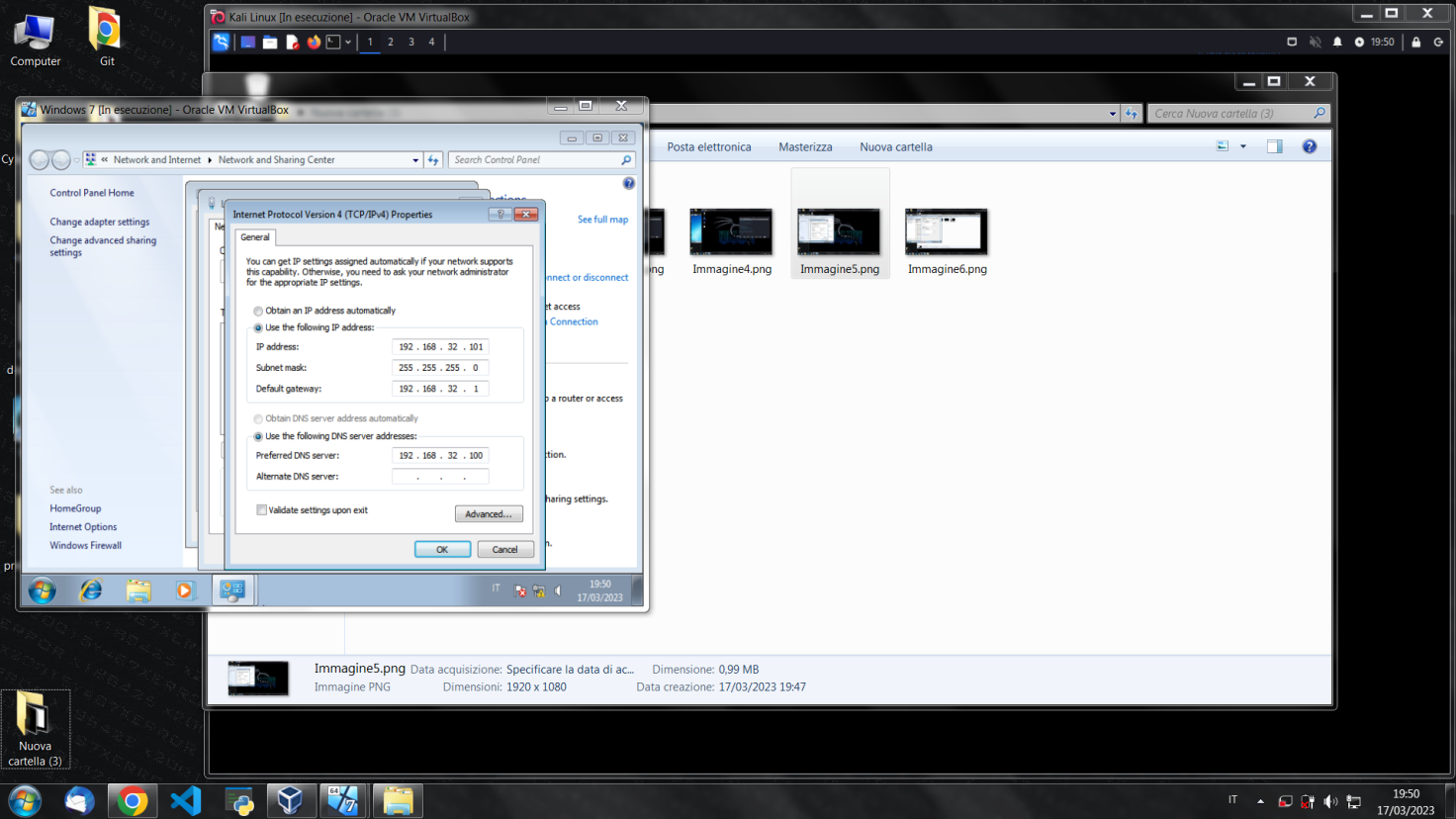
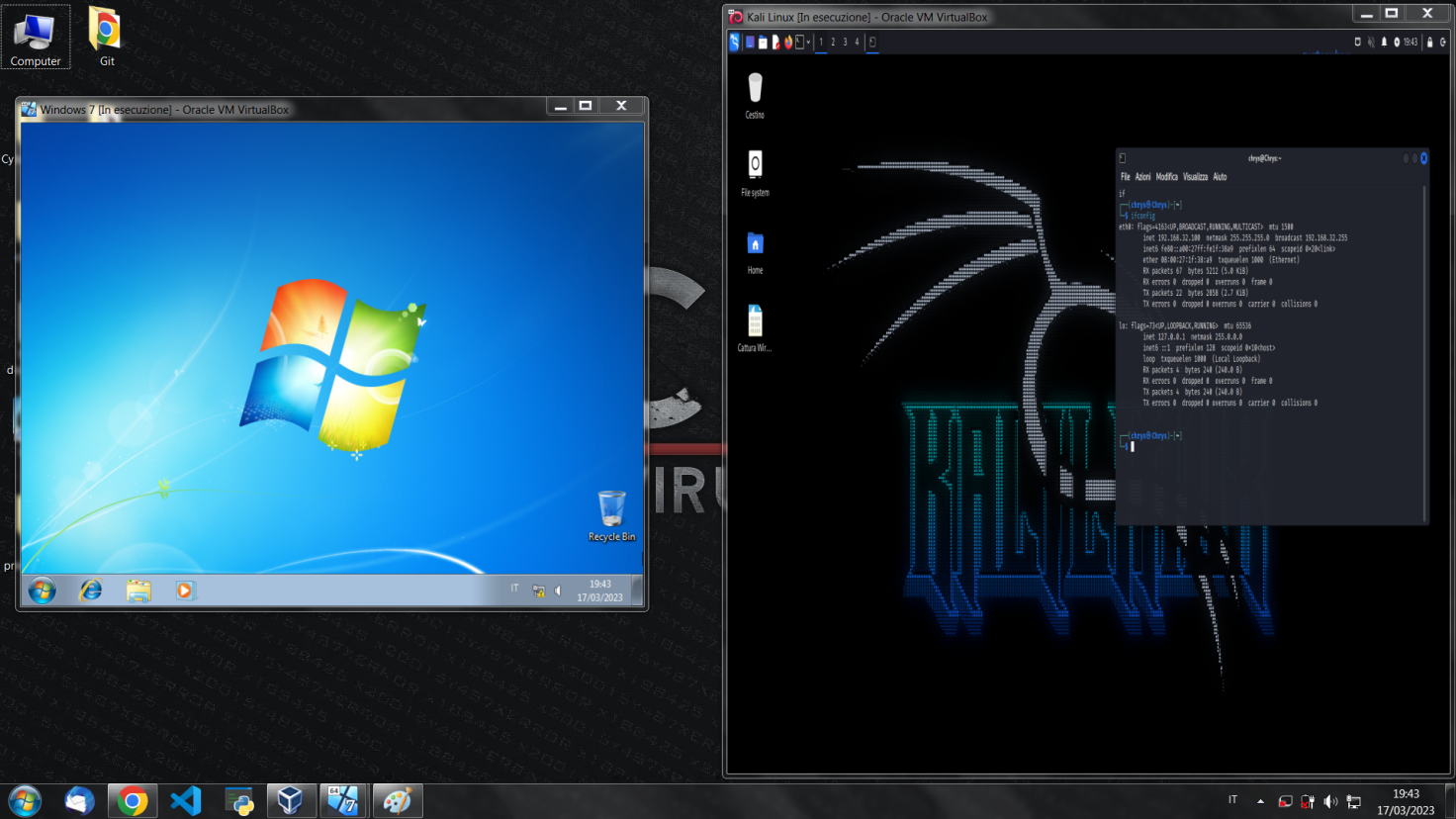
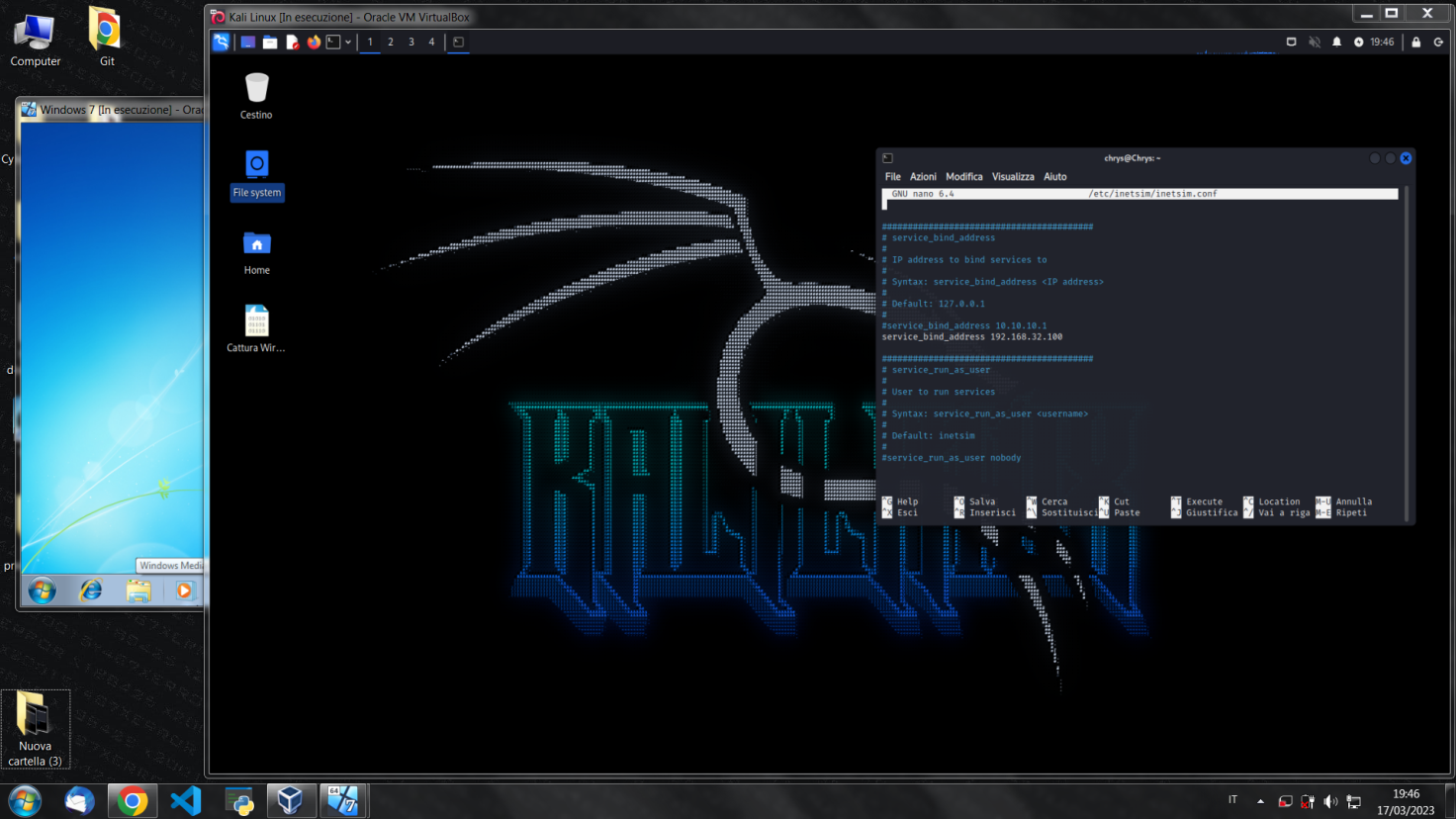
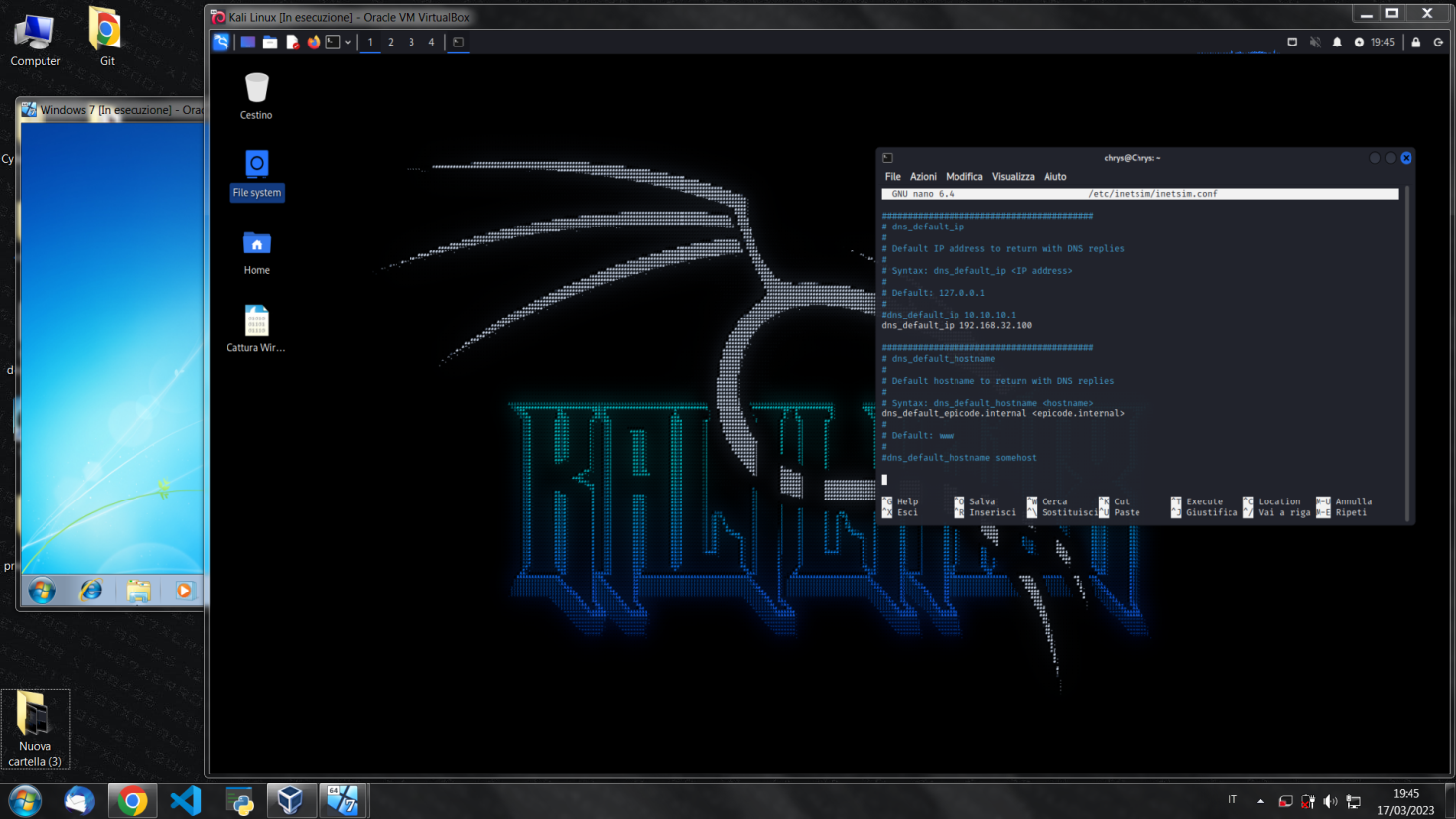
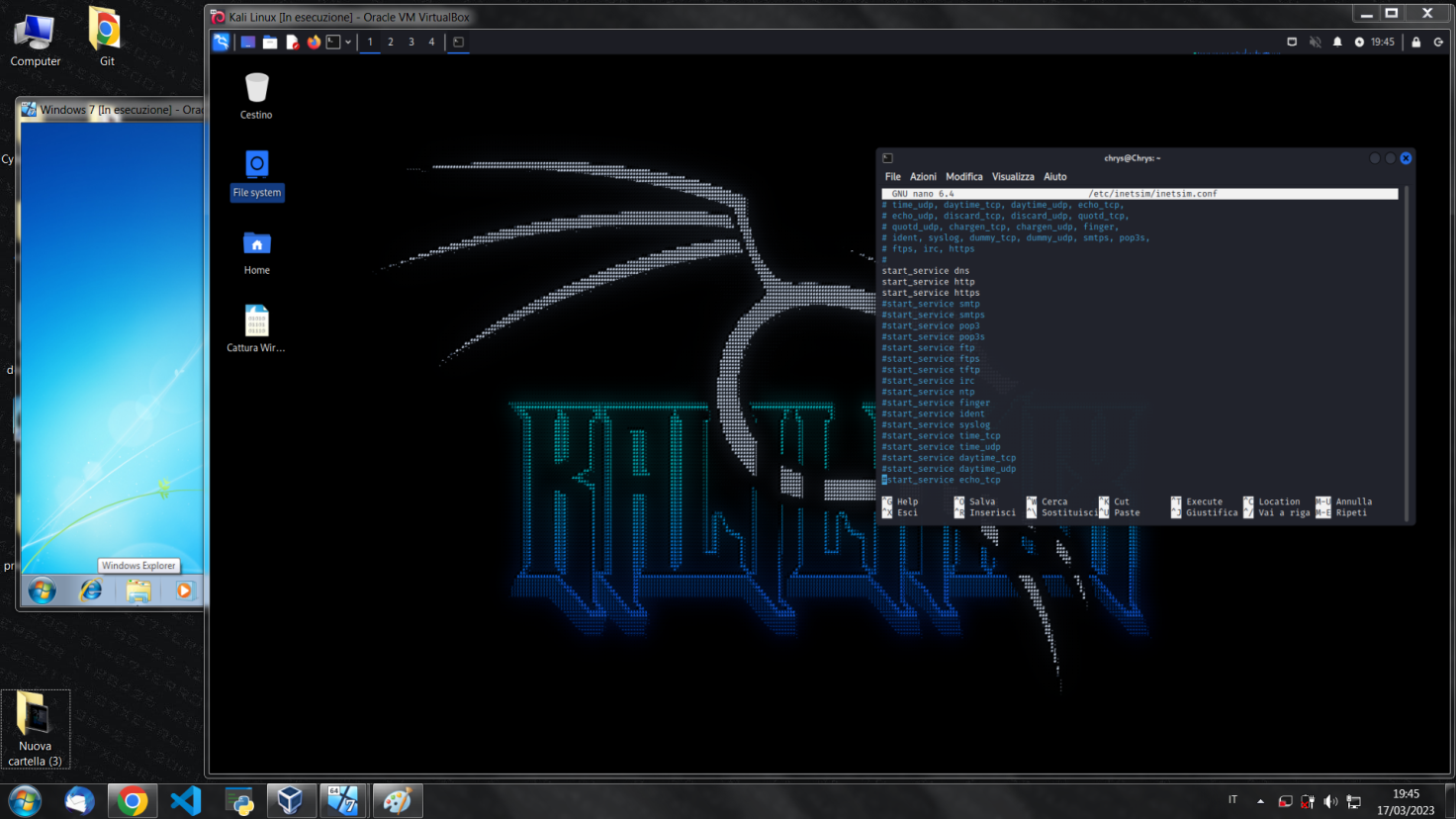
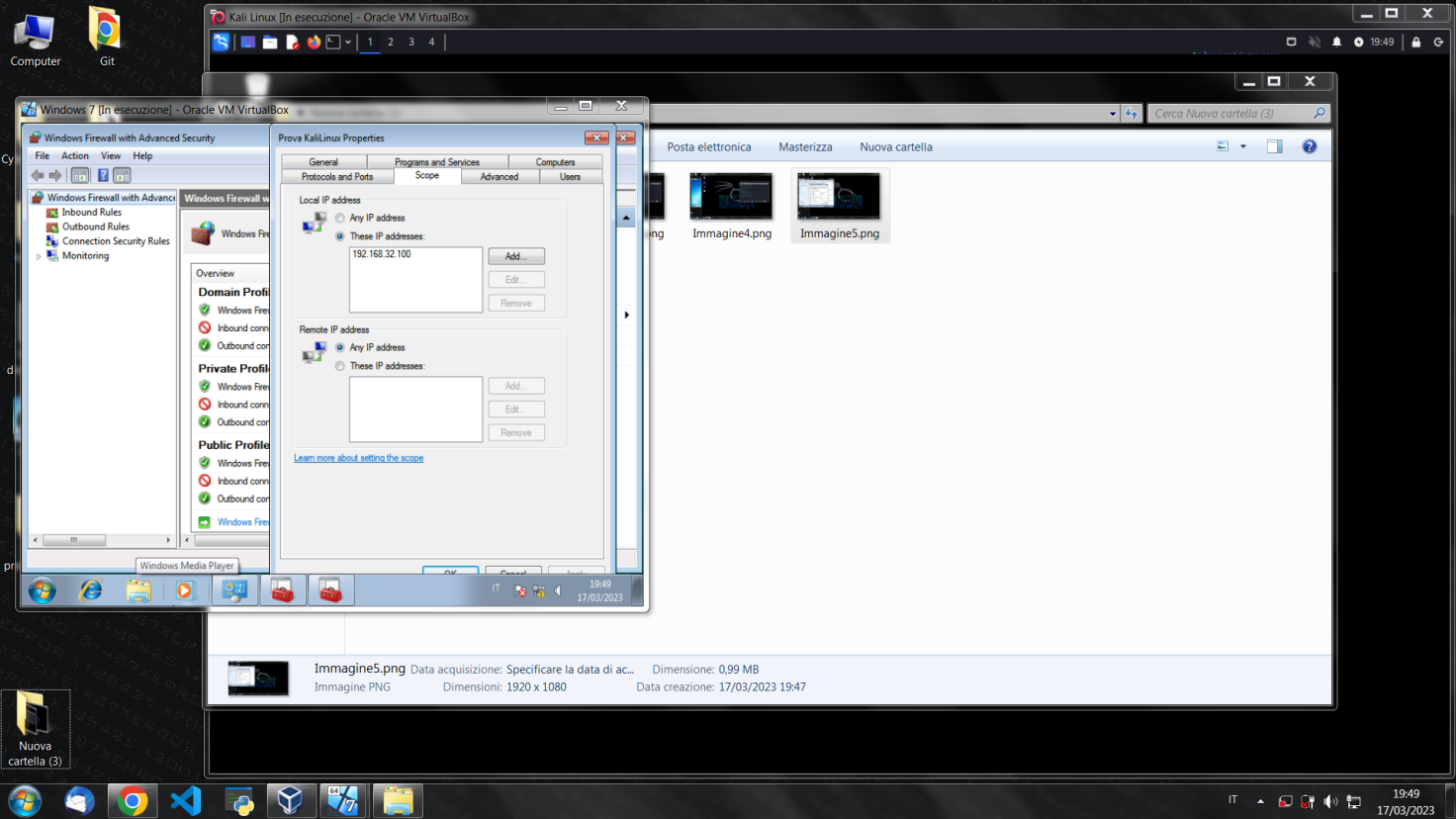
1. Avvio delle macchine virtuali con il successivo settaggio dei parametri Ip,Gateway e Subnetmask degli ambienti virtuali.

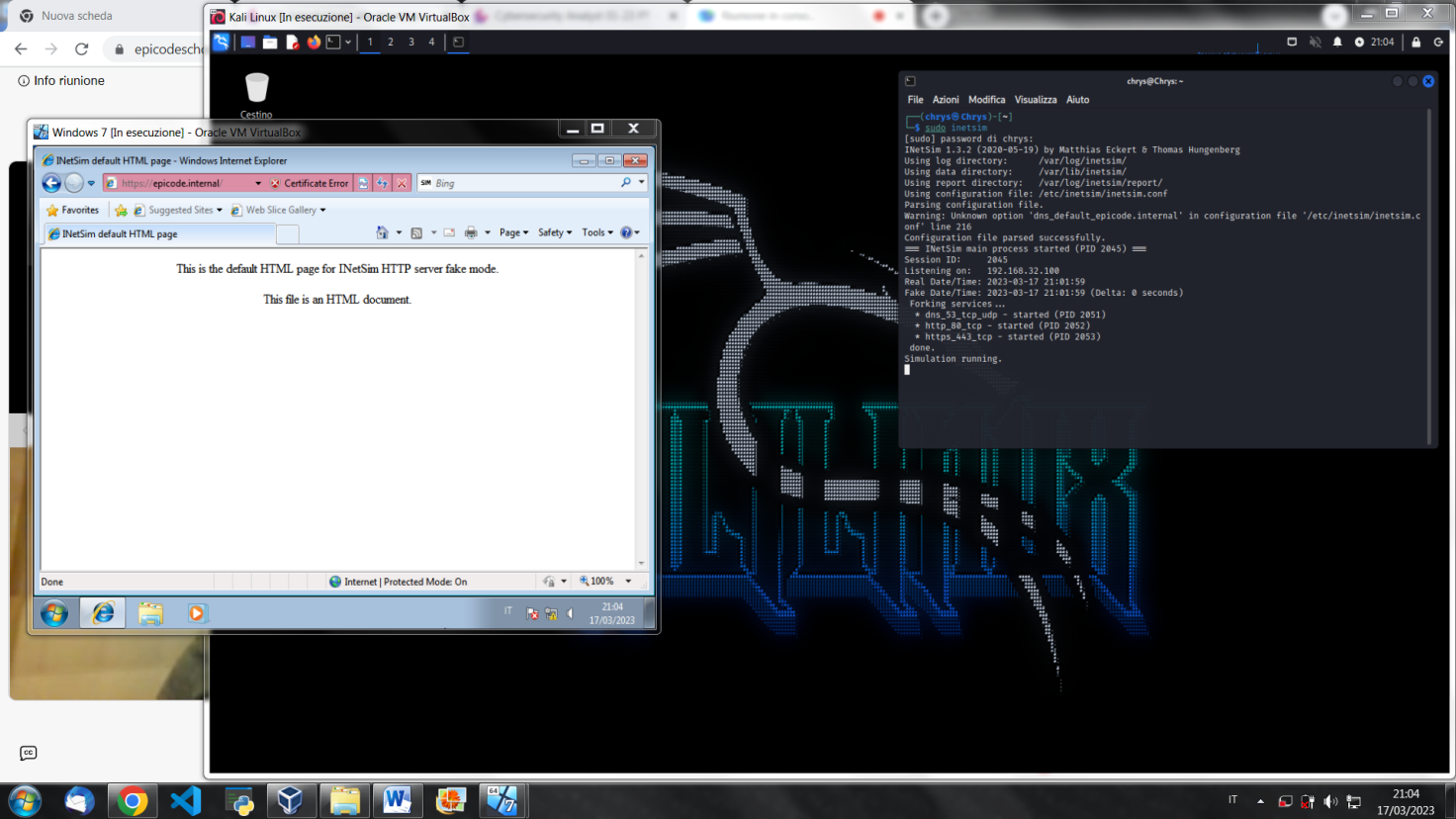
2)Chiamata del comando “ sudo nano /etc/inetsim/inetsim.conf “ per la modifica e abilitazione dei protocolli di nostro interesse per la corretta comunicazione tra le macchine.

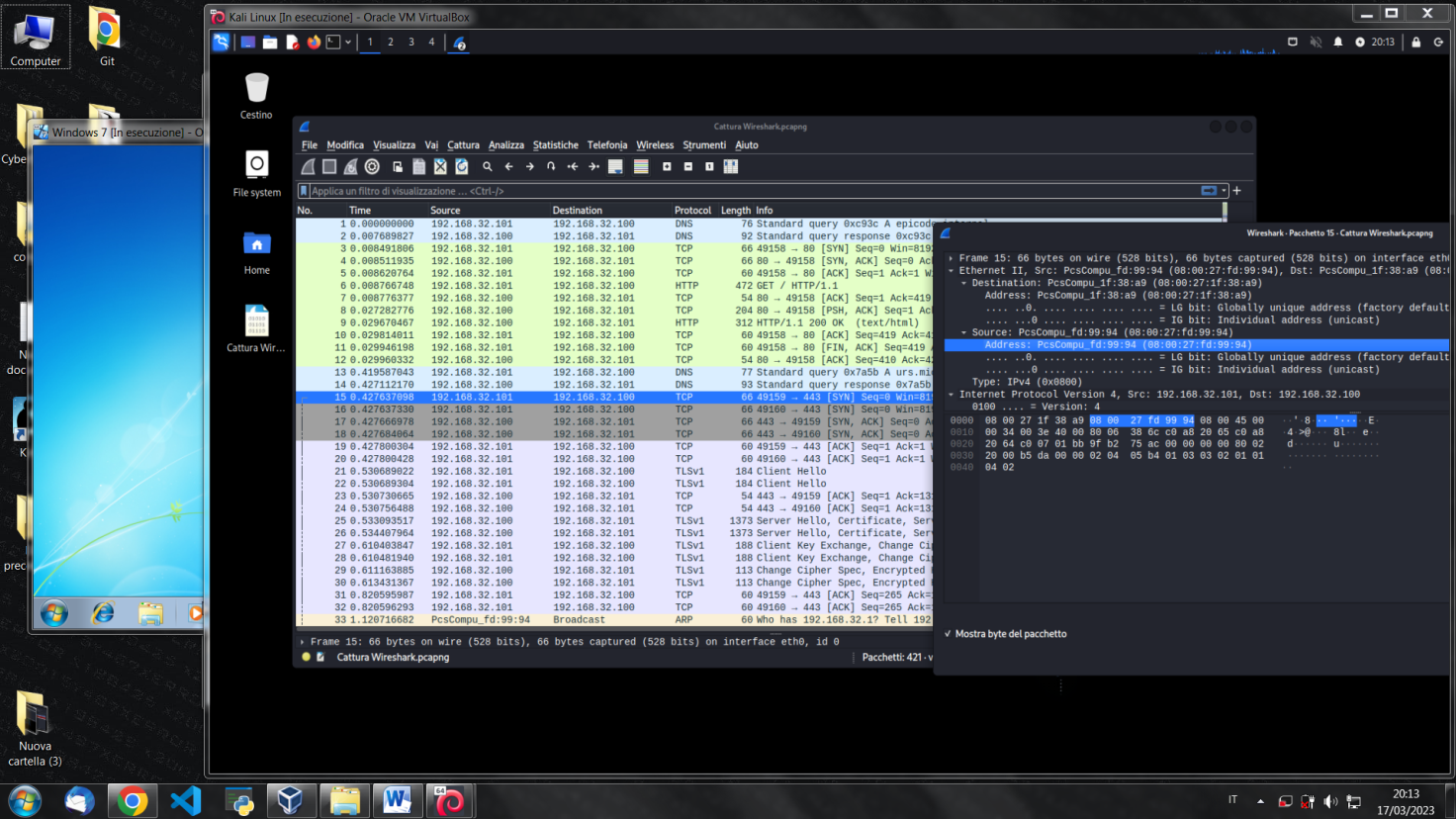
3)Impostato come DNS l’indirizzo Ip di Kali per permettere la chiamata di questo indirizzo sulla macchina Windows 7 e impostato anche il valore “ epicode.internal “ nel campo hostname,per la chiamata epicode.internal direttamente da Browser.

4)Abilitazione/disabilitazione dei servizi attraverso il carattere “ # “,in questo caso andremo ad abilitare solo i servizi pertinenti al completamento del nostro esercizio,abilitando solo DNS,HTTP,HTTPS.

5)Concessione di permessi di accesso ”interrogazione” alla macchina Windows da parte di KaliLinux attraverso l inserimento dell Ip Kali nella lista degli Ip a cui dare libero accesso nel settaggio avanzato del Firewall.

6)Avvio di Inetsim in KaliLinux attraverso il comando “ sudo inetsim “ che ci permetterà appunto di poter interrogare il DNS di Kali attraverso il Browser della macchina Windows.

* Questo è il caso d interrogazione ‘ epicode.internal ‘ con protocollo http.
* Caso interrogazione ‘ epicode.internal ‘ con protocollo https.

7)Esecuzione di WireShark su Kali con interrogazione di “ epicode.internal “ sul browser di Windows per il controllo dei protocolli che si attivano. Esempio HTT

Esempio protocollo HTTPS.