

Emy Mangogna - W3D4 - Pratica

Ex. 1 Configurare una policy nel firewall di Windows per permettere il ping in entrata dalla macchina Kali. Windows(192.168.50.102) Kali(192.168.50.100)

> Verifica della comunicazione tra le macchine;

```
Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Nemi77>ping 192.168.50.100

Pinging 192.168.50.100 with 32 bytes of data:
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fig.1 Ping effettuato da Windows a Kali è avvenuto con successo

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
[kali㉿kali)-[~]
$ ping -c 4 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.

— 192.168.50.102 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3052ms
```

Fig.2 Ping effettuato da Kali a Windows è fallito; La policy predefinita del firewall di Windows blocca le richieste ICMP in ingresso (ping) per ragioni di sicurezza

> Sarà necessario creare una nuova regola nelle policy dei firewall di Windows per permettere le richieste ICMP in ingresso

The screenshot shows the Windows Defender Firewall with Advanced Security interface. On the left, the navigation pane has 'Inbound Rules' selected. The main area displays a list of rules, with 'Allow_Ping' highlighted. To the right, a context menu is open over the 'Allow_Ping' rule, listing actions such as 'New Rule...', 'Filter by Profile', 'Filter by State', 'Filter by Group', 'View', 'Refresh', 'Export List...', 'Help', 'Disable Rule', 'Cut', 'Copy', 'Delete', 'Properties', and 'Help'. The 'Delete' option is highlighted with a red box.

```

File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
[~] (kali㉿kali) ~
$ ping -c 4 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
— 192.168.50.102 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3052ms

[~] (kali㉿kali) ~
$ ping -c 4 192.168.50.102
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=0.677 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.62 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.770 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.53 ms

— 192.168.50.102 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3042ms
rtt min/avg/max/mdev = 0.677/1.150/1.620/0.429 ms

[~] (kali㉿kali) ~
$ 

```

Fig.3 Ping effettuato da Kali a Windows avvenuto con successo

Ex. 2 - Utilizzo dell'utility InetSim per l'emulazione di servizi Internet e Cattura di pacchetti con Wireshark

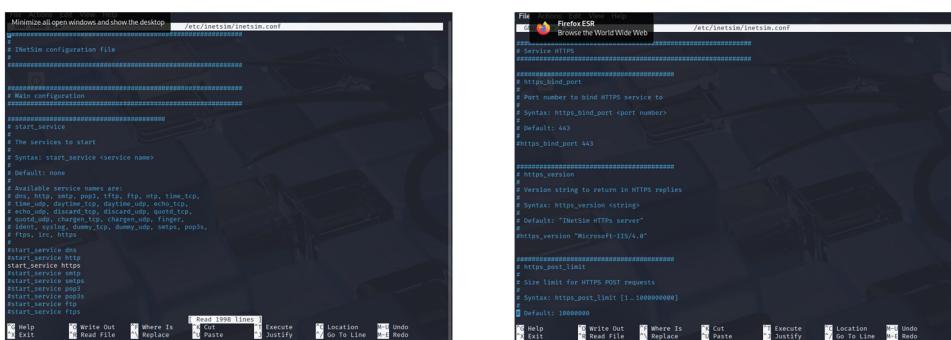


Fig. 4 Attivazione del servizio HTTPS emulato da InetSim e dettagli dei parametri del servizio. Questa configurazione permette di simulare solo il servizio HTTPS, per testare il comportamento del client in una rete controllata.

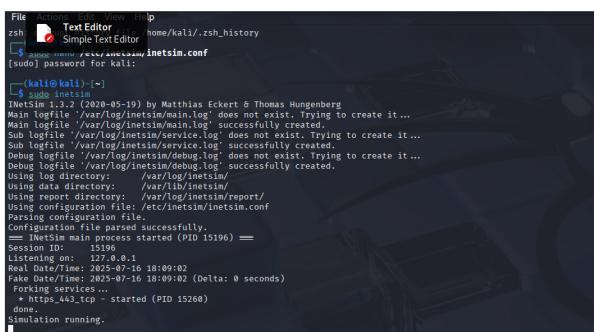


Fig. 5 Verificare che iNetSim stia simulando correttamente i servizi richiesti: assegnazione della porta HTTPS (443) e conferma che il servizio è in ascolto sull'interfaccia di loopback (127.0.0.1).

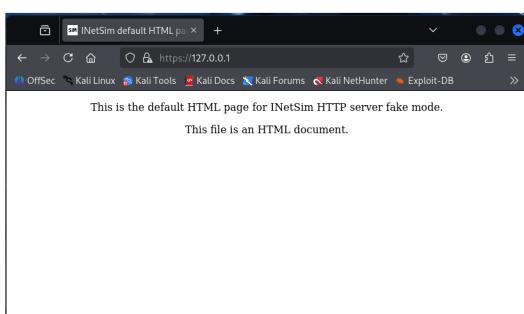


Fig. 6 Conferma del corretto funzionamento della simulazione della risposta di un generico server HTTPS.

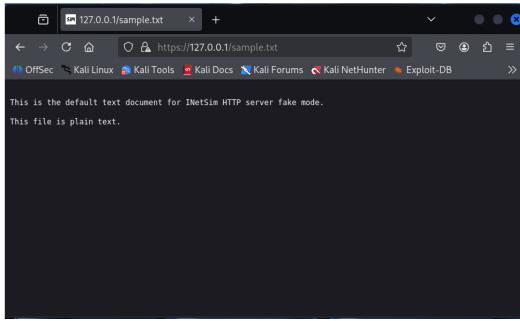


Fig. 7 Conferma della simulazione di contenuti statici da parte di iNetSim. Il server simulato restituisce un file .txt predefinito.

Ex. 3 - Cattura dei pacchetti con Wireshark.

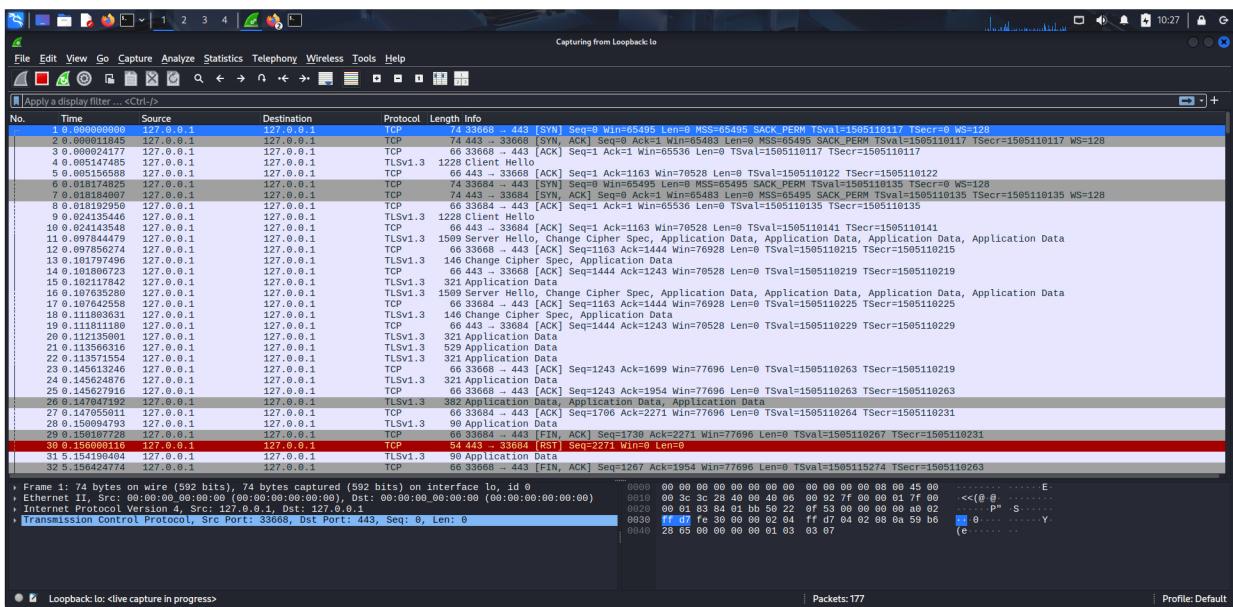


Fig. 7 Analisi del traffico HTTPS locale con Wireshark: pacchetti TCP sulla porta 443 simulati da iNetSim, catturati sull'interfaccia loopback.

Ex. Facoltativo - Simulare altri servizi con InetSim, procedere con lo sniffing delle comunicazioni e analizzare il contenuto dei pacchetti

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
[(kali㉿kali)-~]
└─$ ftp 127.0.0.1 inetsim/inetsim.conf
Connected to 127.0.0.1.
220 INetSim FTP Service ready.
Name (127.0.0.1:kali): emy
331 Please specify the password.
Password:
230 Login successful.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.netsim/report/
ftp> ls
226 Transfer complete.
500 Unknown command.
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
-rw-rw-r-- 1 1098 1098 28 Jul 17 11:02 sample.txt
226 Transfer complete.
ftp> bye
221 Goodbye.
[(kali㉿kali)-~]erted (PID: 116001)
└─$ 
Simulation running.
```

Fig.1 Servizio FTP simulato con InetSim: Connessione al server FTP simulato su 127.0.0.1 effettuata con credenziali personalizzate (**username: emy/password:1234**). Dopo il login, il comando “ls” ha restituito inizialmente “500 Unknown command” ma ha comunque attivato la connessione dati e mostrato il file simulato sample.txt.

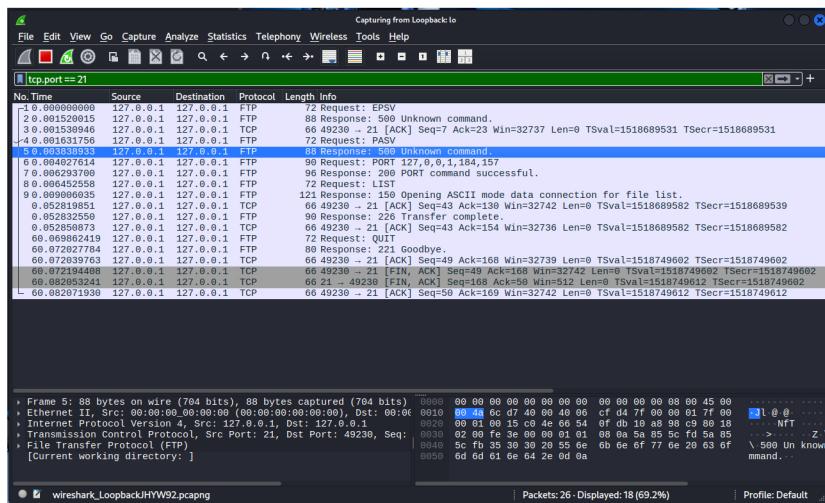


Fig. 2 Cattura traffico FTP con Wireshark