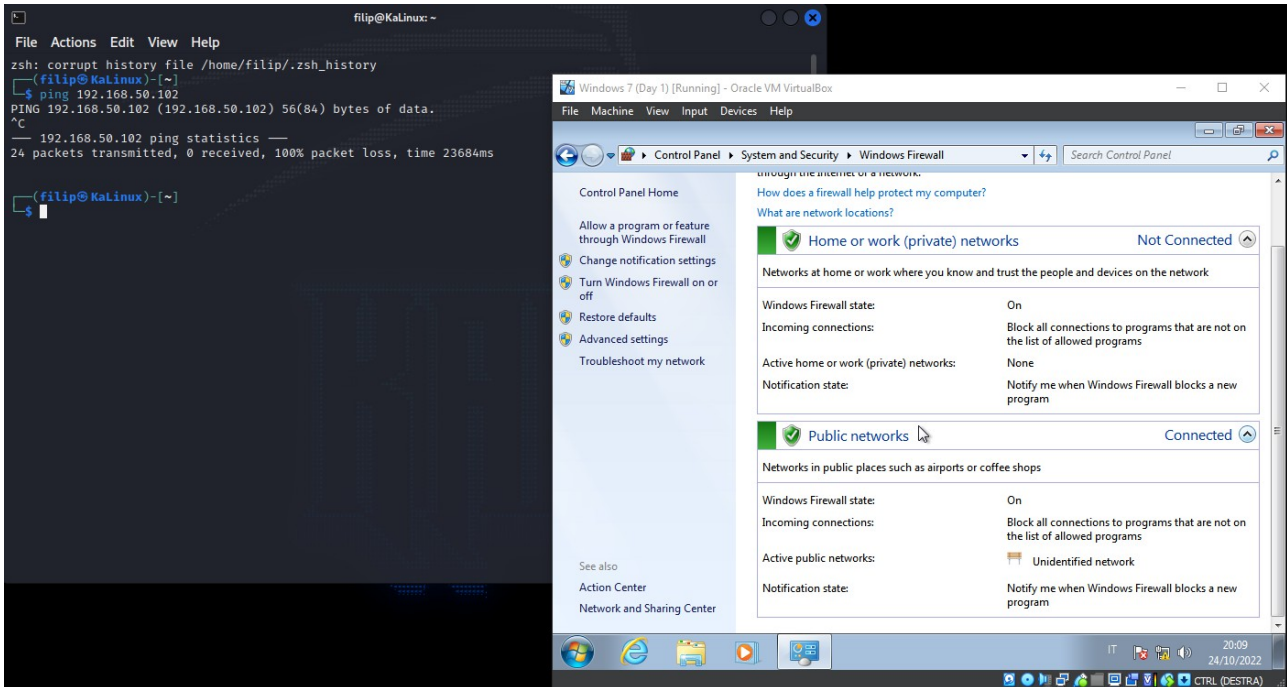


## Report:

Oggi useremo il laboratorio virtuale con Oracle VM VirtualBox per configurare il firewall della MV Windows 7 a permettere

Se il Windows 7 ha il firewall attivo e in esecuzione, la nostra richiesta ping inviata dal Kali Linux sarà Drop, ovvero il firewall scarta il pacchetto senza inviare nessun messaggio diagnostico al Kali come rappresentato in immagine:

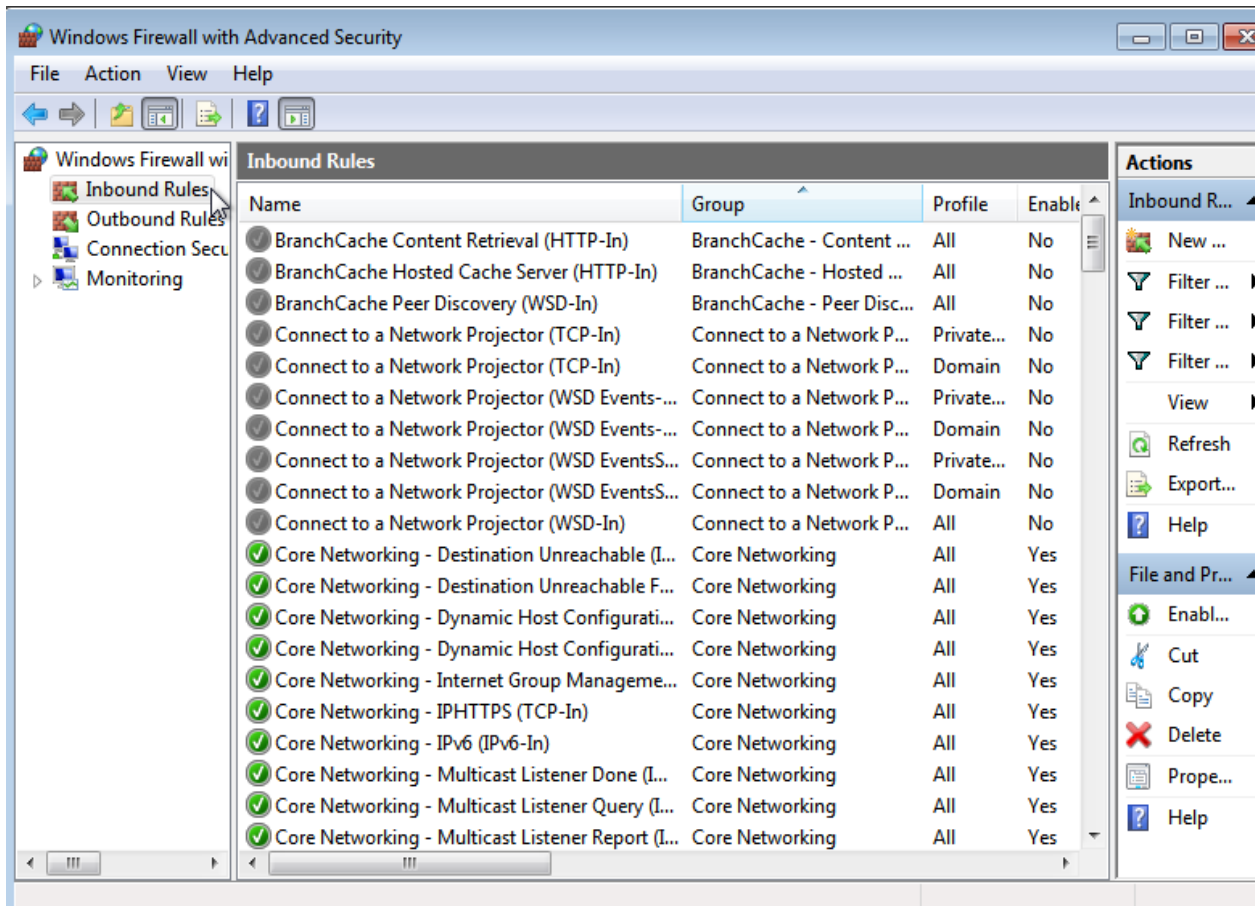


Possiamo vedere che il Kali ha inviato i 24 pacchetti di richieste senza ricevere una risposta, quindi abbiamo la perdita del 100% dei pacchetti e l'ultimo abbiamo il tempo in quanto è stata eseguita la richiesta.

```
(filip@KaliLinux)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
^C  
— 192.168.50.102 ping statistics —  
24 packets transmitted, 0 received, 100% packet loss, time 23684ms
```

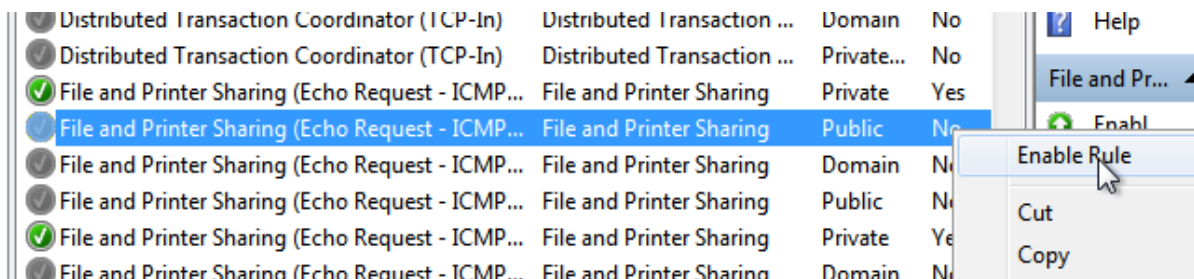
Per abilitare il passaggio dei pacchetti ICMP attraverso il Win7 firewall, dobbiamo:

1. Aprire il Start (hotkey Windows),
2. System and Security,
3. Windows Firewall,
4. Advanced Settings (nella barra di sinistra),
5. Inbound Rules (nella barra di sinistra)



Qui bisogna cercare:

Nome: File and Printer (Echo Request – ICMPv4-In)  
 Group: File and Printer Sharing  
 Profile: Public  
 Enabled: No > YES



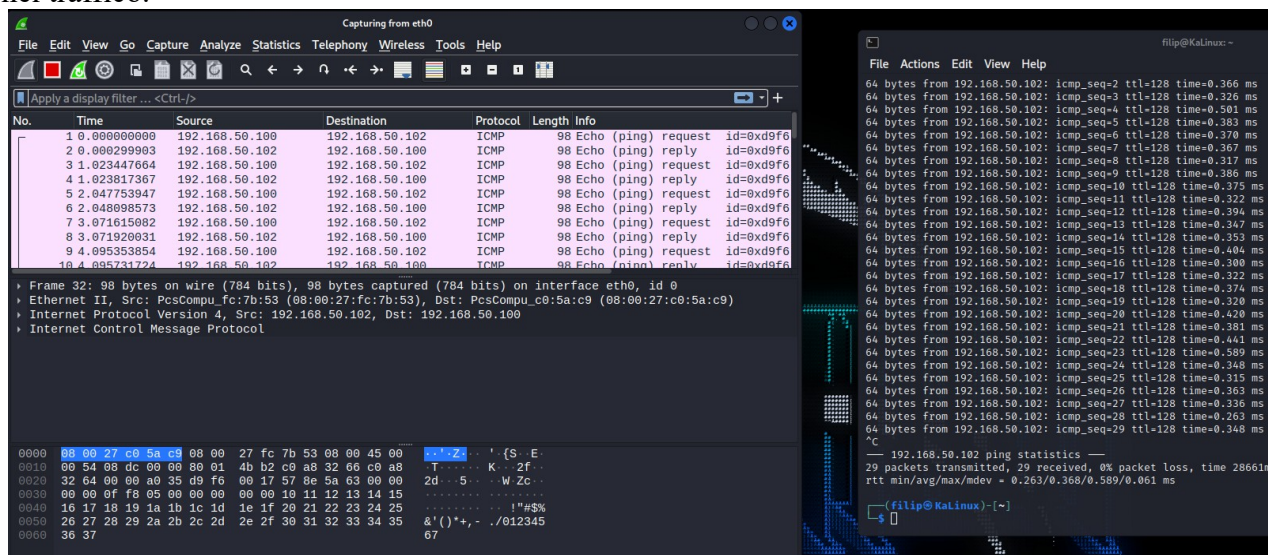
Dopo aver abilitato questa "Rule" (Regola) possiamo tornare al Kali dove possiamo provare a dare il comando -ping al IP del Win7 e ci uscirà questo risultato:

```
File Actions Edit View Help

(filip@KaliLinux)-[~]
$ 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=0.666 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.326 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.321 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.337 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.367 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.365 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.357 ms
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=0.322 ms
^C
— 192.168.50.102 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7159ms
rtt min/avg/max/mdev = 0.321/0.382/0.666/0.108 ms

(filip@KaliLinux)-[~]
```

Possiamo notare che questa volta 8 pacchetti sono inviati, 8 ricevuti, 0% persi e il tempo. A questo punto possiamo avviare il Wireshark sul Kali, che ci permetterà di analizzare i pacchetti nel traffico.

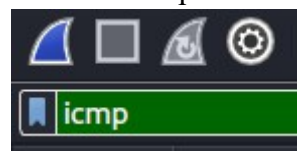
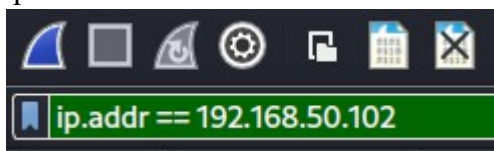


In questo caso non è un problema, però usando il Wireshard mentre si è connessi Online, potrebbe essere difficile da traciare i pacchetti. Per questo si può usare il filter, inserendo:

"ip.addr == >IP<"

oppure

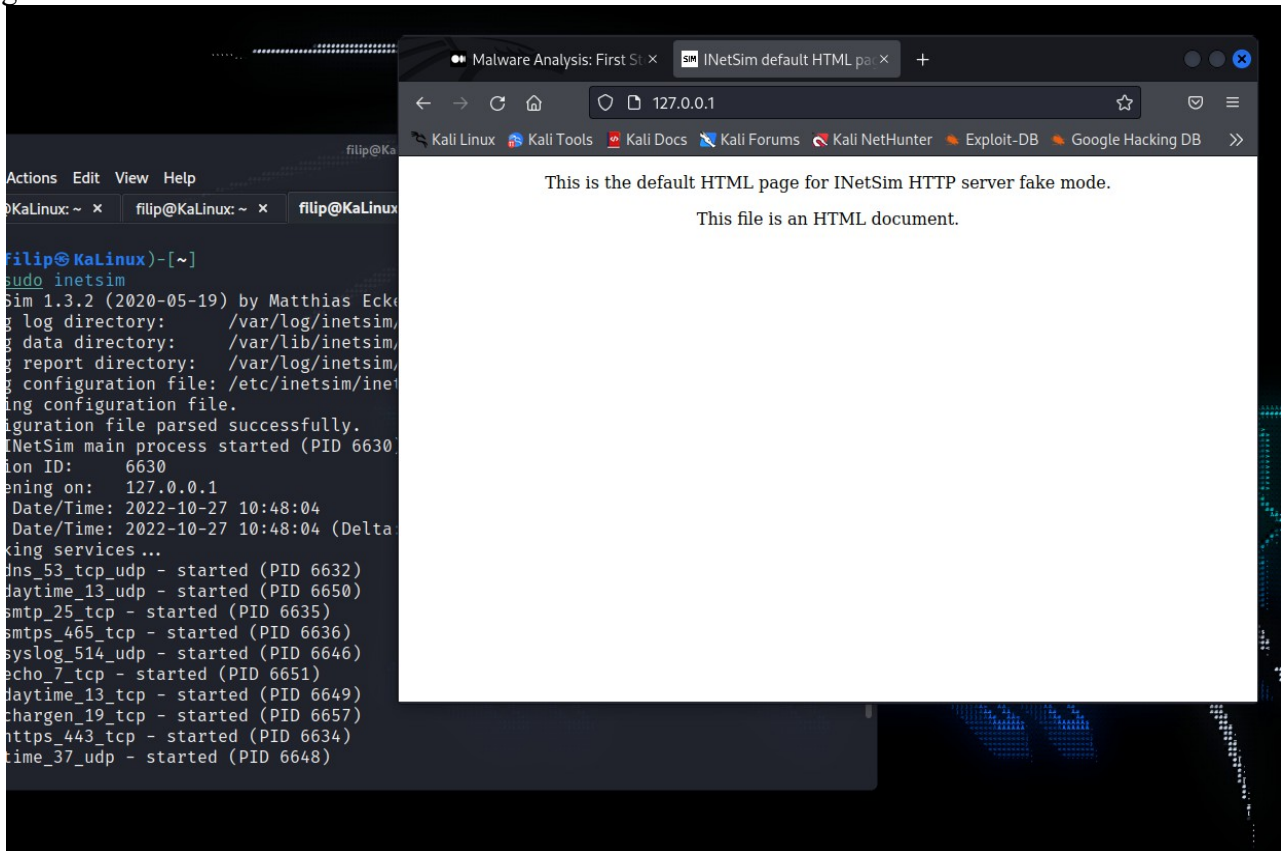
"icmp"



Usando il "Filter" sarà molto più semplice monitorare i pacchetti.



Sul Terminal scriviamo "sudo inetsim" per avviare il tool InetSim, le impostazioni default sono già impostate, quindi possiamo aprire il Firefox e scrivere IP "127.0.0.1", dovrebbe darci una pagina del genere:



Tornando sul terminal abbiamo le informazioni dove si trovano i "log file"

27/10/2022

Filip S.