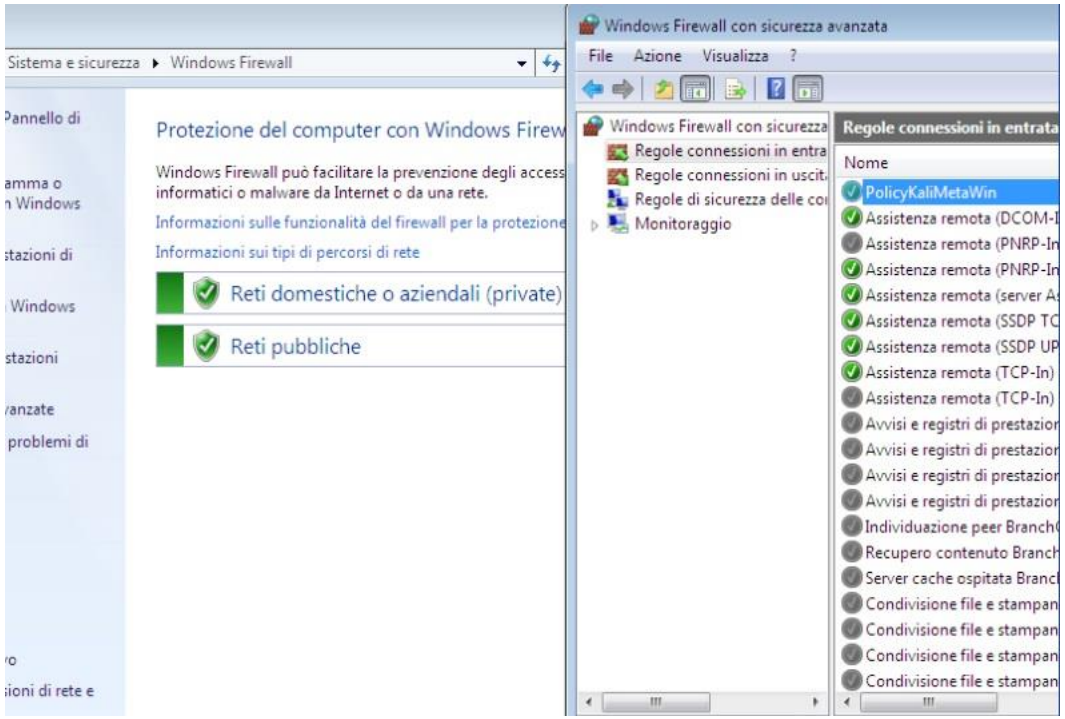
Configurazione Policy per Ping da Linux a Windows 7

Utilizzo dell'utility INetSim per simulazione di servizi Internet

Cattura dei pacchetti tramite WireShark

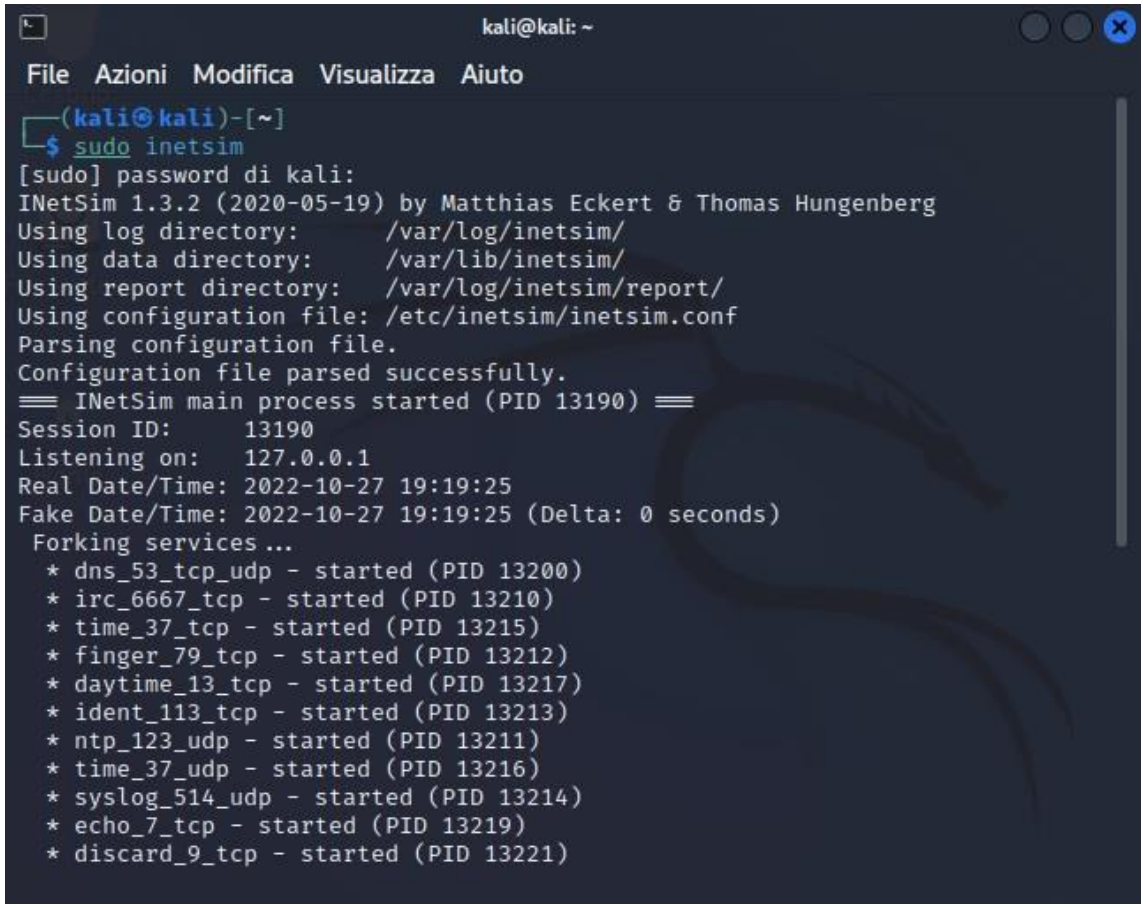
Orlando Tangari

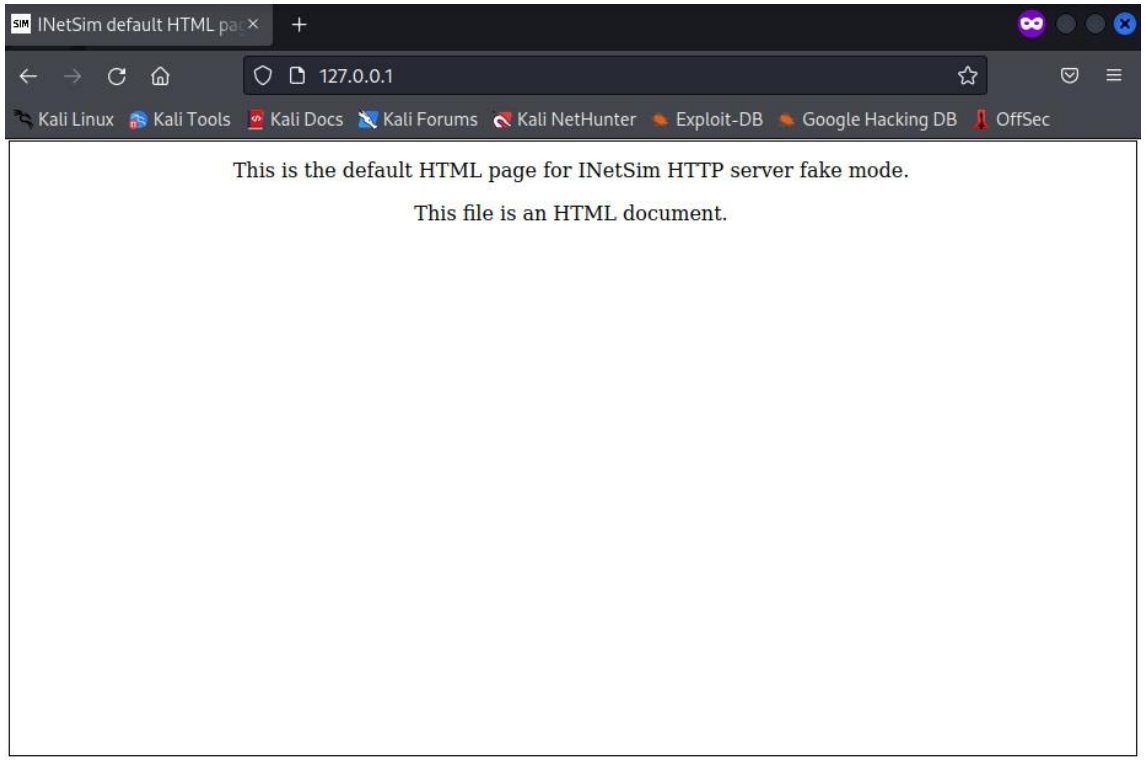



```
metasploitable login: msfadmin
Password:
Last login: Thu Oct 27 15:34:29 EDT 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=10.9 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.922 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.901 ms

--- 192.168.50.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.901/4.255/10.943/4.729 ms
msfadmin@metasploitable:~$
```

Configurazione Policy Windows Firewall

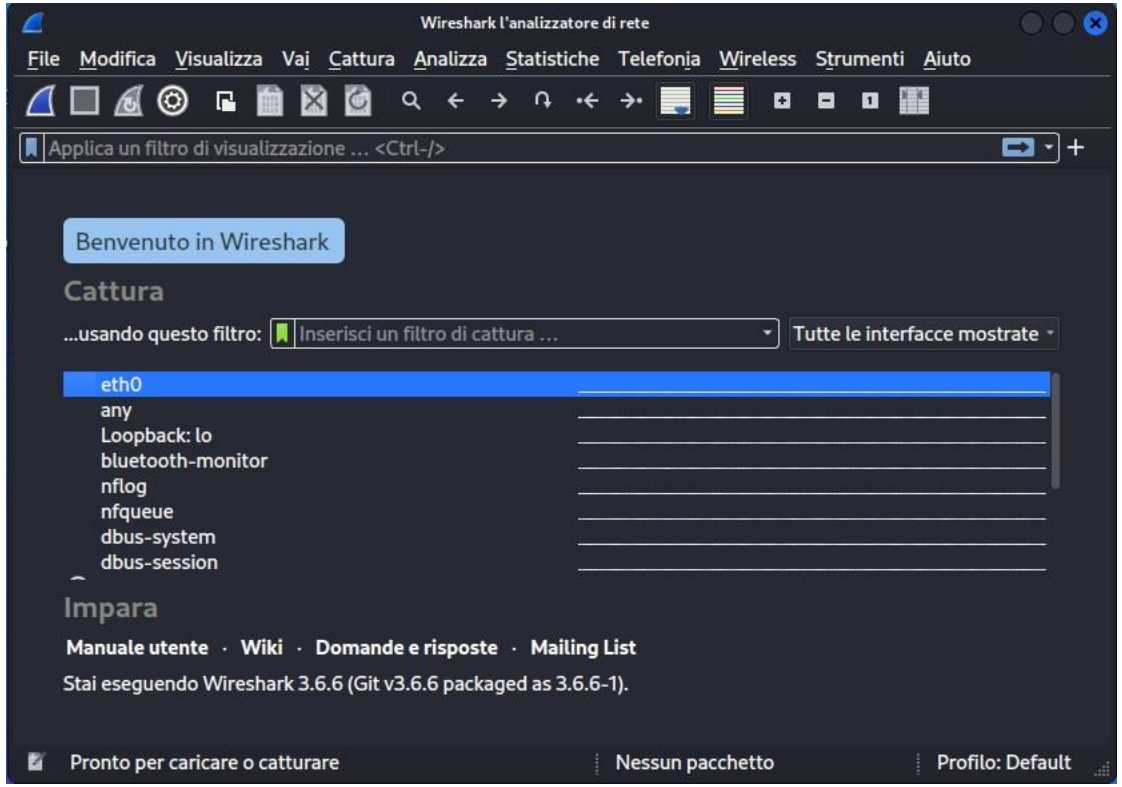
Tramite le impostazioni avanzate del Windows Firewall si crea: una nuova regola per tutti i programmi, con protocollo ICMPv4, agli indirizzi IP 192.168.50.100 (Kali Linux) e 192.168.50.101 (Meta), per effettuare il *ping* da macchine Linux a macchina Windows (192.168.50.102) avendo il firewall attivo.

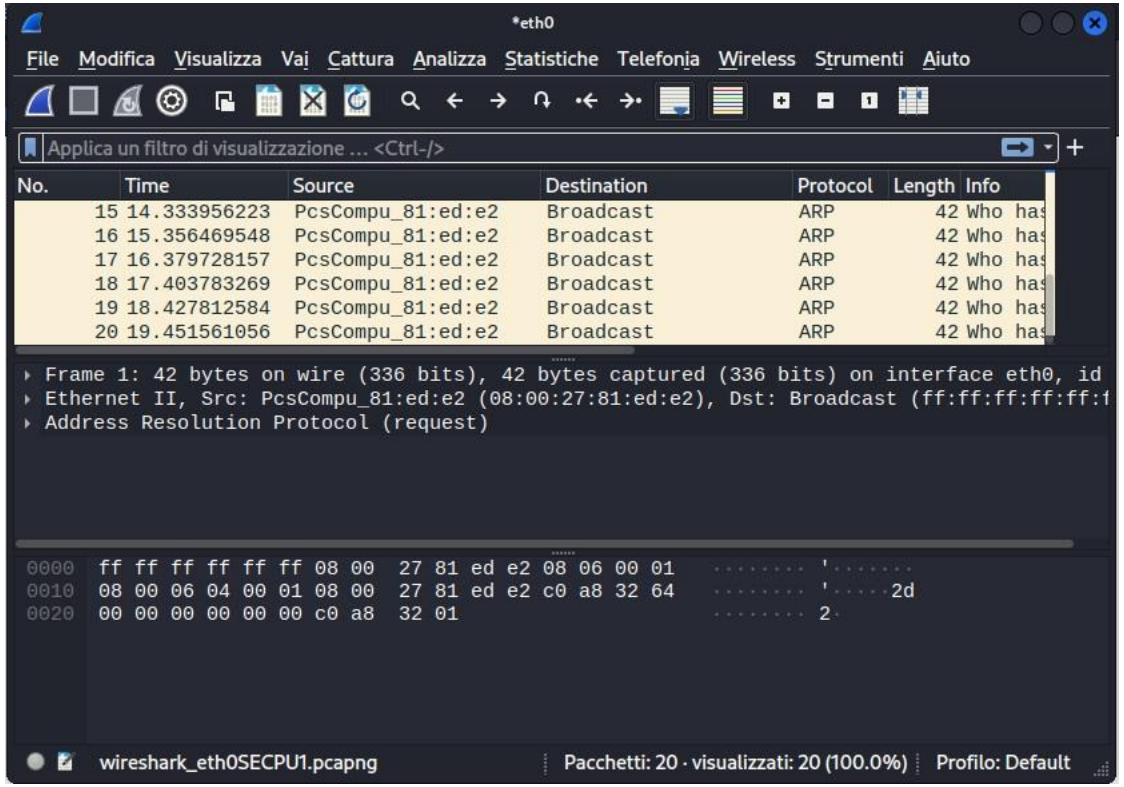




Simulazione di una navigazione sul Web tramite INetSim

Attraverso il terminale di Kali Linux, si digita il comando, con privilegi di amministratore, *sudo inetsim*, per avviare il software di simulazione web INetSim ed il suo relativo server HTTP.
Tramite il browser Firefox, si accede alla pagina di INetSim con l'indirizzo *127.0.0.1* .





Cattura dei pacchetti tramite WireShark

Attraverso WireShark, software per analisi di protocollo o packet sniffer, si catturano e analizzano i pacchetti dell'interfaccia(NIC) *eth0.*

A cattura effettuata, si possono analizzare pacchetti con diversi protocolli, tra cui *ARP*, utilizzati per associare un indirizzo MAC a un indirizzo IP di un host su una LAN.