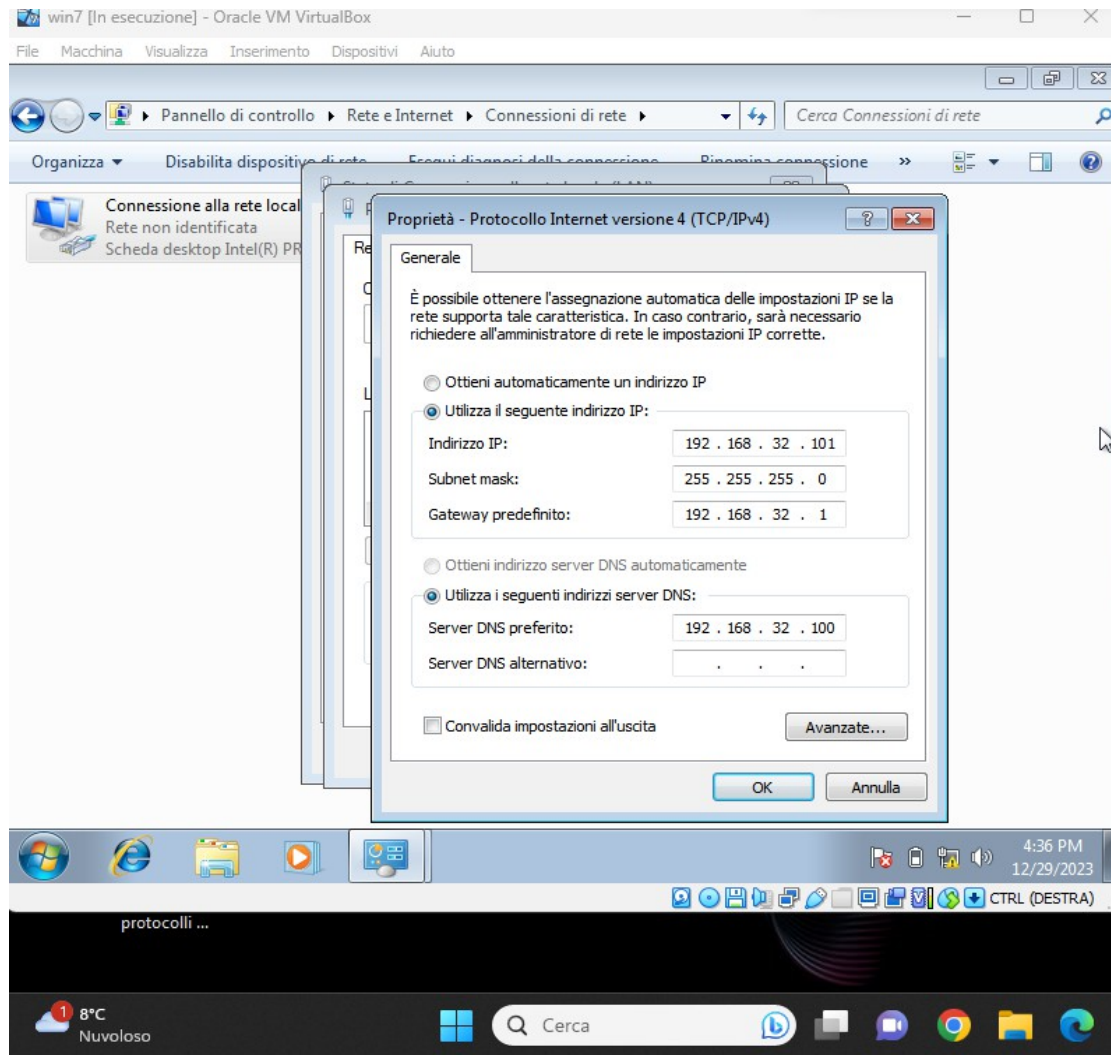


ESERCITAZIONE PRATICA W4D4

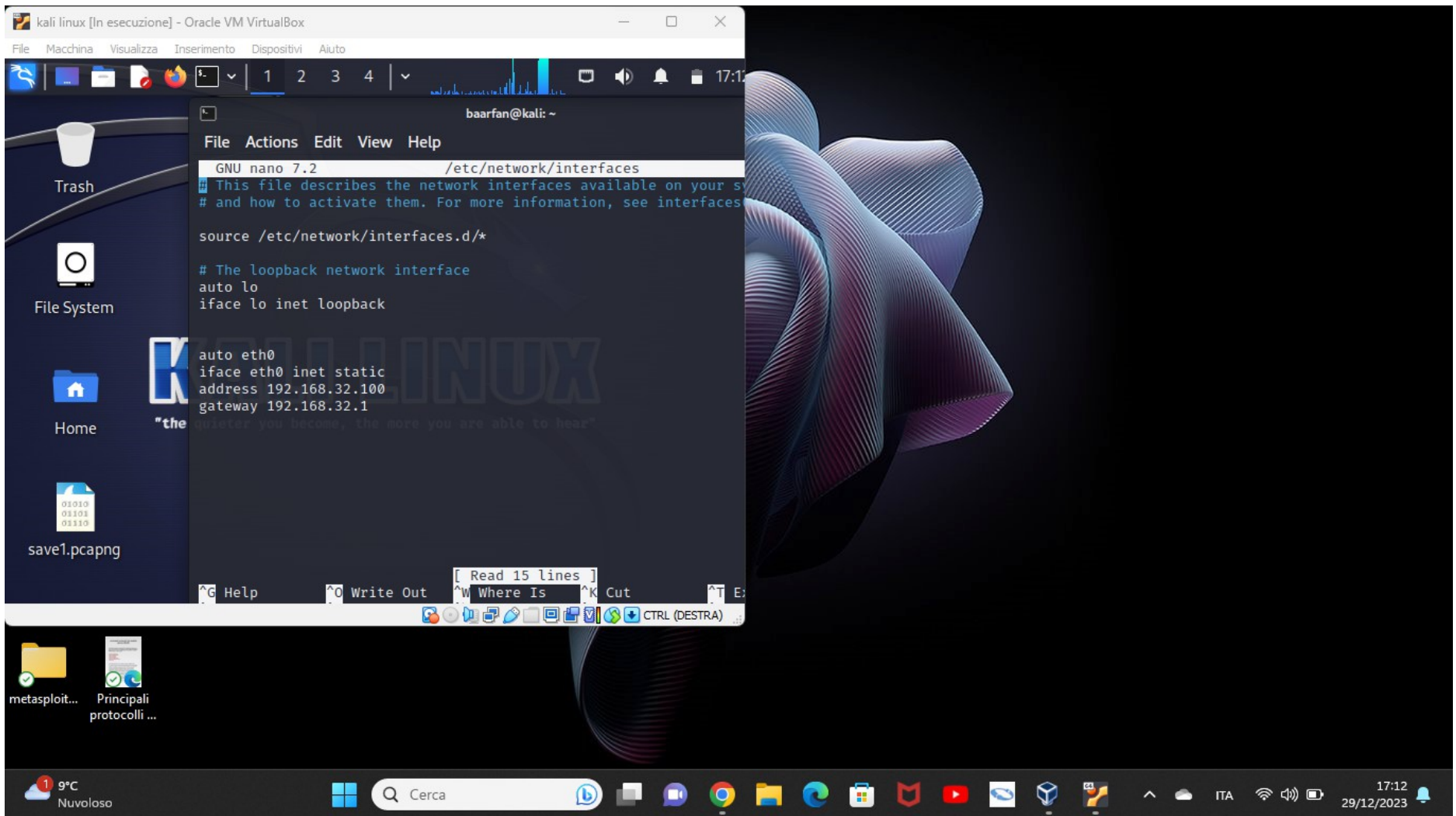
REQUISITI E SERVIZI

- KALI LINUX □ □ IP 192.168.32.100
- WINDOWS 7 □ □ IP 192.168.32.101
- HTTPS SERVER: ATTIVO
- SERVIZIO DNS PER RISOLUZIONE NOMI DI DOMINIO: ATTIVO

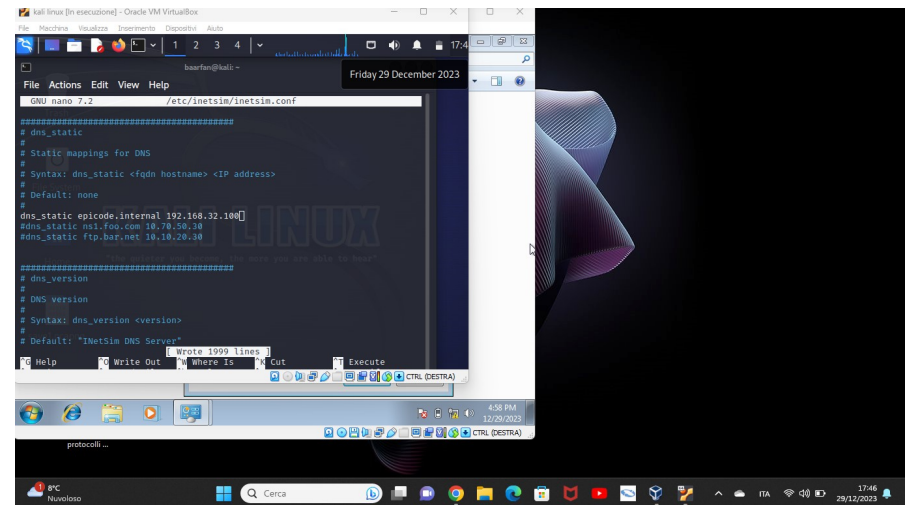
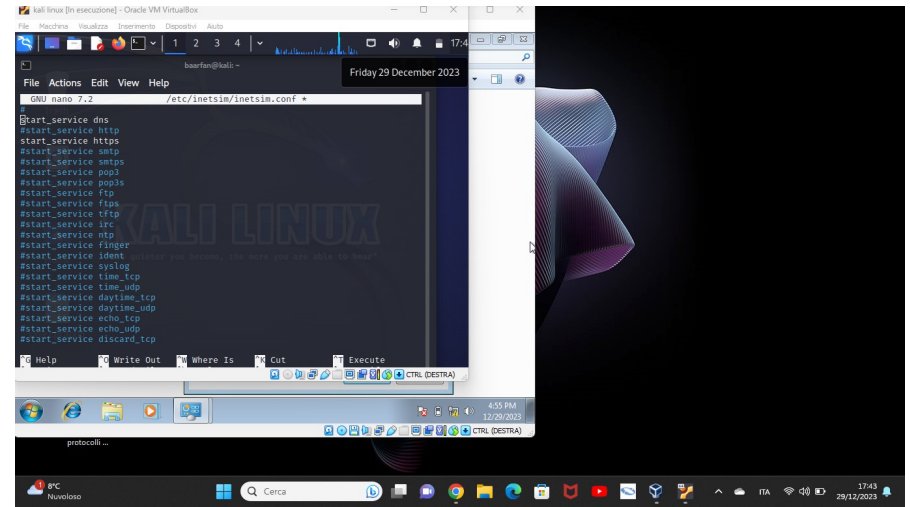
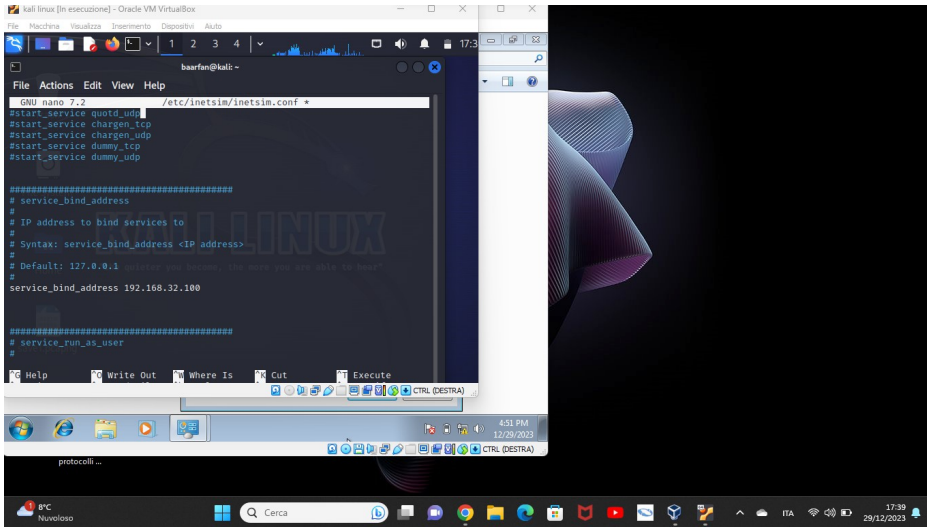
CONFIGURAZIONE SCHEDA DI RETE DI WIN 7



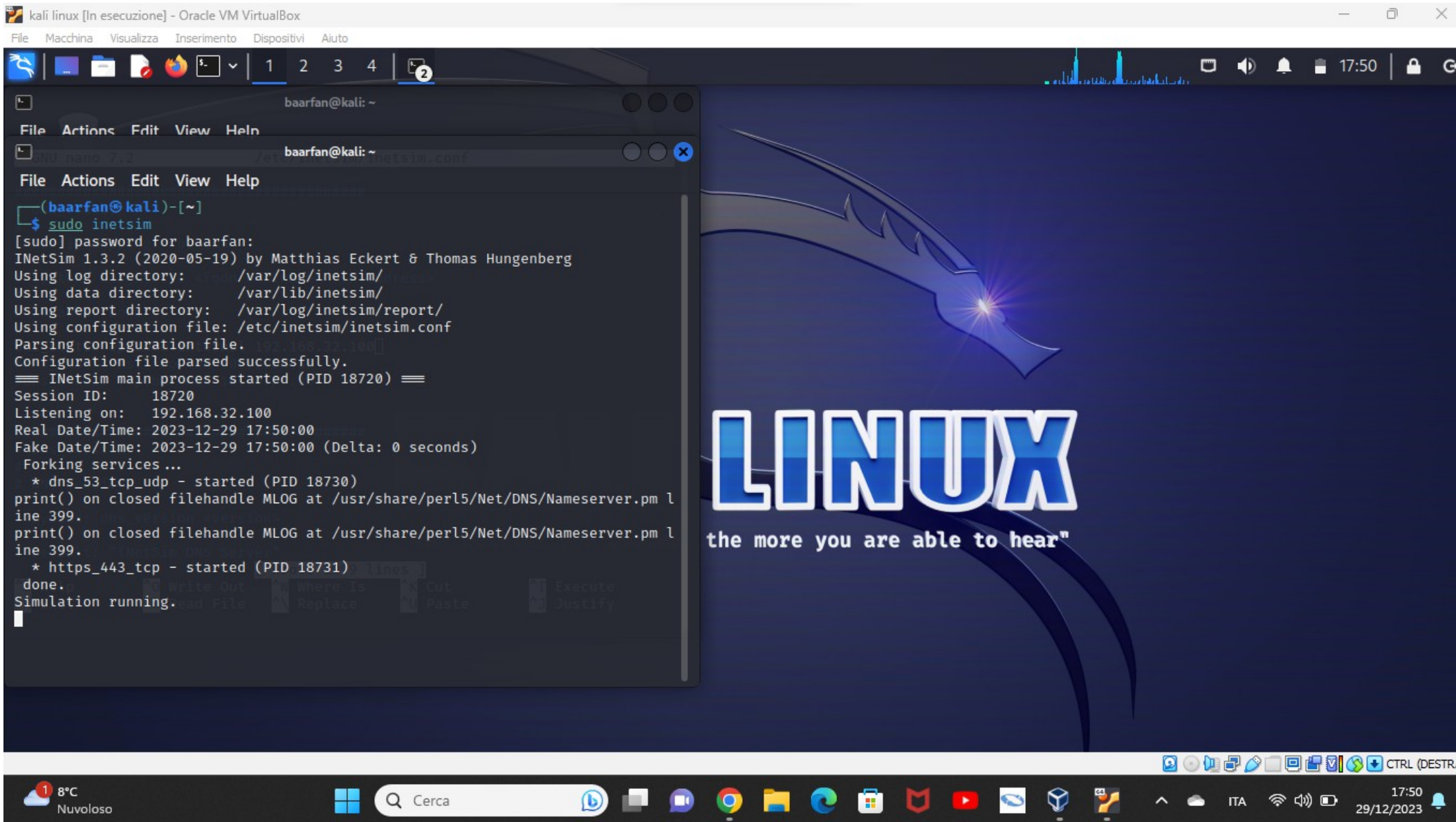
CONFIGURAZIONE IP DI KALI LINUX



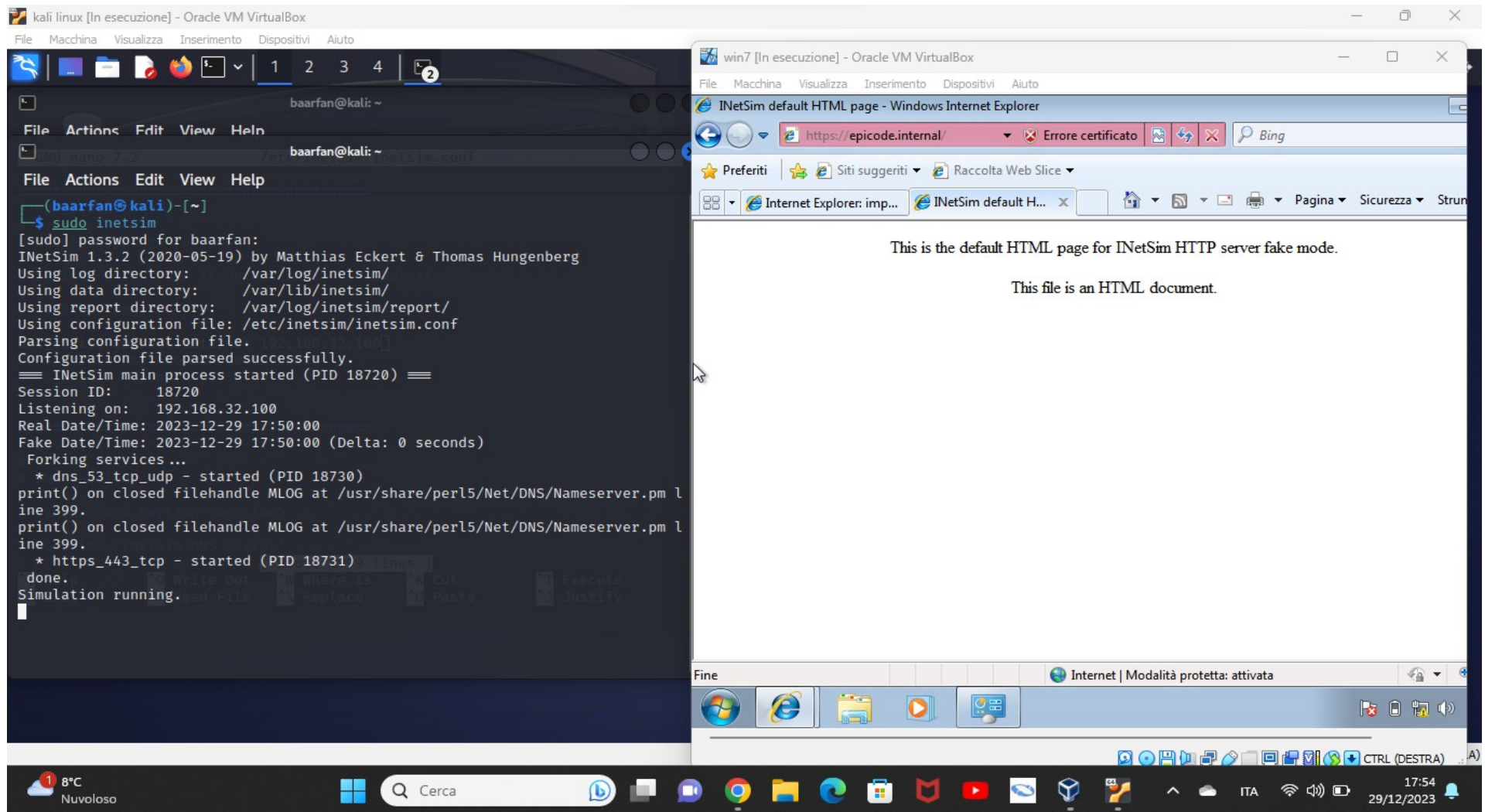
CONFIGURAZIONE INETSIM DNS & HTTPS



AVVIO SIMULAZIONE INETSIM



TEST CON WIN 7 (PAGINA EPICODE.INTERNAL)



CATTURA WIRESHARK HTTPS

The screenshot displays a Kali Linux virtual machine environment. On the left, a terminal window shows the execution of `sudo inetSim`. The output indicates that InetSim 1.3.2 is running, listening on 192.168.32.100, and has started services for `dns_53_tcp_udp` (PID 18730) and `https_443_tcp` (PID 18731). The simulation is running.

On the right, the Wireshark network protocol analyzer is open, capturing traffic from the `eth0` interface. The packet list shows several packets, with packet 9 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP).

No.	Time	Source	Destination	Protocol	Length	Info
3	0.002386250	192.168.32.101	192.168.32.100	DNS	71	Standard query
4	0.106148867	192.168.32.100	192.168.32.101	DNS	71	Standard query
5	5.349271836	PcsCompu_f4:f0:dd	PcsCompu_83:28:ee	ARP	42	Who has 192.168.32.100
6	5.350683515	PcsCompu_83:28:ee	PcsCompu_f4:f0:dd	ARP	60	192.168.32.100
7	27.351086263	192.168.32.101	192.168.32.100	TCP	66	61134 → 443 [
8	27.352066393	192.168.32.100	192.168.32.101	TCP	66	443 → 61134 [
9	27.354338111	192.168.32.101	192.168.32.100	TCP	60	61134 → 443 [
10	27.355714757	192.168.32.101	192.168.32.100	TLSv1	210	Client Hello

The packet details for the selected packet (Frame 9) show the following structure:

- Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0
- Ethernet II, Src: PcsCompu_83:28:ee (08:00:27:f4:f0:dd), Dst: PcsCompu_f4:f0:dd (08:00:27:83:28:ee)
- Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
- Transmission Control Protocol, Src Port: 61134, Dst Port: 443

The status bar at the bottom of the Wireshark window indicates: `eth0: <live capture in progress>`, `Packets: 44 · Displayed: 44 (100.0%)`, and `Profile: Default`.

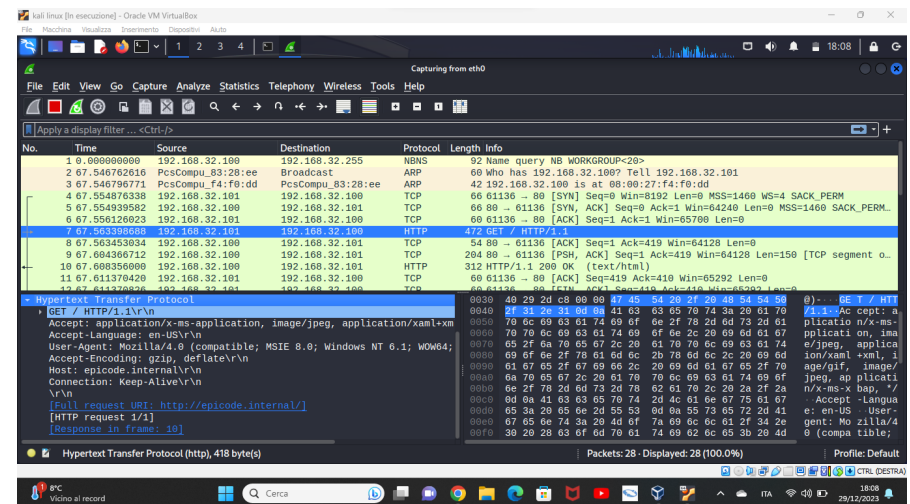
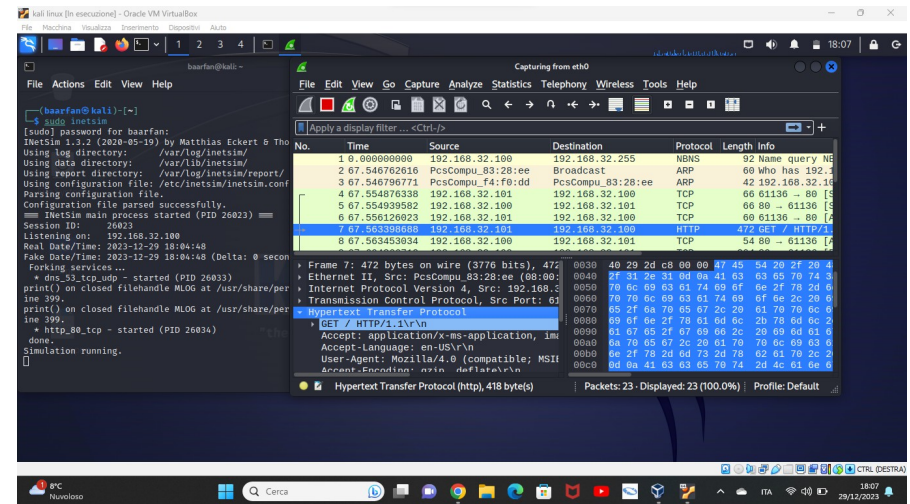
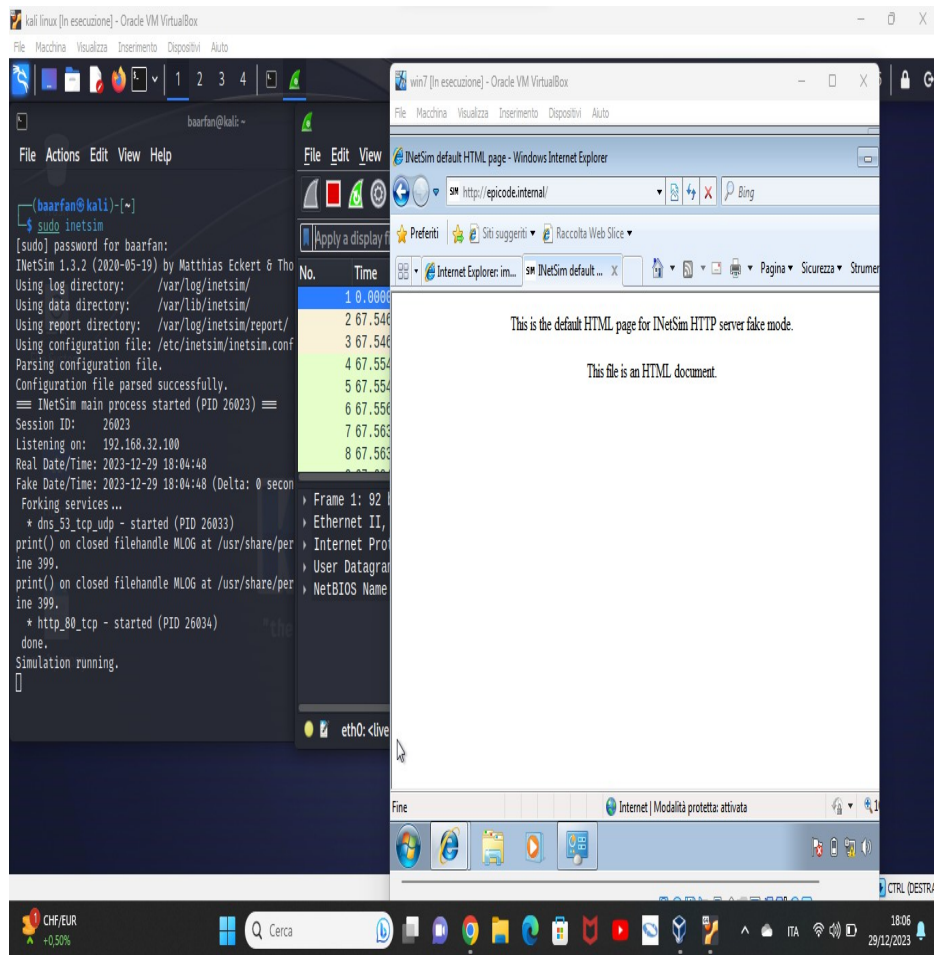
TEST ABILITANDO PROTOCOLLO HTTP E NON HTTPS

The screenshot displays a Kali Linux virtual machine environment. In the foreground, a terminal window shows the configuration of the inetsim service. The configuration file `/etc/inetsim/inetsim.conf` is being edited with nano. The configuration includes enabling various services like dns, http, smtp, and ftp. The `start_service http` command has been executed, and the service is running on port 80.

In the background, the Wireshark network protocol analyzer is open, capturing traffic on the `eth0` interface. The packet list shows several DNS and TCP packets. A dialog box is visible, asking to save the captured packets before starting a new capture. The dialog has two buttons: "Continue without Saving" and "Cancel".

The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 18:03 on 29/12/2023.

CATTURA CON WIRESHARK HTTP



DRAME BA ARPHANG CSPT04 W4D4

CONSIDERAZIONI

ATTRAVERSO LA CONFIGURAZIONE DI INETSIM E LA CONSEGUENTE CATTURA D'IMMAGINI SULL'APPLICAZIONE ABBIAMO AVUTO MODO DI EVIDENZIARE COME LAVORANO I PROTOCOLLI INTERNET HTTPS ED HTTP; VIENE CHIARAMENTE RISCONTRATO COME IL PRIMO OPERI CIFRANDO I PROPRI PACCHETTI, A DIFFERENZA DEL PROTOCOLLO HTTP CHE HA UNA PROTEZIONE MOLTO PIU LEGGERA E PERMETTA LA LETTURA CHIARA DI MOLTI Più ELEMENTI.