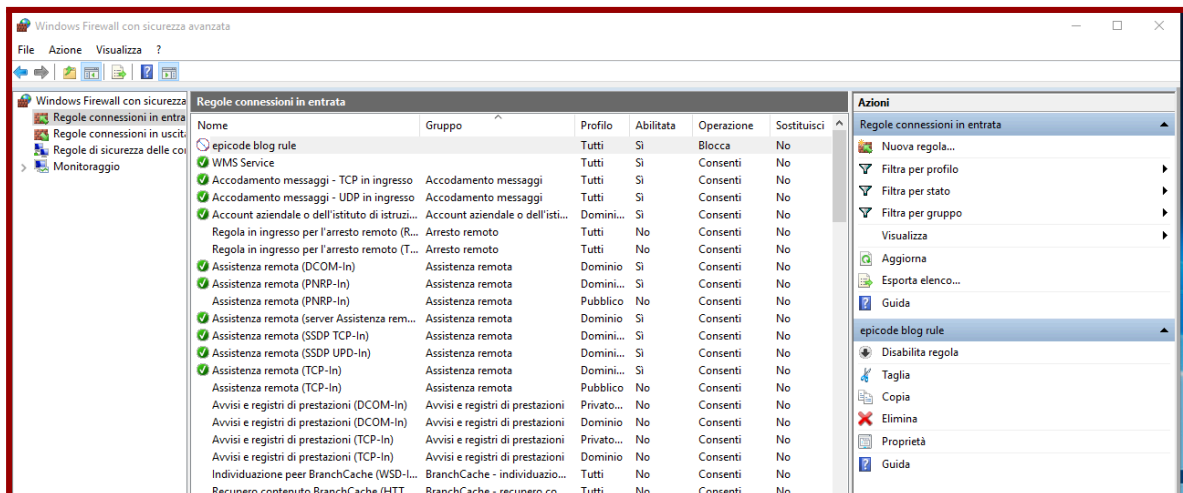


# RISOLUZIONE ESERCIZI W3D4

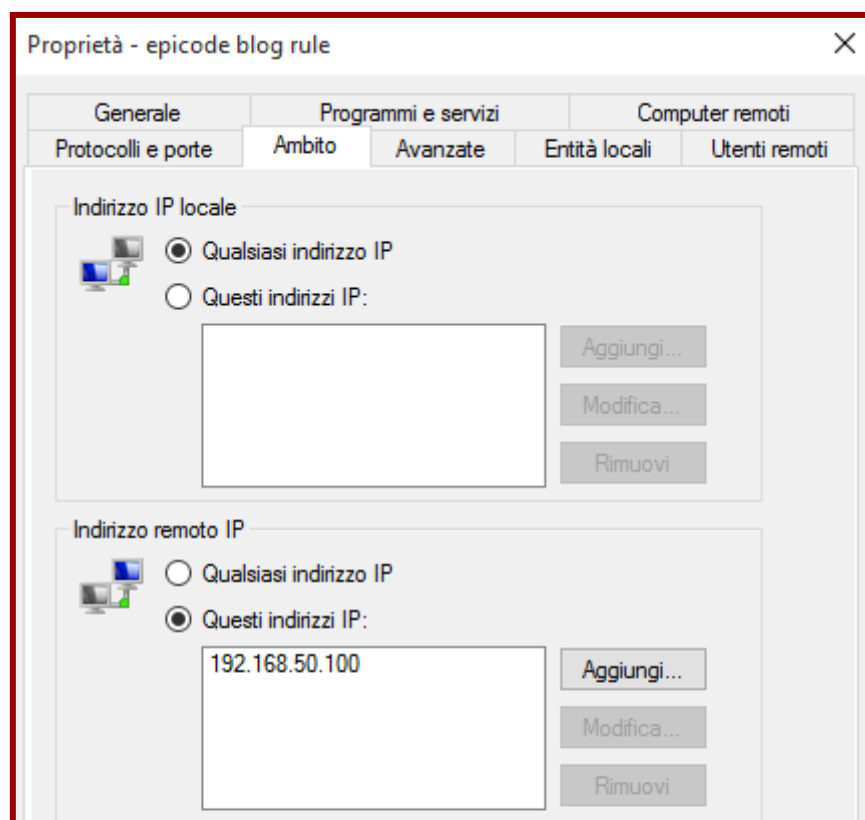
- Configurare policy per non permettere il ping da macchina Linux a macchina Windows nel nostro laboratorio Windows firewall)
- Utilizzo dell'utility InetSim per l'emulazione di servizi Internet
  - Cattura di pacchetti con Wireshark

## CONFIGURAZIONE FIREWALL POLICY

fase uno, configurazione regole del firewall di windows



(Abbiamo creato una nuova regola in cima chiamata "epicode block rule")



testiamo il funzionamento inviando un ping da kali verso windows

```
kali@kali: ~  
Sessione Azioni Modifica Visualizza Aiuto  
comando «ifconfig» da deb net-tools  
Provare: sudo apt install <nome deb>  
  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255  
    inet6 fe80::dc13:6a31:8d77:2630 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:e3:41:f0 txqueuelen 1000 (Ethernet)  
    RX packets 15 bytes 1456 (1.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 32 bytes 3556 (3.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
^
```

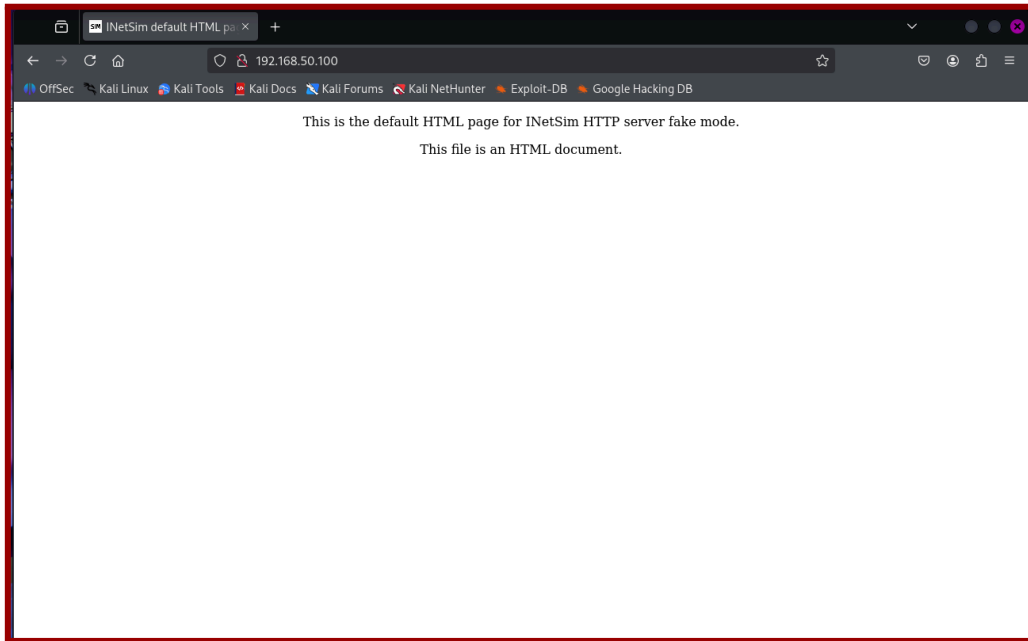
(come vediamo in questo esempio, i pacchetti di dati non arrivano a destinazione)

```
kali@kali: ~  
Sessione Azioni Modifica Visualizza Aiuto  
  
$ 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=41 ttl=128 time=0.666 ms  
64 bytes from 192.168.50.102: icmp_seq=42 ttl=128 time=0.528 ms  
64 bytes from 192.168.50.102: icmp_seq=43 ttl=128 time=1.12 ms  
64 bytes from 192.168.50.102: icmp_seq=44 ttl=128 time=1.20 ms  
64 bytes from 192.168.50.102: icmp_seq=45 ttl=128 time=0.430 ms  
64 bytes from 192.168.50.102: icmp_seq=46 ttl=128 time=0.456 ms  
64 bytes from 192.168.50.102: icmp_seq=47 ttl=128 time=0.571 ms  
64 bytes from 192.168.50.102: icmp_seq=48 ttl=128 time=0.697 ms  
64 bytes from 192.168.50.102: icmp_seq=49 ttl=128 time=0.397 ms  
64 bytes from 192.168.50.102: icmp_seq=50 ttl=128 time=1.53 ms  
64 bytes from 192.168.50.102: icmp_seq=51 ttl=128 time=1.03 ms  
64 bytes from 192.168.50.102: icmp_seq=52 ttl=128 time=0.508 ms  
64 bytes from 192.168.50.102: icmp_seq=53 ttl=128 time=0.939 ms  
64 bytes from 192.168.50.102: icmp_seq=54 ttl=128 time=0.833 ms  
64 bytes from 192.168.50.102: icmp_seq=55 ttl=128 time=0.575 ms  
^X@s64 bytes from 192.168.50.102: icmp_seq=56 ttl=128 time=0.577 ms  
64 bytes from 192.168.50.102: icmp_seq=57 ttl=128 time=0.446 ms  
64 bytes from 192.168.50.102: icmp_seq=58 ttl=128 time=0.452 ms  
64 bytes from 192.168.50.102: icmp_seq=59 ttl=128 time=0.536 ms  
^C  
— 192.168.50.102 ping statistics —  
59 packets transmitted, 19 received, 67.7966% packet loss, time 59124ms  
rtt min/avg/max/mdev = 0.397/0.709/1.528/0.306 ms  
  
(kali@kali)-[~]  
$
```

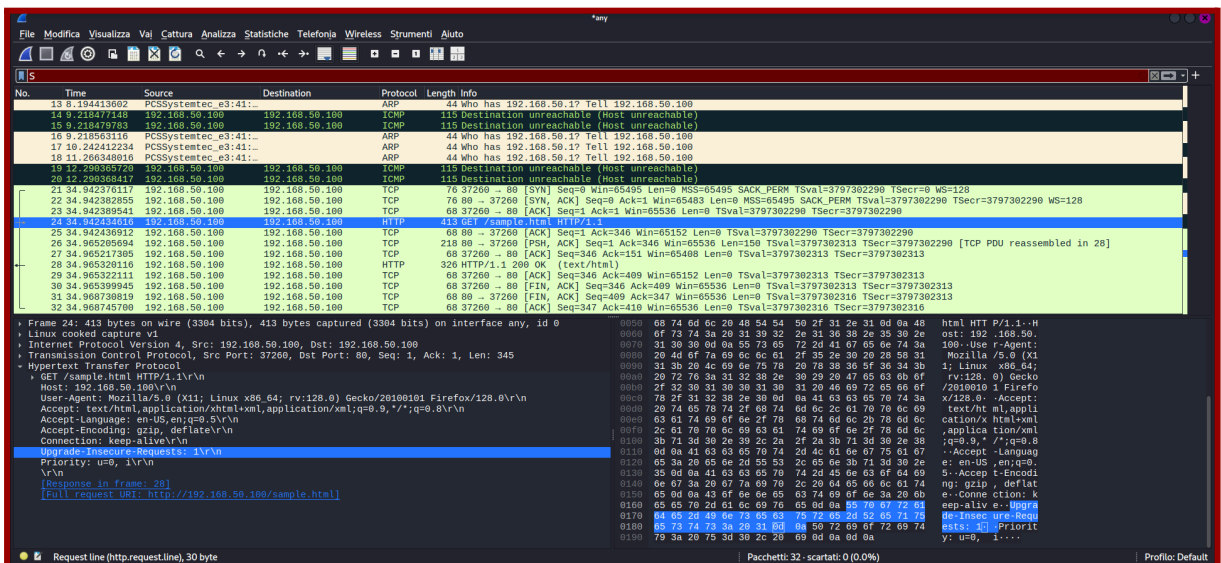
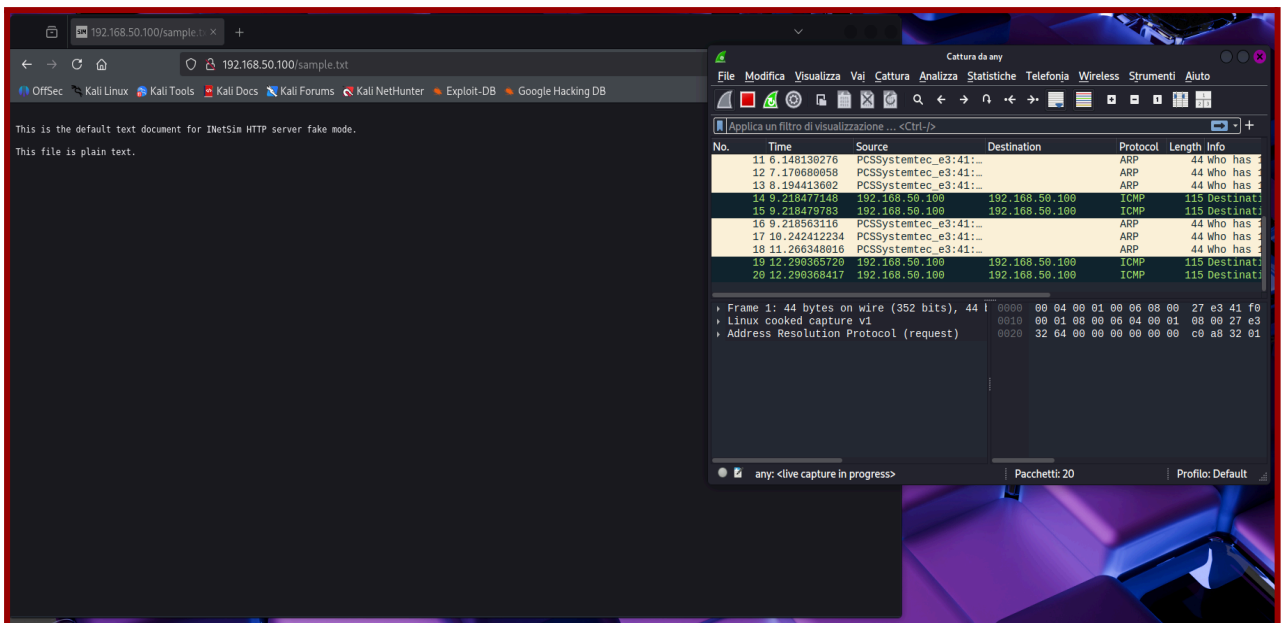
(test inverso, con la regola disattiva funziona tutto)

**PAGINA SEGUENTE PER CONSEGNE FACOLTATIVE**

# SCREEN TEST InetSim + Wireshark



## (Home InetSim)



## sniffing con wireshark