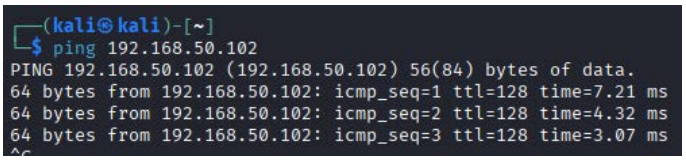
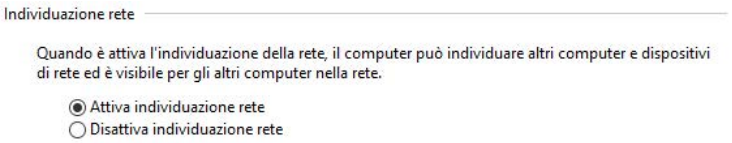
W3D4 - Esercizio 5
FW Rule + PT Capture

Richiesta 1

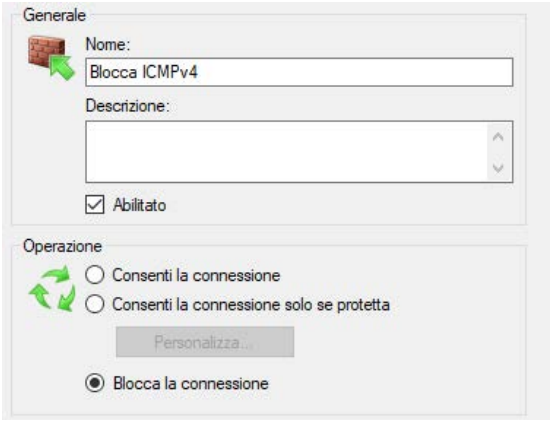
La prima richiesta riguarda la realizzazione di una regola Firewall nella macchina Windows 10 per permettere la ricezione di pacchetti ICMP.

Avendo risolto già in precedenza la problematica del ping tramite l'apposita spunta nelle impostazioni di rete, ho optato per la creazione di una regola che invece bloccano i pacchetti:





Dopo essermi accertato della corretta ricezione dei pacchetti, ho potuto procedere nella creazione della regola:



Di conseguenza, il comando ping dalla macchina Kali non ha avuto esito positivo.

Richiesta 2

La seconda richiesta riguarda l'attivazione del servizio Intesim sulla macchina Kali per emulare al livello applicativo un servizio https (in questo caso).

Per rendere operativo tale servizio è opportuno aprire il file di configurazione inetsim.conf tramite la digitazione sul terminale del percorso,

dunque sudo nano /etc/inetsim/inetsim.conf

All'apertura del file, al suo interno è stato specificato come servizio attivo solo l'https,

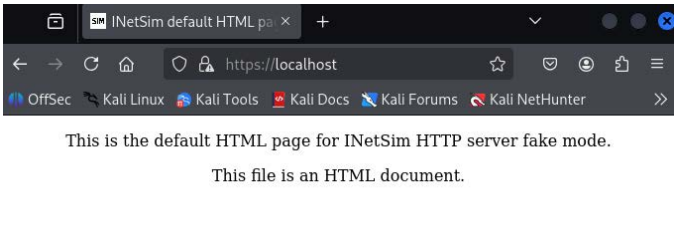
```
#
#start_service dns
#start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
```

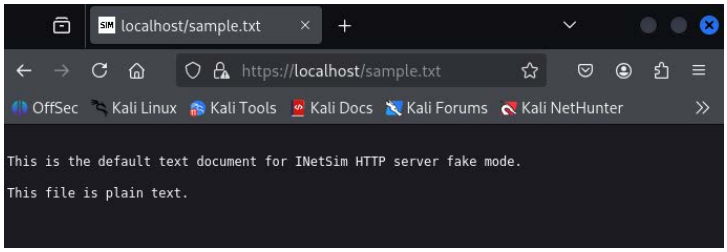
successivamente è stato reso operativo tramite l'invio del comando sudo inetsim (necessita di privileggi di root).

Per verificare il corretto funzionamento del servizio è stato sufficiente digitare su un browser il seguente URL:

https://127.0.0.1 (o in alternativa https://localhost)

In aggiunta, è possibile raggiungere uno dei fake file messi a disposizione di inetsim aggiungendo /sample.txt (nome del file risorsa)





Avviando Wireshark e posizionandoci in ascolto sull'interfaccia loopback (127.0.0.1) mentre eseguiamo un https request, si potranno scorgere numerosi pacchetti TCP che mostrano la sequenza 3 way handshake (syn, syn-ack, ack)

No.	Time	Source	Destination	Protocol	Length	Info
29	50.138128399	127.0.0.1	127.0.0.1	TCP	74	59294 → 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=24701728 …
30	50.138136960	127.0.0.1	127.0.0.1	TCP	74	443 → 59294 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSva…
31	50.138145109	127.0.0.1	127.0.0.1	TCP	66	59294 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=24701728 TSecr=24701728
32	50.139706137	127.0.0.1	127.0.0.1	TLSv1.3	1278	Client Hello (SNI=localhost)
33	50.139711028	127.0.0.1	127.0.0.1	TCP	66	443 → 59294 [ACK] Seq=1 Ack=1213 Win=71552 Len=0 TSval=24701730 TSecr=24701…
34	50.143692241	127.0.0.1	127.0.0.1	TLSv1.3	1509	Server Hello, Change Cipher Spec, Application Data, Application Data, Appli…
35	50.143692241	127.0.0.1	127.0.0.1	TCP	66	59294 → 443 [ACK] Seq=1213 Ack=1444 Win=76928 Len=0 TSval=24701734 TSecr=24…
36	50.147694242	127.0.0.1	127.0.0.1	TLSv1.3	146	Change Cipher Spec, Application Data
37	50.147694242	127.0.0.1	127.0.0.1	TLSv1.3	321	Application Data
38	50.199720241	127.0.0.1	127.0.0.1	TCP	66	59294 → 443 [ACK] Seq=1293 Ack=1699 Win=77696 Len=0 TSval=24701782 TSecr=24…
39	50.199720241	127.0.0.1	127.0.0.1	TLSv1.3	321	Application Data
40	50.199720241	127.0.0.1	127.0.0.1	TCP	66	59294 → 443 [ACK] Seq=1293 Ack=1954 Win=77696 Len=0 TSval=24701790 TSecr=24…
41	51.846795173	127.0.0.1	127.0.0.1	TLSv1.3	521	Application Data
42	51.856880186	127.0.0.1	127.0.0.1	TLSv1.3	239	Application Data
43	51.856894390	127.0.0.1	127.0.0.1	TCP	66	59294 → 443 [ACK] Seq=1748 Ack=2127 Win=77696 Len=0 TSval=24703447 TSecr=24…
44	51.857072948	127.0.0.1	127.0.0.1	TLSv1.3	346	Application Data
45	51.857078932	127.0.0.1	127.0.0.1	TCP	66	59294 → 443 [ACK] Seq=1748 Ack=2407 Win=77696 Len=0 TSval=24703447 TSecr=24…
46	51.857148699	127.0.0.1	127.0.0.1	TLSv1.3	90	Application Data
47	51.857156277	127.0.0.1	127.0.0.1	TCP	66	59294 → 443 [FIN, ACK] Seq=1772 Ack=2407 Win=77696 Len=0 TSval=24703447 TSe…
48	51.859168954	127.0.0.1	127.0.0.1	TLSv1.3	90	Application Data