

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

```
kali@kali: ~
File Actions Edit View Help
GNU nano 8.4 /etc/inetsim/inetsim.conf *

Syntax: start_service <service name>

Default: none

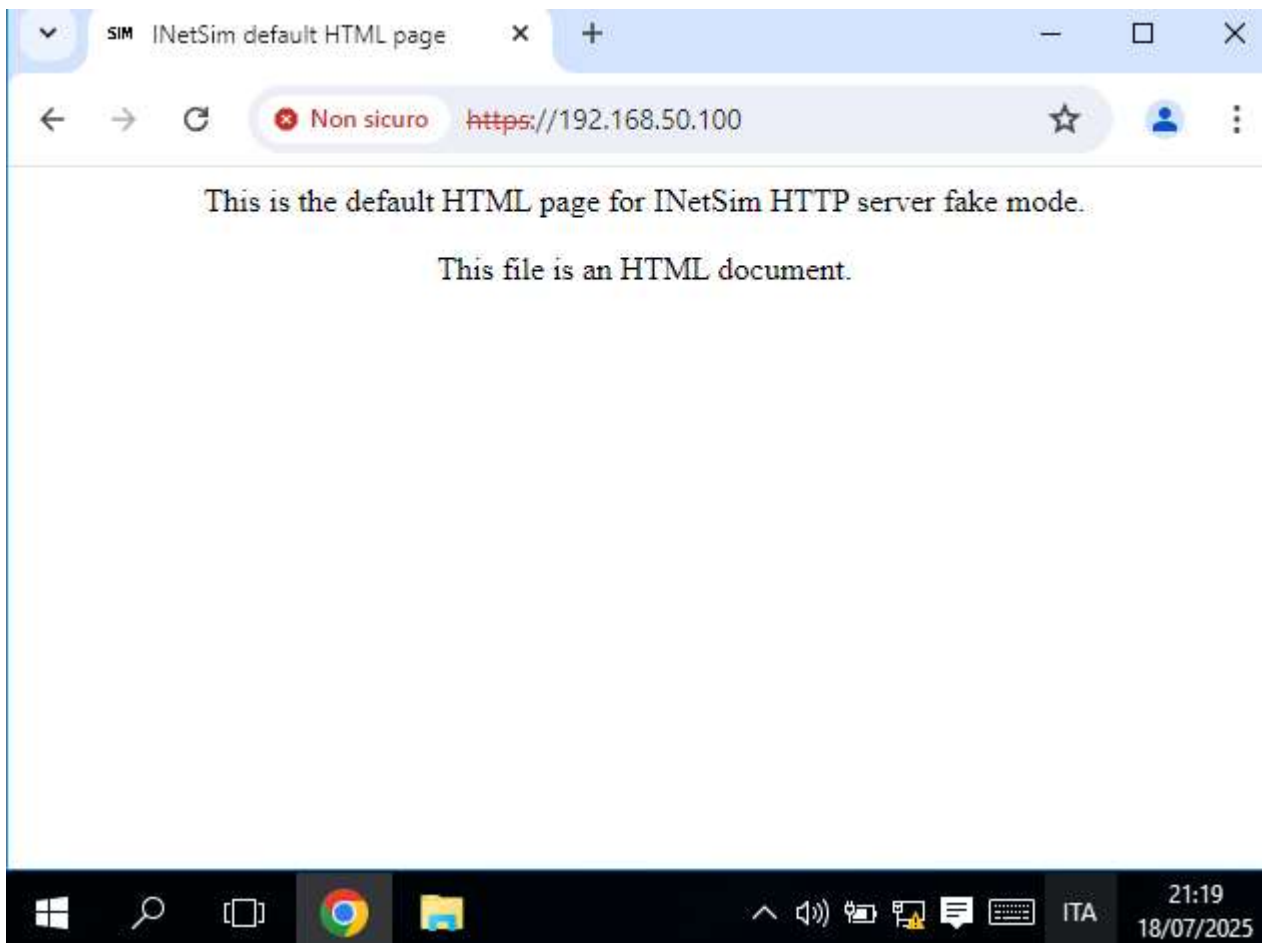
Available service names are:
dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
time_udp, daytime_tcp, daytime_udp, echo_tcp,
echo_udp, discard_tcp, discard_udp, quotd_tcp,
quotd_udp, chargen_tcp, chargen_udp, finger,
ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
ftps, irc, https

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

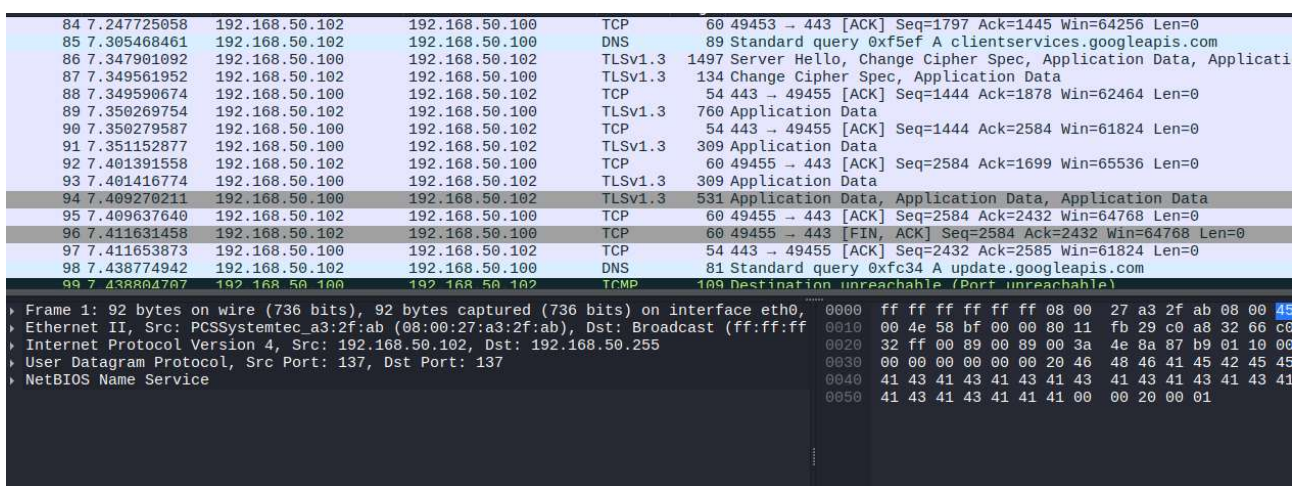
[ Cancelled ]

G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location
X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

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



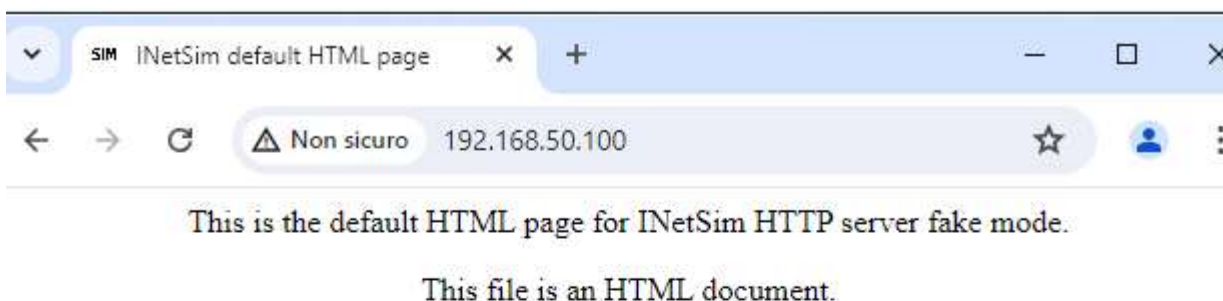
E da qui possiamo analizzare i pacchetti che partono che si comunicano le due macchine.

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 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
```

Cerchiamo dal browser di windows la stessa cosa ma con protocollo

http invece che HTTPS



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

No.	Time	Source	Destination	Protocol	Length	Info
67	13.568966070	192.168.50.102	192.168.50.100	DNS	76	Standard query
68	13.902280219	192.168.50.102	192.168.50.100	TCP	66	49467 → 80
69	13.902310159	192.168.50.100	192.168.50.102	TCP	66	80 → 49467
70	13.902415833	192.168.50.102	192.168.50.100	TCP	66	49468 → 80
71	13.902423977	192.168.50.100	192.168.50.102	TCP	66	80 → 49468
72	13.902525691	192.168.50.102	192.168.50.100	TCP	60	49467 → 80
73	13.902863089	192.168.50.102	192.168.50.100	TCP	60	49468 → 80
74	13.906697250	192.168.50.102	192.168.50.100	HTTP	530	GET / HTTP
75	13.906718835	192.168.50.100	192.168.50.102	TCP	54	80 → 49468
76	13.955512675	192.168.50.100	192.168.50.102	TCP	204	80 → 49468
77	13.961187160	192.168.50.100	192.168.50.102	HTTP	312	HTTP/1.1 200

▶ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
 ▶ Ethernet II, Src: PCSSystemtec_a3:2f:ab (08:00:00:08:00:11), Dst: 08:00:00:08:00:0a
 ▶ Internet Protocol Version 4, Src: 192.168.50.102, Dst: 192.168.50.100
 ▶ User Datagram Protocol, Src Port: 56296, Dst Port: 53
 ▶ Domain Name System (query)