

Report W3D4

- **Introduzione**

Il presente report consiste nello svolgimento di due esercizi.

- La configurazione di un policy firewall su windows .
- Cattura di pacchetti con Wireshark.
- Come simulare alcuni servizi di rete con Inetsim.

L'obiettivo principale è comprendere le basi della comunicazione tra macchine in rete, analizzare i pacchetti di dati trasmessi e simulare scenari realistici per test di sicurezza. Queste competenze sono fondamentali per un professionista della cybersecurity, in quanto consentono di monitorare il traffico di rete e configurare correttamente firewall e servizi.

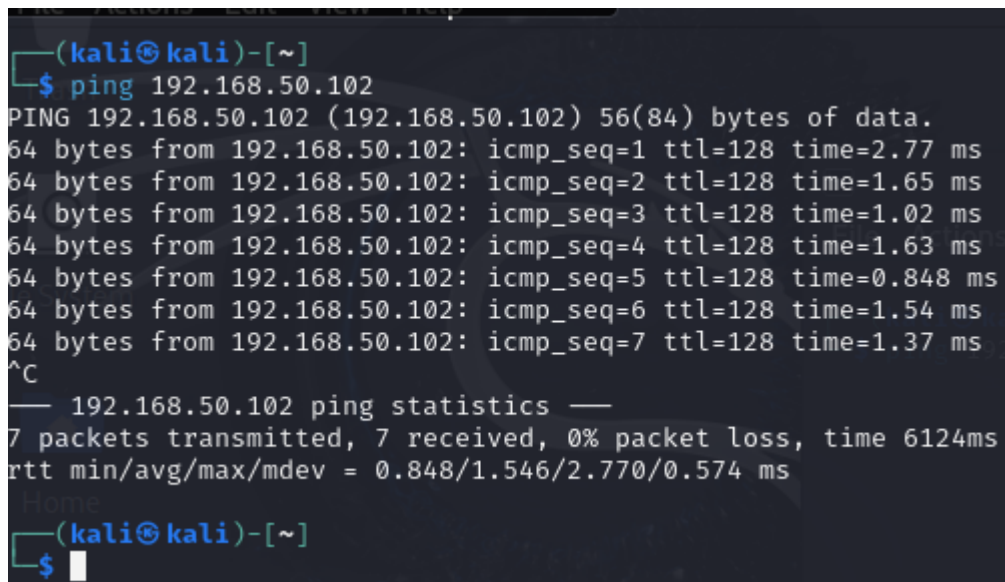
- **Attività svolta**

- **Configurazione policy firewall su windows**

A causa dell'impossibilità di comunicare tra la macchina Windows e Linux, dovuta a una policy restrittiva del firewall di Windows 7, è stata aggiunta una nuova regola per consentire la comunicazione ICMPv4.

→ Pannello di controllo > Visualizza stato della rete e attività > Windows Firewall > Impostazione avanzate > Regole connessioni in entrata > Nuova regola > Personalizza > Avanti > Tutti i programmi > Avanti > Scegliamo ICMPv4 > Avanti > Consenti la connessione > Avanti > Avanti > nome e descrizione > avanti

Risultato: La comunicazione tra le macchine è stata ristabilita con successo. L'ICMPv4 è fondamentale per diagnosticare problemi di rete attraverso strumenti come il comando 'ping'.



```
(kali@kali)-[~]
$ 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=2.77 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.65 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.02 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.63 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.848 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.54 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=1.37 ms
^C
— 192.168.50.102 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6124ms
rtt min/avg/max/mdev = 0.848/1.546/2.770/0.574 ms
Home
(kali@kali)-[~]
$
```

Report W3D4

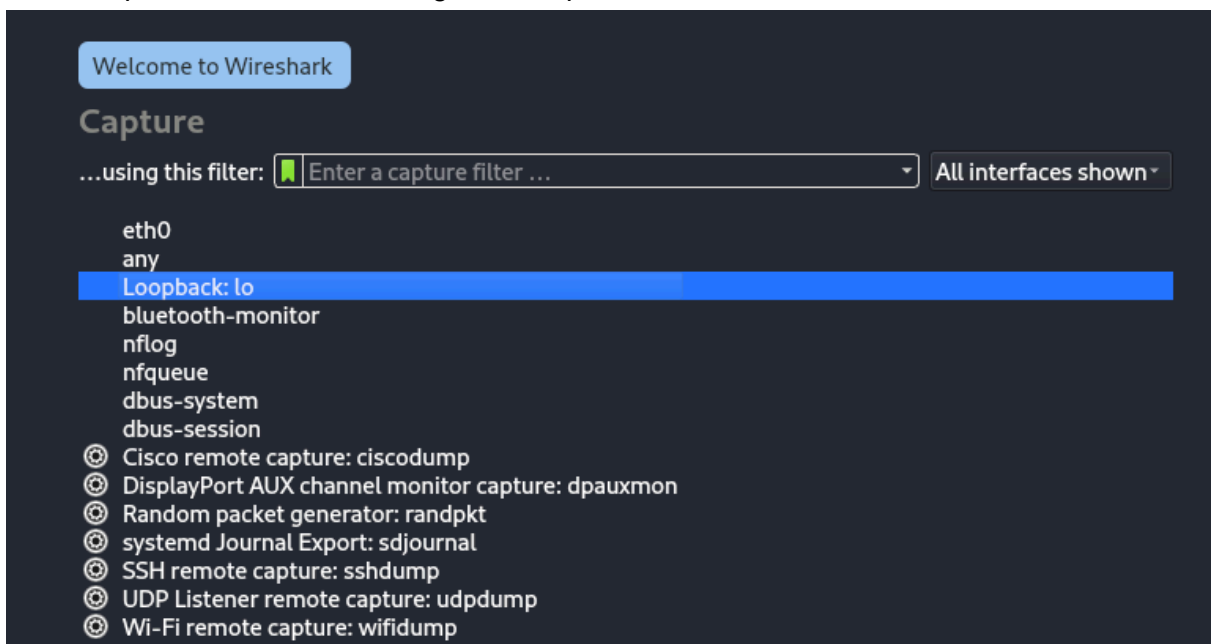
- **Cattura dei pacchetti**

Per la cattura dei pacchetti useremo un programma pre installato su kali chiamato wireshark e invece per la simulazione dei servizi Inetsim, così da emulare una situazione reale:

- Per prima cosa dobbiamo configurare Inetsim attraverso il command `sudo nano /etc/inetsim/inetsim.conf` e mettere # a tutti i servizi che non vogliamo emulare nel nostro caso vogliamo emulare solo l'https quindi sarà l'unico senza come vedremo

```
GNU nano 8.2
# ftps, irc, https
#
#start_service dns
#start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
```

- Adesso apriamo Wireshark e scegliamo loopback

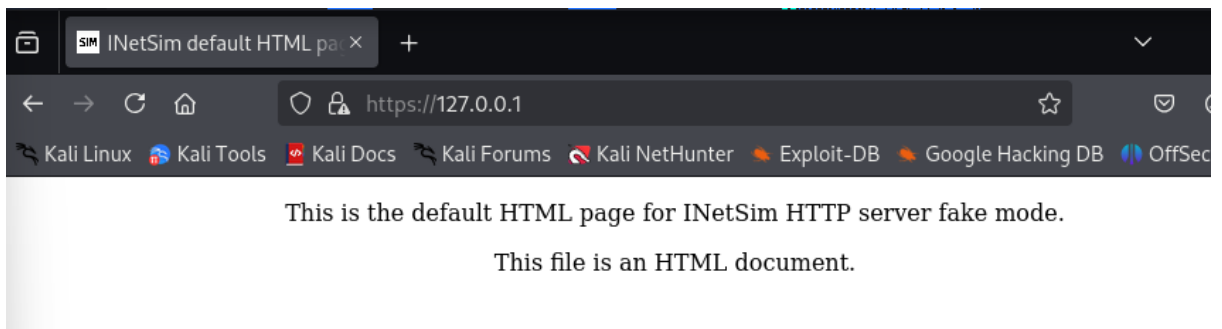


Report W3D4

→ Eseguiamo il comando `sudo inetsim` per simulare il servizio http

```
(kali㉿kali)-[~]
$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 12730) ==
Session ID:      12730
Listening on:    127.0.0.1
Real Date/Time:  2025-03-18 10:48:53
Fake Date/Time: 2025-03-18 10:48:53 (Delta: 0 seconds)
Forking services ...
  * https_443_tcp - started (PID 12740)
  done.
Simulation running.
```

→ Apriamo mozilla e scriviamo `https://127.0.0.1` se ci viene scritto come nella foto vuol dire che l'abbiamo fatto bene



→ Adesso ritornando su wireshark vedremo tutti i pacchetti che ci sono tra cui l'ICMP e TCP che instaura il 3 way handshake e LSV quando il 3 way handshake è finito

ICMP	99	Destination unreachable (Host unreachable)
ICMP	99	Destination unreachable (Host unreachable)
ICMP	112	Destination unreachable (Host unreachable)
ICMP	112	Destination unreachable (Host unreachable)
ICMP	112	Destination unreachable (Host unreachable)
TCP	74	45734 → 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM
TCP	74	443 → 45734 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=6549
TCP	66	45734 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=8918234
TLSv1.3	705	Client Hello