## Policy e Packet captur

Come prima cosa controlliamo che la kali comunica con windows con il comando PING

```
File Actions Edit View Help

(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=2.34 ms

64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.08 ms

64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.921 ms

^C

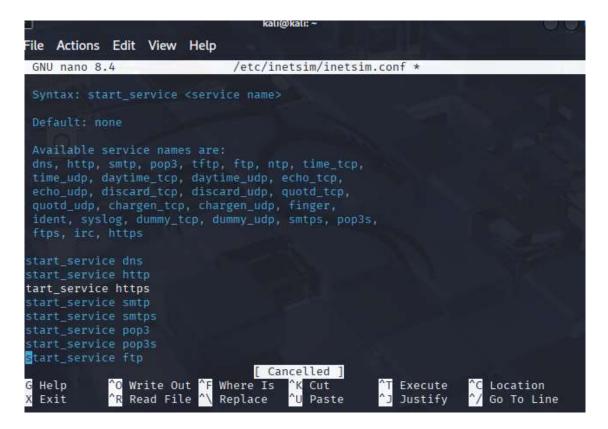
192.168.50.102 ping statistics —

3 packets transmitted, 3 received, 0% packet loss, time 2002ms

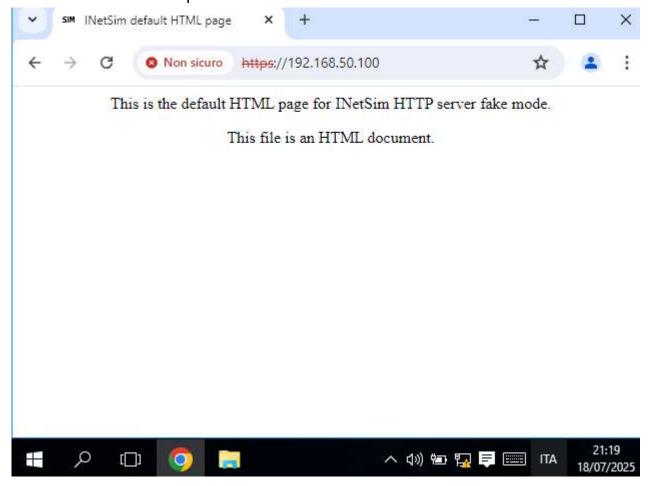
rtt min/avg/max/mdev = 0.921/1.448/2.341/0.634 ms

(kali@kali)-[~]
```

Come seconda cosa configuriamo il file inetsim.conf per utilizzare solo il servizio HTTPS



Facciamo partire inetti dalla kali e dalla macchina windows andremo sul browser e cercheremo l'indirizzo ip della macchina kali con un servizio HTTPS attivo



Come possiamo vedere tutto funziona perfettamente. Ora controlliamo dalla kali il traffico di rete con wireshark

```
60 49453 - 443 [ACK] Seq=1797 Ack=1445 Win=64256 Len=0
89 Standard query 0xf5ef A clientservices.googleapis.com
1497 Server Hello, Change Cipher Spec, Application Data, Applicati
134 Change Cipher Spec, Application Data
54 443 - 49455 [ACK] Seq=1444 Ack=1878 Win=62464 Len=0
         84 7.247725058
85 7.305468461
                                                                                               192.168.50.100
192.168.50.100
                                               192.168.50.102
                                                                                                                                                DNS
                                               192.168.50.100
         86 7.347901092
                                                                                               192.168.50.102
                                                                                                                                                TLSv1.3
         87 7.349561952
88 7.349590674
                                               192.168.50.102
192.168.50.100
                                                                                               192.168.50.100
192.168.50.102
                                                                                                                                               TLSv1.3
TCP
                                                                                                                                                TLSv1.3
                                                                                                                                                                      760 Application Data
54 443 → 49455 [ACK] Seq=1444 Ack=2584 Win=61824 Len=0
309 Application Data
         89 7.350269754
                                               192,168,50,102
                                                                                               192,168,50,100
         90 7.350279587
91 7.351152877
                                              192.168.50.100
192.168.50.100
                                                                                               192.168.50.102
192.168.50.102
                                                                                                                                                TCP
TLSv1.3
                                                                                                                                                                      60 49455 - 443 [ACK] Seq=2584 Ack=1699 Win=65536 Len=0
309 Application Data
         92 7.401391558
                                               192,168,50,102
                                                                                               192.168.50.100
                                                                                                                                                TCP
                                                                                                                                                TLSv1.3
         93 7.401416774
                                               192,168,50,100
                                                                                               192.168.50.102
                                                                                                                                                                      589 Application Data, Application Data, Application Data

60 49455 - 443 [ACK] Seq=2584 Ack=2432 Win=64768 Len=0

60 49455 - 443 [FIN, ACK] Seq=2584 Ack=2432 Win=64768 Len=0

54 443 - 49455 [ACK] Seq=2432 Ack=2585 Win=61824 Len=0

81 Standard query 0xfc34 A update.googleapis.com
                                                                                                                                               TLSv1.3
         94 7.409270211
95 7.409637640
                                               192.168.50.100
192.168.50.102
                                                                                               192.168.50.102
192.168.50.100
         96 7.411631458
97 7.411653873
98 7.438774942
                                                                                               192.168.50.100
192.168.50.102
192.168.50.100
                                               192.168.50.102
                                                                                                                                                DNS
         99 7 438804707
                                               192 168 50 100
                                                                                                192 168 50 102
                                                                                                                                                                        109 Destination unreachable (Port unreachable)
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface eth0, Ethernet II, Src: PCSSystemtec_a3:2f:ab (08:00:27:a3:2f:ab), Dst: Broadcast (ff:ff:ff Internet Protocol Version 4, Src: 192.168.50.102, Dst: 192.168.50.255 User Datagram Protocol, Src Port: 137, Dst Port: 137 NetBIOS Name Service
                                                                                                                                                                                                                   ff ff ff ff ff 68 00
00 4e 58 bf 00 00 80 11
32 ff 00 89 00 89 00 3a
00 00 00 00 00 20 46
41 43 41 43 41 43 41 43
41 43 41 43 41 41 00
                                                                                                                                                                                                                                                                            27 a3 2f ab 08
fb 29 c0 a8 32
4e 8a 87 b9 01
48 46 41 45 42
41 43 41 43 41
00 20 00 01
                                                                                                                                                                                                                                                                                                                00
66
10
45
43
```

E da qui possiamo analizzare i pacchetti che partono che si comunicano le due macchine.

Possiamo rifare la stessa cosa con un altro servizio invece che HTTPS possiamo usare http quindi dobbiamo modificare il file inetti.conf per attivare il servizio http

```
GNU nano 8.4 /etc/inetsim/inetsim.conf *

# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#

#start_service dns
start_service http
#start_service smtp
#start_service smtp
#start_service pop3
#start_service ftp
#start_service ftp
#start_service ftp
#start_service irc
#start_service irc
#start_service inger
#start_service ident
#start_service ident
#start_service ident
#start_service itme_tcp
#start_service time_tcp
#start_service time_tcp
#start_service time_udp
```

Cerchiamo dal browser di windows la stessa cosa ma con protocollo

## http invece che HTTPS



This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

## E poi andremo a vedere le differenze da wireshark controllando il contenuto dei pacchetti

No.	Time	Source	Destination	n			Prote	col	Lengt	Info		
	67 13.568966070	192.168.50.102	192.168	.50.10	0		DNS		7	6 Sta	ndar	d q
	68 13.902280219	192.168.50.102	192.168	.50.10	0		TCP		6	6 494	67 -	. 80
	69 13.902310159	192.168.50.100	192.168	.50.10	2		TCP		6	6 80	- 49	467
	70 13.902415833	192.168.50.102	192.168	.50.10	0		TCP		6	6 494	68 -	. 80
	71 13.902423977	192.168.50.100	192.168	.50.10	2		TCP		6	6 80	- 49	468
	72 13.902525691	192.168.50.102	192.168	.50.10	Θ		TCP		6	9 494	67 -	. 80
	73 13.902863089	192.168.50.102	192.168	.50.10	0		TCP		6	9 494	68 -	. 80
	74 13.906697250	192.168.50.102	192.168	.50.10	0		HTTI	)	53	9 GET	1 +	ITTP.
	75 13.906718835	192.168.50.100	192.168	.50.10	2		TCP		5	4 80	- 49	468
	76 13.955512675	192.168.50.100	192.168	.50.10	2		TCP		20	4 80	→ 49	468
	77 13.961187160	192.168.50.100	192.168	.50.10	2		HTTI	)	31	2 HTT	P/1.	1 2
→ Fr	ame 1: 76 bytes or	n wire (608 bits),	76 b 0000	08 00	27	с9	0e d	a 08	00	27 a3	2f	ab
		SSystemtec_a3:2f:al		00 36	5e	1c	00 0	9 80	11	f6 77	C0	a8
11 11 11 11 11		ersion 4, Src: 192.:		32 64	db	e8	00 3	5 00	2a	6b 86	14	e9
		col, Src Port: 5629		00 00	00	00	00 0	0 07	62	65 61	63	6f
	main Name System (		0040	76 74	32	03	63 6	f 6d	00	00 01	00	01
	W)			-								