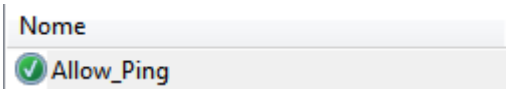
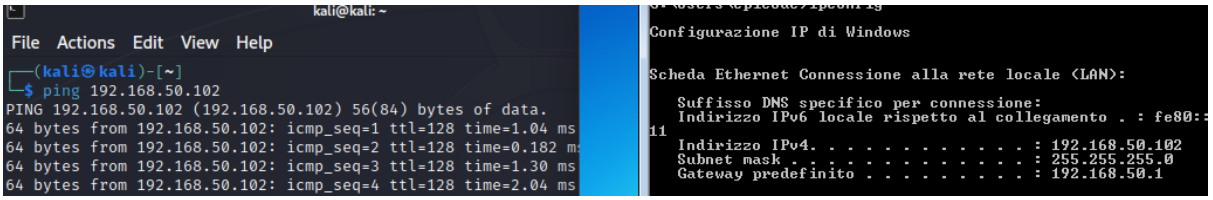
FAR PINGARE LE DUE VM

Per permettere a Windows di pingare con Kali dobbiamo **intervenire sulle regole Policy** di entrata **di W7**, quindi creiamo una nuova regola Top and Down. Andando su **Windows Firewall-Impostazioni avanzate-regole connessioni in entrata-Nuova regola.**

1) Custom
2) All Programs
3) Protocollo ICMPv4
4) Limitare gli accessi IP. (per adesso tutti)
5) Allow the connection, doman private pubblic
6) Dare un nome ed una descrizione



KALI W7 IP

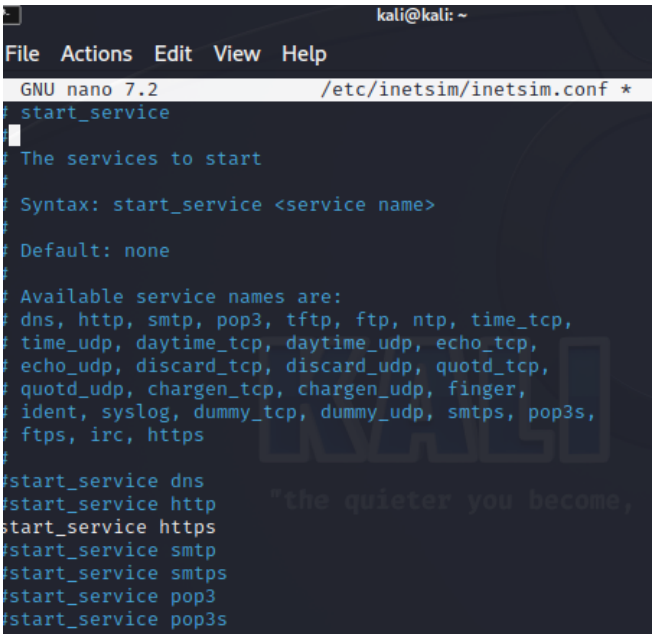


UTILIZZO DELL'UTILITY INETSIM PER L'EMULAZIONE DEI SERVIZI INTERNET

Si utilizza **Wireshark** per la **cattura dei pacchetti** e l'**analisi** del **contenuto** dei pacchetti, a supporto utilizzeremo **Inetsim (simula servizi Internet)**, Simula alcuni servizi come L'HTTP e L'HTTPS.

1)Bisogna configurare Inet sim tramite il comando sudo nano /etc/inetsim/inetsim.conf per decidere quali servizi avviare e su quali porte avviarli.

2)Attivare solo il servizio HTTPs aggiungendo un cancelletto(altgr+à) prima di ogni riga tranne quella dell'https, cosi andremo a commentare tutti i servizi tranne quelli dell'HTTPs. A questo punto con un nuovo avvio di inetsim si analizzerà il traffico de del solo protocollo HTTPs

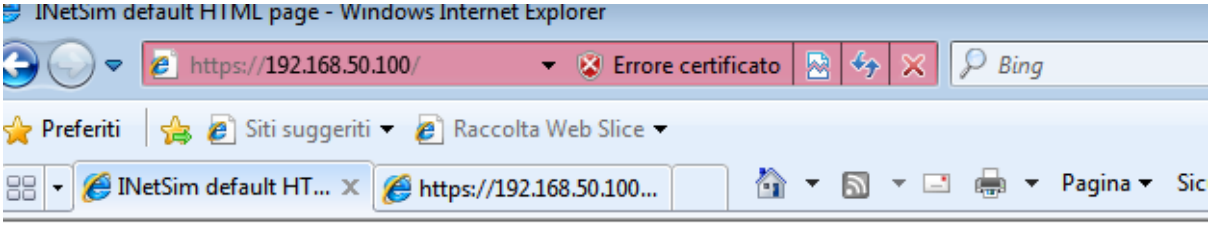


3) scendere di pagine e modificare e commentare service_bind_address, basta eliminare il cancelletto sulla linea. Per inscenare una situazione reale Inetsim ci mette a disposizione dei FakeFile, ovvero dei file vuoti con delle estensioni che possiamo richiedere come se fossero delle risorse reali.

4)Lanciamo inetsim dal terminale con il comando sudo inetsim

5)Avviamo il browser da W7(Client) con l'indirizzo IP di Kali(server) HTTPs://192.168.50.100 (in questo caso Kali fa da Server e da Client).

Otterremo questo:

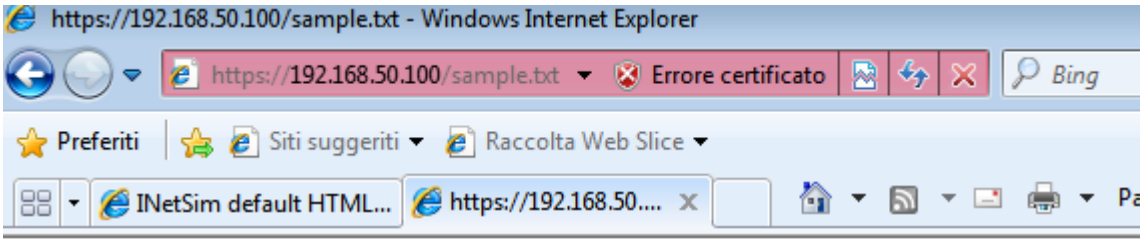


This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

6) Richiediamo i file fittizi messi a disposizione da Inetsim. Sul browser di W7 digitiamo https://192.168.50.100/sample/txt

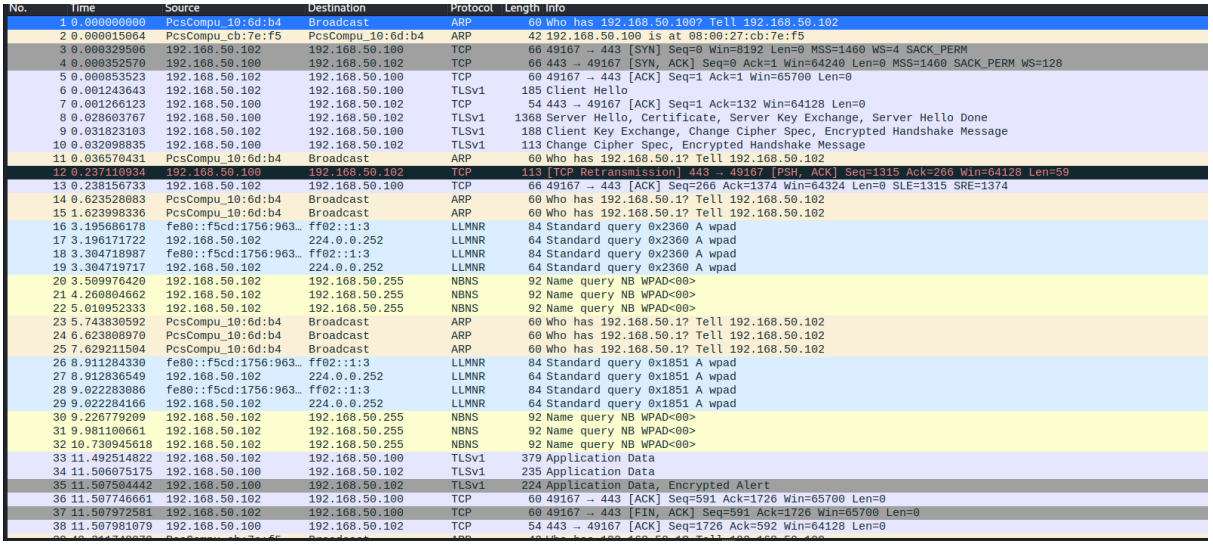
Otterremo questo:




```
This is the default text document for INetSim HTTP server fake mode.

This file is plain text.
```

7)Catturiamo i **Pacchetti** con Wireshark utilizzando **ETH0** e refreshando il browser su W7 cattureremo i seguenti pacchetti



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.100? Tell 192.168.50.102
2	0.000015064	PcsCompu_cb:7e:f5	PcsCompu_10:6d:b4	ARP	42	192.168.50.100 is at 08:00:27:cb:7e:f5
3	0.000329506	192.168.50.102	192.168.50.100	TCP	66	49167 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4	0.000352570	192.168.50.100	192.168.50.102	TCP	66	443 → 49167 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.000853523	192.168.50.102	192.168.50.100	TCP	60	49167 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.001243643	192.168.50.102	192.168.50.100	TLSv1	185	Client Hello
7	0.001266123	192.168.50.100	192.168.50.102	TCP	54	443 → 49167 [ACK] Seq=1 Ack=132 Win=64128 Len=0
8	0.028603767	192.168.50.100	192.168.50.102	TLSv1	1368	Server Hello, Certificate, Server Key Exchange, Server Hello Done
9	0.031823103	192.168.50.102	192.168.50.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.032098835	192.168.50.100	192.168.50.102	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
11	0.036570431	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
12	0.237110934	192.168.50.100	192.168.50.102	TCP	113	[TCP Retransmission] 443 → 49167 [PSH, ACK] Seq=1315 Ack=266 Win=64128 Len=59
13	0.238156733	192.168.50.102	192.168.50.100	TCP	66	49167 → 443 [ACK] Seq=266 Ack=1374 Win=64324 Len=0 SLE=1315 SRE=1374
14	0.623528083	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
15	1.623998336	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
16	3.195686178	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	84	Standard query 0x2360 A wpad
17	3.196171722	192.168.50.102	224.0.0.252	LLMNR	64	Standard query 0x2360 A wpad
18	3.304718987	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	84	Standard query 0x2360 A wpad
19	3.304719717	192.168.50.102	224.0.0.252	LLMNR	64	Standard query 0x2360 A wpad
20	3.509976420	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
21	4.260804662	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
22	5.010952333	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
23	5.743830592	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
24	6.623808970	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
25	7.629211504	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
26	8.911284330	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	84	Standard query 0x1851 A wpad
27	8.912836549	192.168.50.102	224.0.0.252	LLMNR	64	Standard query 0x1851 A wpad
28	9.022283086	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	84	Standard query 0x1851 A wpad
29	9.022284166	192.168.50.102	224.0.0.252	LLMNR	64	Standard query 0x1851 A wpad
30	9.226779209	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
31	9.981100661	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
32	10.730945618	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
33	11.492514822	192.168.50.102	192.168.50.100	TLSv1	379	Application Data
34	11.506075175	192.168.50.100	192.168.50.102	TLSv1	235	Application Data
35	11.507504442	192.168.50.100	192.168.50.102	TLSv1	224	Application Data, Encrypted Alert
36	11.507746661	192.168.50.102	192.168.50.100	TCP	60	49167 → 443 [ACK] Seq=591 Ack=1726 Win=65700 Len=0
37	11.507972581	192.168.50.102	192.168.50.100	TCP	60	49167 → 443 [FIN, ACK] Seq=591 Ack=1726 Win=65700 Len=0
38	11.507981079	192.168.50.100	192.168.50.102	TCP	54	443 → 49167 [ACK] Seq=1726 Ack=592 Win=64128 Len=0

8) Confronto pacchetti HTTP:

	Time	Source	Destination	Protocol	Length	Info
10	5.165795183	PcsCompu_10:6d:b4	PcsCompu_cb:7e:f5	ARP	60	192.168.50.102 is at 08:00:27:10:6d:b4
11	18.796814275	fe80::f5cd:1756:963…	ff02::1:2	DHCPv6	150	Solicit XID: 0x872ac1 CID: 000100012cfc104f080027106db4
12	18.930728253	192.168.50.102	192.168.50.100	TCP	66	49171 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
13	18.930761582	192.168.50.100	192.168.50.102	TCP	66	80 → 49171 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
14	18.931360467	192.168.50.102	192.168.50.100	TCP	60	49171 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	18.937055270	192.168.50.102	192.168.50.100	HTTP	459	GET /sample.txt HTTP/1.1
16	18.937071201	192.168.50.100	192.168.50.102	TCP	54	80 → 49171 [ACK] Seq=1 Ack=406 Win=64128 Len=0
17	18.961855177	192.168.50.100	192.168.50.102	TCP	204	80 → 49171 [PSH, ACK] Seq=1 Ack=406 Win=64128 Len=150 [TCP segment of a reassembled PDU]
18	18.963025732	192.168.50.100	192.168.50.102	HTTP	151	HTTP/1.1 200 OK (text/plain)
19	18.963414774	192.168.50.102	192.168.50.100	TCP	60	49171 → 80 [ACK] Seq=406 Ack=249 Win=65452 Len=0
20	18.963551066	192.168.50.102	192.168.50.100	TCP	60	49171 → 80 [FIN, ACK] Seq=406 Ack=249 Win=65452 Len=0
21	18.963559846	192.168.50.100	192.168.50.102	TCP	54	80 → 49171 [ACK] Seq=249 Ack=407 Win=64128 Len=0
22	18.981170541	192.168.50.102	192.168.50.100	TCP	66	49172 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
23	18.981194028	192.168.50.100	192.168.50.102	TCP	66	80 → 49172 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
24	18.981585498	192.168.50.102	192.168.50.100	TCP	60	49172 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
25	18.981768127	192.168.50.102	192.168.50.100	HTTP	325	GET /favicon.ico HTTP/1.1
26	18.981777195	192.168.50.100	192.168.50.102	TCP	54	80 → 49172 [ACK] Seq=1 Ack=272 Win=64128 Len=0
27	18.991735239	192.168.50.100	192.168.50.102	TCP	207	80 → 49172 [PSH, ACK] Seq=1 Ack=272 Win=64128 Len=153 [TCP segment of a reassembled PDU]
28	18.992931860	192.168.50.100	192.168.50.102	HTTP	252	HTTP/1.1 200 OK (image/x-icon)
29	18.993141907	192.168.50.102	192.168.50.100	TCP	60	49172 → 80 [ACK] Seq=272 Ack=353 Win=65348 Len=0
30	18.993257930	192.168.50.102	192.168.50.100	TCP	60	49172 → 80 [FIN, ACK] Seq=272 Ack=353 Win=65348 Len=0
31	18.993267228	192.168.50.100	192.168.50.102	TCP	54	80 → 49172 [ACK] Seq=353 Ack=273 Win=64128 Len=0
32	28.366638055	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
33	28.905619609	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
34	29.900319802	PcsCompu_10:6d:b4	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.102
35	31.516017322	fe80::f5cd:1756:963…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
36	31.516831383	192.168.50.102	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
37	31.517070664	fe80::f5cd:1756:963…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
38	31.517070904	192.168.50.102	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
39	31.517791087	fe80::f5cd:1756:963…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
40	31.517791337	192.168.50.102	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
41	31.518395259	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	88	Standard query 0x37d7 ANY Windows7
42	31.518395470	192.168.50.102	224.0.0.252	LLMNR	68	Standard query 0x37d7 ANY Windows7
43	31.521423914	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	84	Standard query 0xa32d A wpad
44	31.521424105	192.168.50.102	224.0.0.252	LLMNR	64	Standard query 0xa32d A wpad
45	31.623257897	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	88	Standard query 0x37d7 ANY Windows7
46	31.623258808	192.168.50.102	224.0.0.252	LLMNR	68	Standard query 0x37d7 ANY Windows7
47	31.623259030	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	84	Standard query 0xa32d A wpad
48	31.623259251	192.168.50.102	224.0.0.252	LLMNR	64	Standard query 0xa32d A wpad
49	31.830969451	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
50	31.908310967	192.168.50.102	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
51	31.908311909	fe80::f5cd:1756:963…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
52	32.580602165	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
53	33.339502802	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
54	34.095891390	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	84	Standard query 0x0718 A wpad
55	34.095892032	192.168.50.102	224.0.0.252	LLMNR	64	Standard query 0x0718 A wpad
56	34.188736093	fe80::f5cd:1756:963…	ff02::1:3	LLMNR	84	Standard query 0x0718 A wpad
57	34.188737257	192.168.50.102	224.0.0.252	LLMNR	64	Standard query 0x0718 A wpad
58	34.388659120	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
59	35.126618866	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>
60	35.880799730	192.168.50.102	192.168.50.255	NBNS	92	Name query NB WPAD<00>

9) L’https lavora sulla porta 443 mentre l’http sull’80. si modificano da qui