora il nostro Firewall (attivo) avrà il permesso per far pingare le due macchine virtuali.

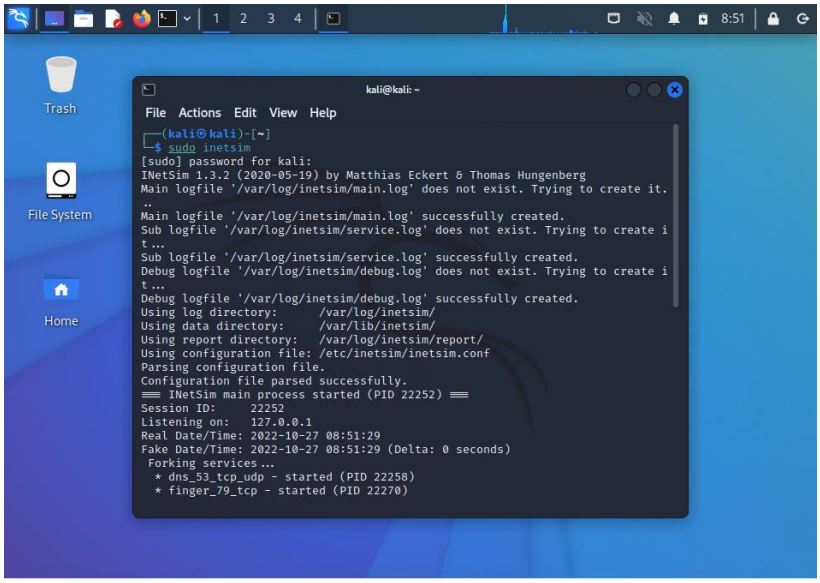
Come prova andremo a fare la prova di ping tra le due macchine per avere conferma dell'effettivo funzionamento della nuova policy del Firewall Windows:



Come possiamo vedere a destra nella schermata del Firewall di Windows abbiamo abilitato la nuova policy e dalla foto di sinistra possiamo vedere che effettivamente le macchine stanno pingando tra loro.

UTILIZZO DELL'UTILITY InetSim E CATTURA DI PACCHETTI CON WIRESHARK

Per l'utilizzo dell'utility pre-installato InetSim per l'emulazione di servizi Internet dovremo aprire il terminal di Kali per poi inserire il comando sudo inetsim:

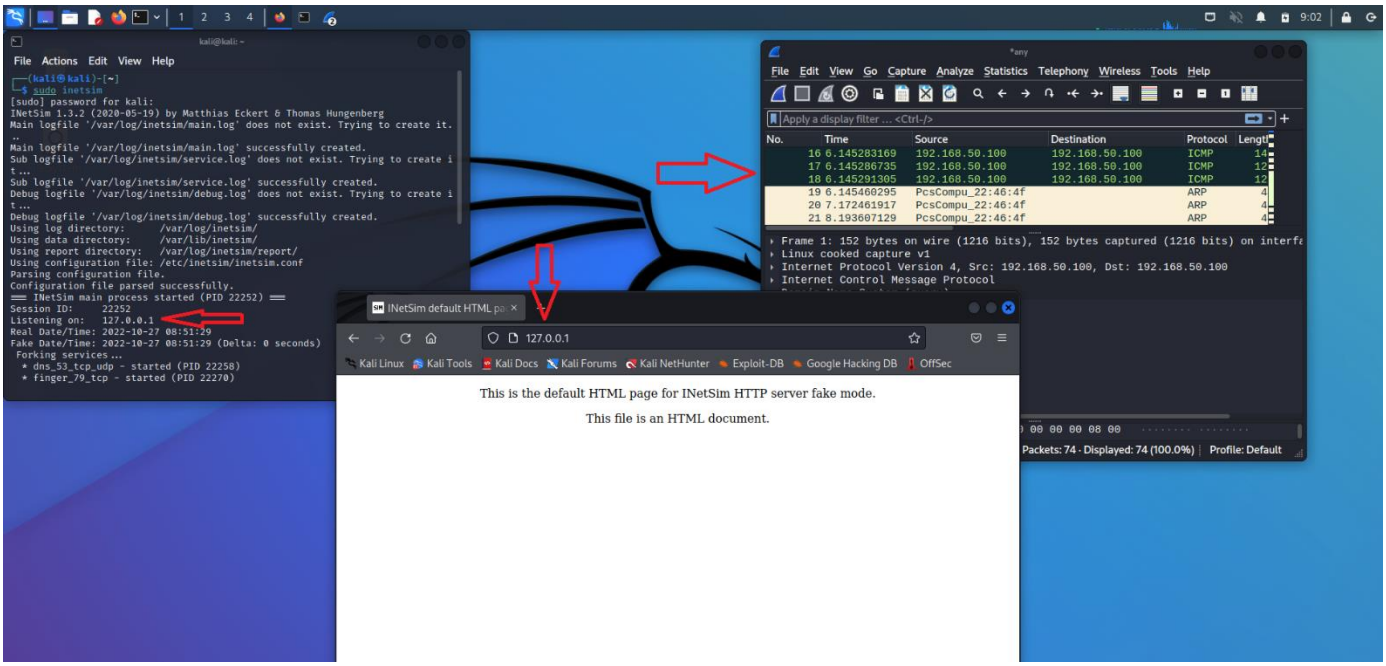


avremo così attivato un server con inetsim come possiamo vedere dalla figura qui a fianco

Ora non ci resterà che andare a vedere l'IP generato dal nostro InetSim per la connessione ad internet;

Aprire Mozzilla dalla macchina Kali ed inserirlo
Aprendo ora l'applicazione Wireshark potremo catturare l'invio di pacchetti ICMP.

Possiamo vedere i tre passaggi nell'immagine qui sotto:



Aprendo l'applicazione Wireshark andremo a clickare su "Loopback:lo" applicheremo il nostro filtro "tcp" e daremo l'avvio alla cattura.

Avremo così una packet capture con Wireshark che evidenzierà il passaggio dei pacchetti tcp.