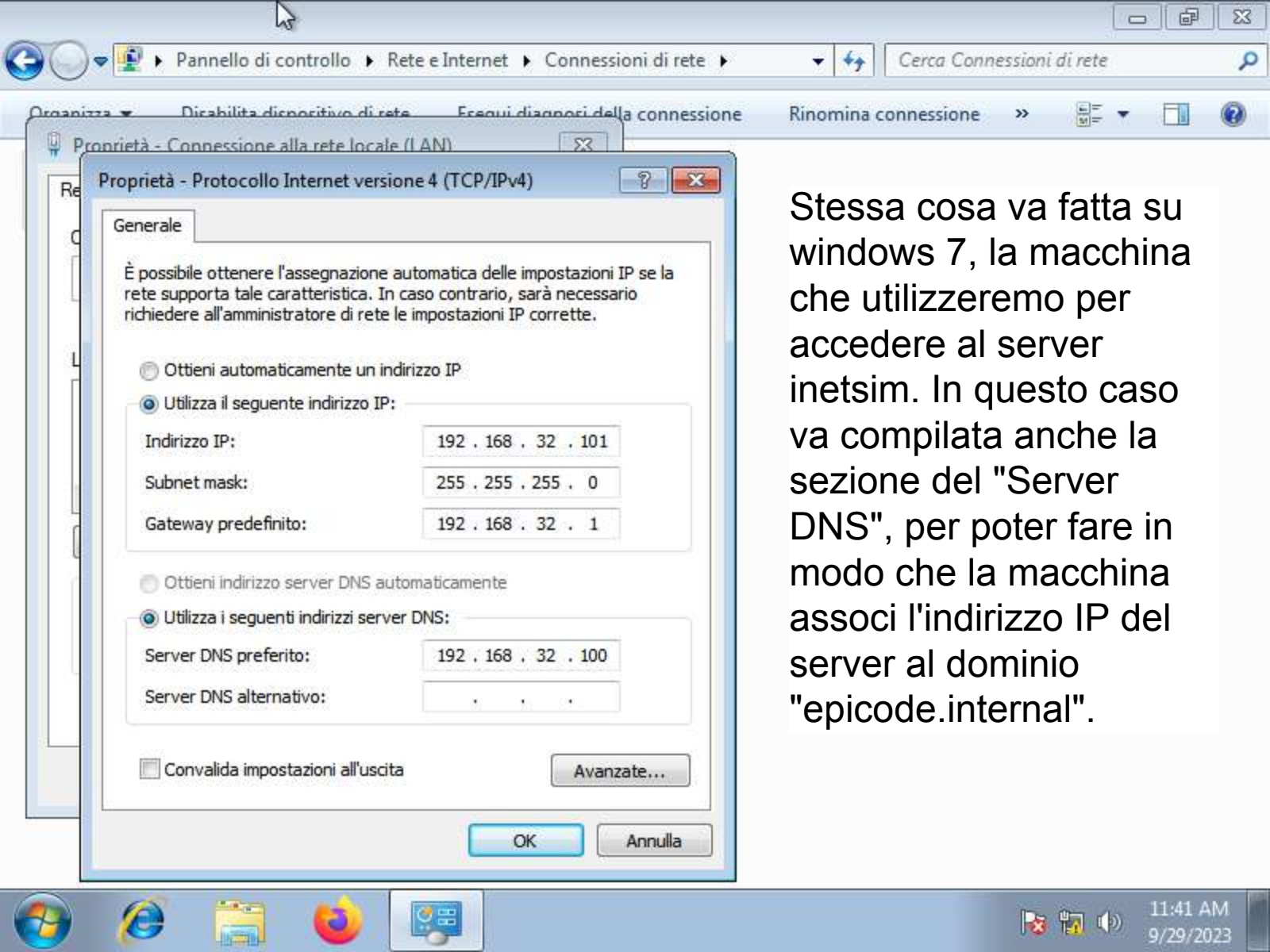
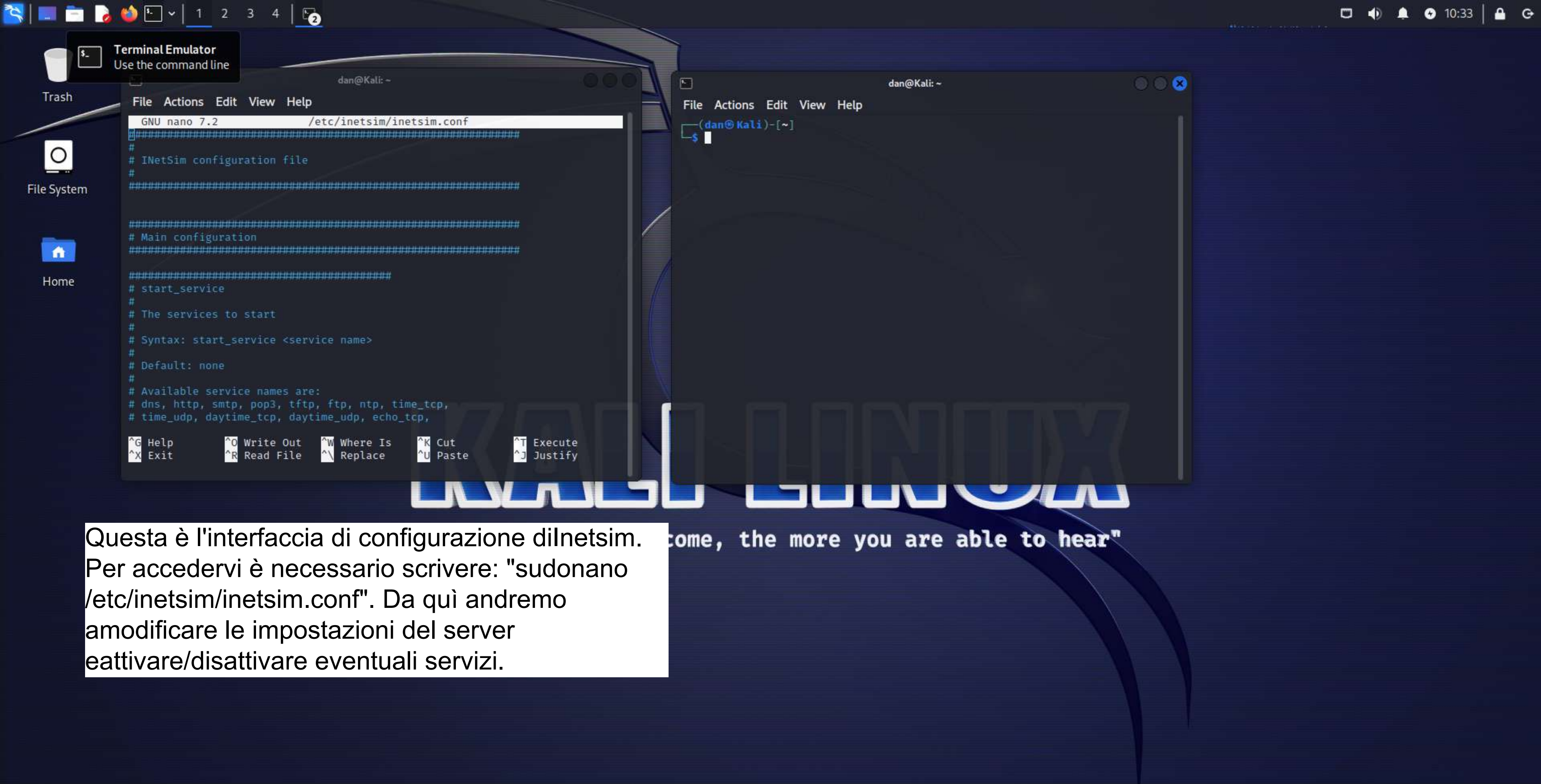


In questo esercizio andremo a creare una connessione tramite "inetsim", un honeypot integrato su Kali Linuux che ci permette di simulare i servizi di un server. Per prima cosa però, bisogna modificare l'indirizzo IP della macchina. Per farlo utilizzeremo il comando: "sudo nano /etc/network/interfaces.d" dove "sudo" ci dà i permessi di amministratore, mentre "nano" è un editor di testo.

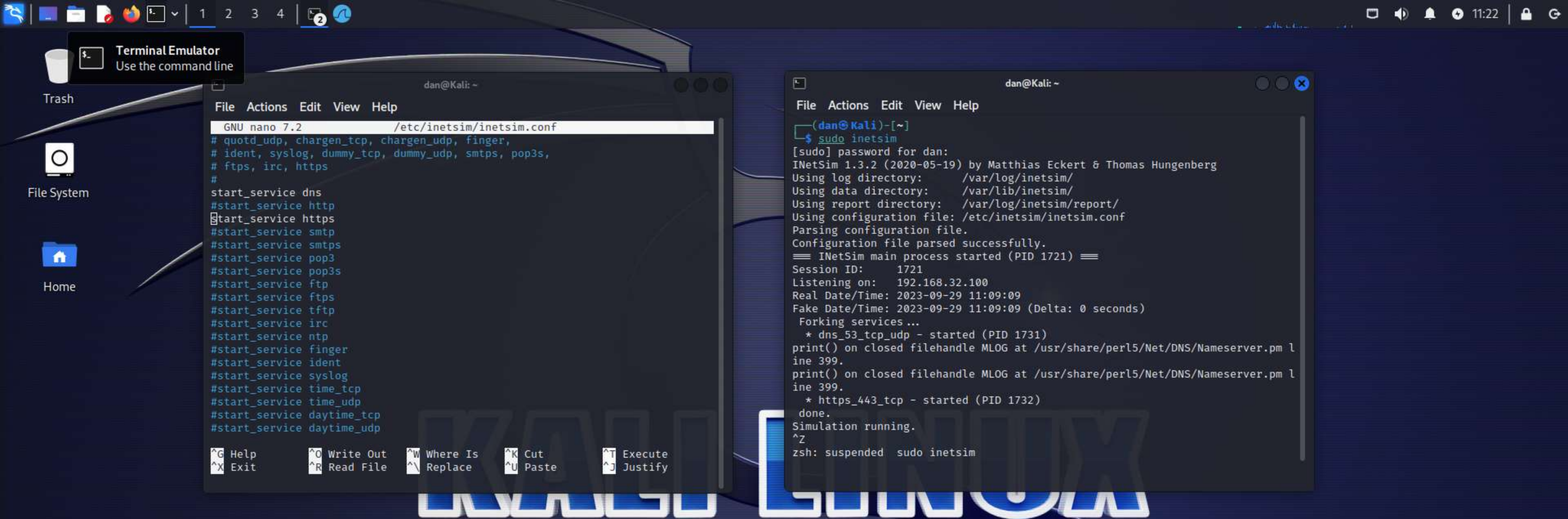


Stessa cosa va fatta su windows 7, la macchina che utilizzeremo per accedere al server inetsim. In questo caso va compilata anche la sezione del "Server DNS", per poter fare in modo che la macchina associ l'indirizzo IP del server al dominio "epicode.internal".



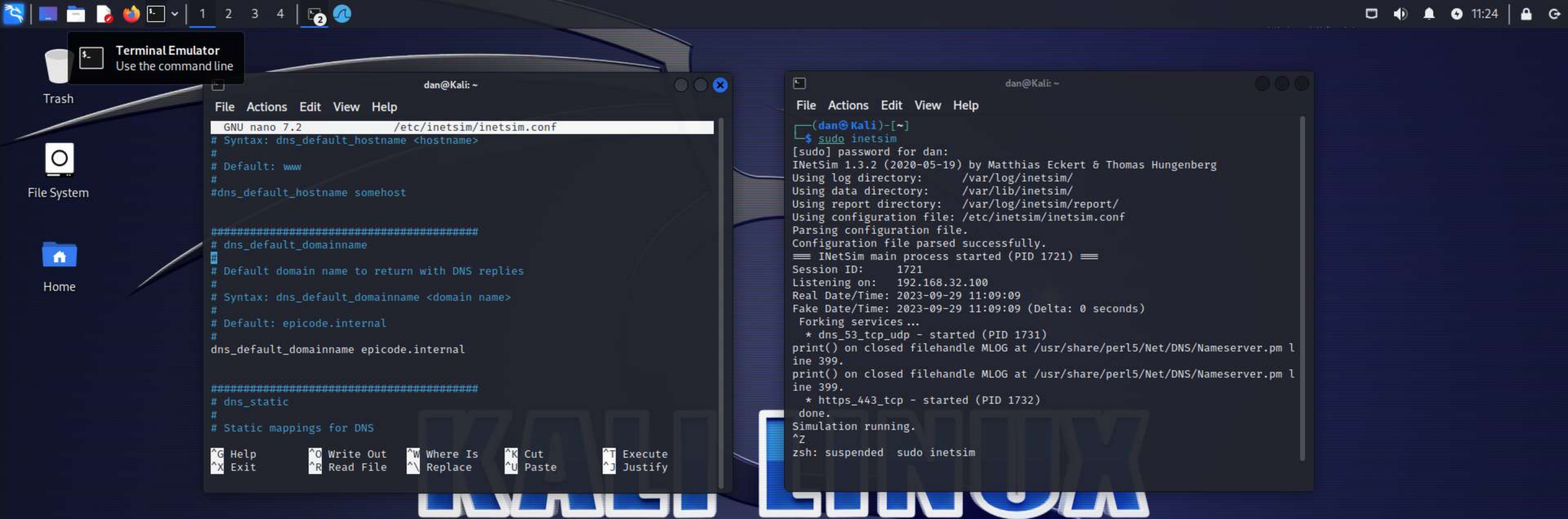


Questa è l'interfaccia di configurazione di inetsim. Per accedervi è necessario scrivere: "sudo nano /etc/inetsim/inetsim.conf". Da qui andremo a modificare le impostazioni del server e attivare/disattivare eventuali servizi.

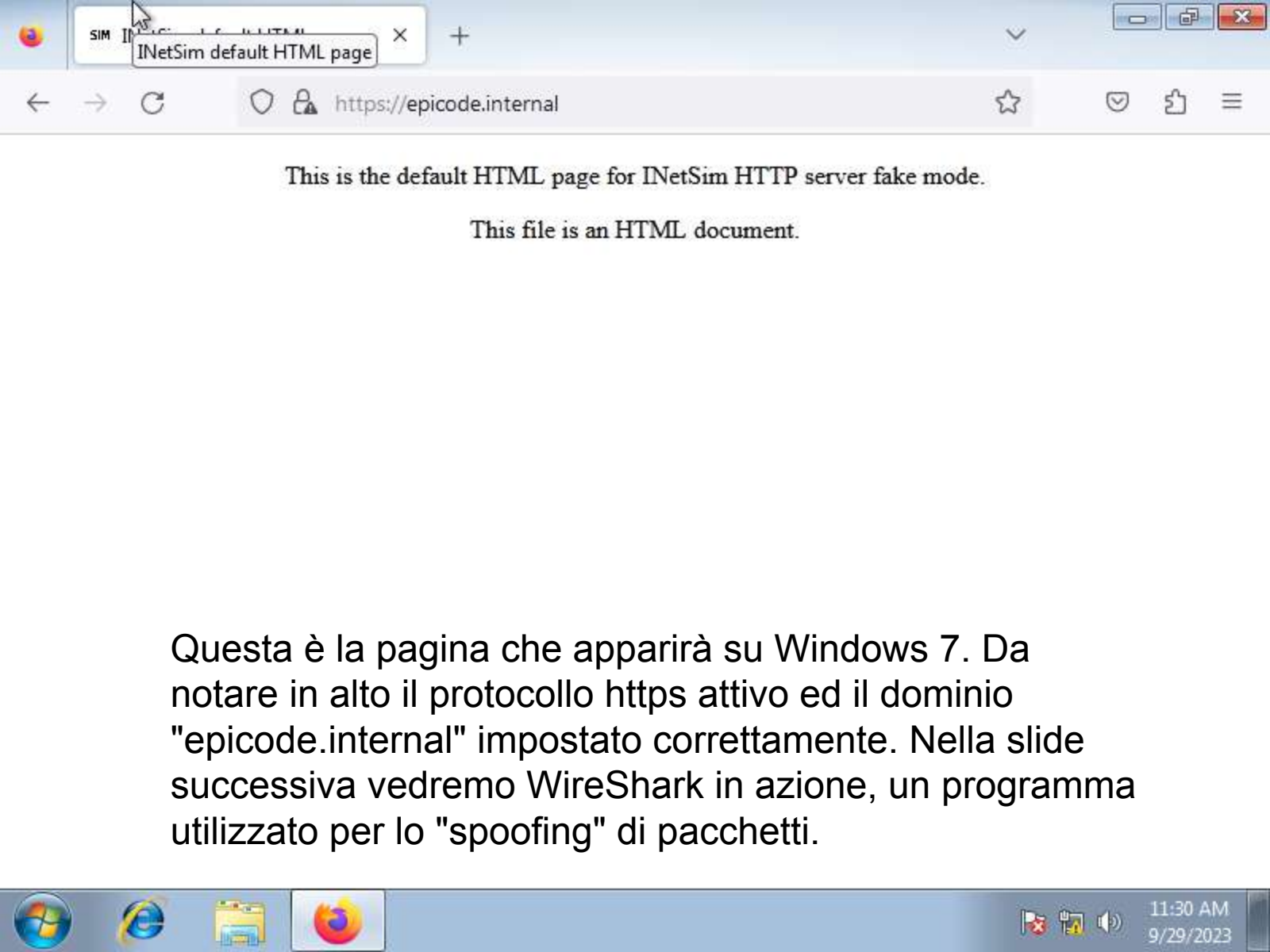


Quella a sinistra è la sezione dei servizi (che si trova nella pagina di configurazione di inetsim) in questo caso andremo ad attivare il servizio dns e https (successivamente proveremo col servizio http). Per farlo, basta usare il "#" prima dello "start\_service" per disattivare o meno un servizio.





Ancora a sinistra, andremo a modificare il dominio, per poter effettivamente associarlo a l'indirizzo IP della macchina Linux. A destra invece c'è inetsim attivato, per farlo basta scrivere "sudo inetsim".

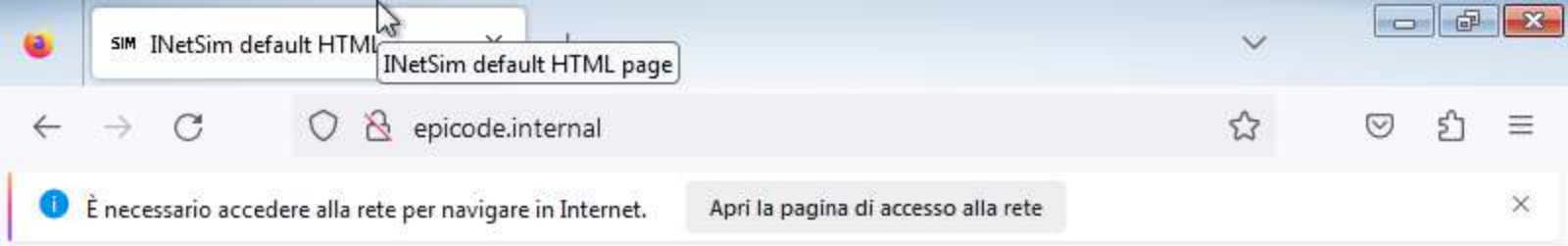


Questa è la pagina che apparirà su Windows 7. Da notare in alto il protocollo https attivo ed il dominio "epicode.internal" impostato correttamente. Nella slide successiva vedremo WireShark in azione, un programma utilizzato per lo "spoofing" di pacchetti.



Da quì si possono vedere tutti i pacchetti trasmessi con gli annessi protocolli. Ciò che ci interessa in questo esercizio è sapere la differenza tra protocollo http ed https. In questo caso (https) si può notare nella zona cerchiata, che le informazioni sono criptate (e pertanto, più sicure).





Questa è la stessa pagina di Windows 7, ma si può notare l'assenza del protocollo https in alto.





Firefox ESR

Browse the World Wide Web

Statistics

Telephony

Wireless

Tools

Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
118	21.173918934	192.168.32.100	192.168.32.101	TCP	204	80 → 49179 [PSH, ACK] Seq=1 Ack=324 Win=64128 Len=150 [TCP segment of a reassembled PDU]
119	21.178543986	192.168.32.100	192.168.32.101	DNS	100	Standard query response 0x3d07 A detectportal.firefox.com A 192.168.32.100
120	21.178564154	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
121	21.178768659	192.168.32.101	192.168.32.100	TCP	60	49179 → 80 [ACK] Seq=324 Ack=410 Win=65280 Len=0
122	21.178872455	192.168.32.101	192.168.32.100	TCP	60	49179 → 80 [FIN, ACK] Seq=324 Ack=410 Win=65280 Len=0
123	21.178880594	192.168.32.100	192.168.32.101	TCP	54	80 → 49179 [ACK] Seq=410 Ack=325 Win=64128 Len=0
124	24.183650934	192.168.32.101	192.168.32.100	DNS	84	Standard query 0xda4d A detectportal.firefox.com
125	24.184050954	192.168.32.101	192.168.32.100	TCP	66	49180 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
126	24.184066802	192.168.32.100	192.168.32.101	TCP	66	80 → 49180 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
127	24.184187989	192.168.32.101	192.168.32.100	TCP	60	49180 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
128	24.184307774	192.168.32.101	192.168.32.100	HTTP	377	GET /canonical.html HTTP/1.1
129	24.184314239	192.168.32.100	192.168.32.101	TCP	54	80 → 49180 [ACK] Seq=1 Ack=324 Win=64128 Len=0
130	24.195104087	192.168.32.100	192.168.32.101	DNS	100	Standard query response 0xda4d A detectportal.firefox.com A 192.168.32.100
131	24.195641863	192.168.32.101	192.168.32.100	DNS	84	Standard query 0x3880 A detectportal.firefox.com
132	24.197134225	192.168.32.100	192.168.32.101	TCP	204	80 → 49180 [PSH, ACK] Seq=1 Ack=324 Win=64128 Len=150 [TCP segment of a reassembled PDU]
133	24.198610039	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
134	24.198745352	192.168.32.101	192.168.32.100	TCP	60	49180 → 80 [ACK] Seq=324 Ack=410 Win=65280 Len=0
135	24.198858069	192.168.32.101	192.168.32.100	TCP	60	49180 → 80 [FIN, ACK] Seq=324 Ack=410 Win=65280 Len=0
136	24.198867401	192.168.32.100	192.168.32.101	TCP	54	80 → 49180 [ACK] Seq=410 Ack=325 Win=64128 Len=0
137	24.207124516	192.168.32.100	192.168.32.101	DNS	100	Standard query response 0x3880 A detectportal.firefox.com A 192.168.32.100

Frame 133: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu\_d8:eb:37 (08:00:27:d8:eb:37), Dst: PcsCompu\_cf:c3:0c (08:00:27:cf:c3:0c)

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101

Transmission Control Protocol, Src Port: 80, Dst Port: 49180, Seq: 151, Ack: 324, Len: 258

[2 Reassembled TCP Segments (408 bytes): #132(150), #133(258)]

Hypertext Transfer Protocol

Line-based text data: text/html (10 lines)

0000 08 00 27 cf c3 0c 08 00 27 d8 eb 37 08 00 45 00

0010 01 2a 33 32 40 00 40 06 44 82 c0 a8 20 64 c0 a8

0020 20 65 00 50 c0 1c 5f b2 7c 7a c0 73 57 96 50 19

0030 01 f5 c3 36 00 00 3c 68 74 6d 6c 3e 0a 20 20 3c

0040 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65

0050 3e 49 4e 65 74 53 69 6d 20 64 65 66 61 75 6c 74

0060 20 48 54 4d 4c 20 70 61 67 65 3c 2f 74 69 74 6c

0070 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c

0080 62 6f 64 79 3e 0a 20 20 20 20 3c 70 3e 3c 2f 70

0090 3e 0a 20 20 20 20 3c 70 20 61 6c 69 67 6e 3d 22

00a0 63 65 6e 74 65 72 22 3e 54 68 69 73 20 69 73 20

00b0 74 68 65 20 64 65 66 61 75 6c 74 20 48 54 4d 4c

00c0 20 70 61 67 65 20 66 6f 72 20 49 4e 65 74 53 69

00d0 6d 20 48 54 54 50 20 73 65 72 76 65 72 20 66 61

00e0 6b 65 20 6d 6f 64 65 2e 3c 2f 70 3e 0a 20 20 20

00f0 20 3c 70 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65

0100 72 22 3e 54 68 69 73 20 66 69 6c 65 20 69 73 20

0110 61 6e 20 48 54 4d 4c 20 64 6f 63 75 6d 65 6e 74

0120 2e 3c 2f 70 3e 0a 20 20 3c 2f 62 6f 64 79 3e 0a

0130 3c 2f 68 74 6d 6c 3e 0a

Frame (312 bytes)

Reassembled TCP (408 bytes)

Packets: 137 · Displayed: 137 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

Col protocollo http, sta volta, si può notare in basso a destra che le informazioni sono leggibili. In questo caso possiamo leggere effettivamente l'intestazione della pagina in html. Evidenziando la differenza tra https ed http.