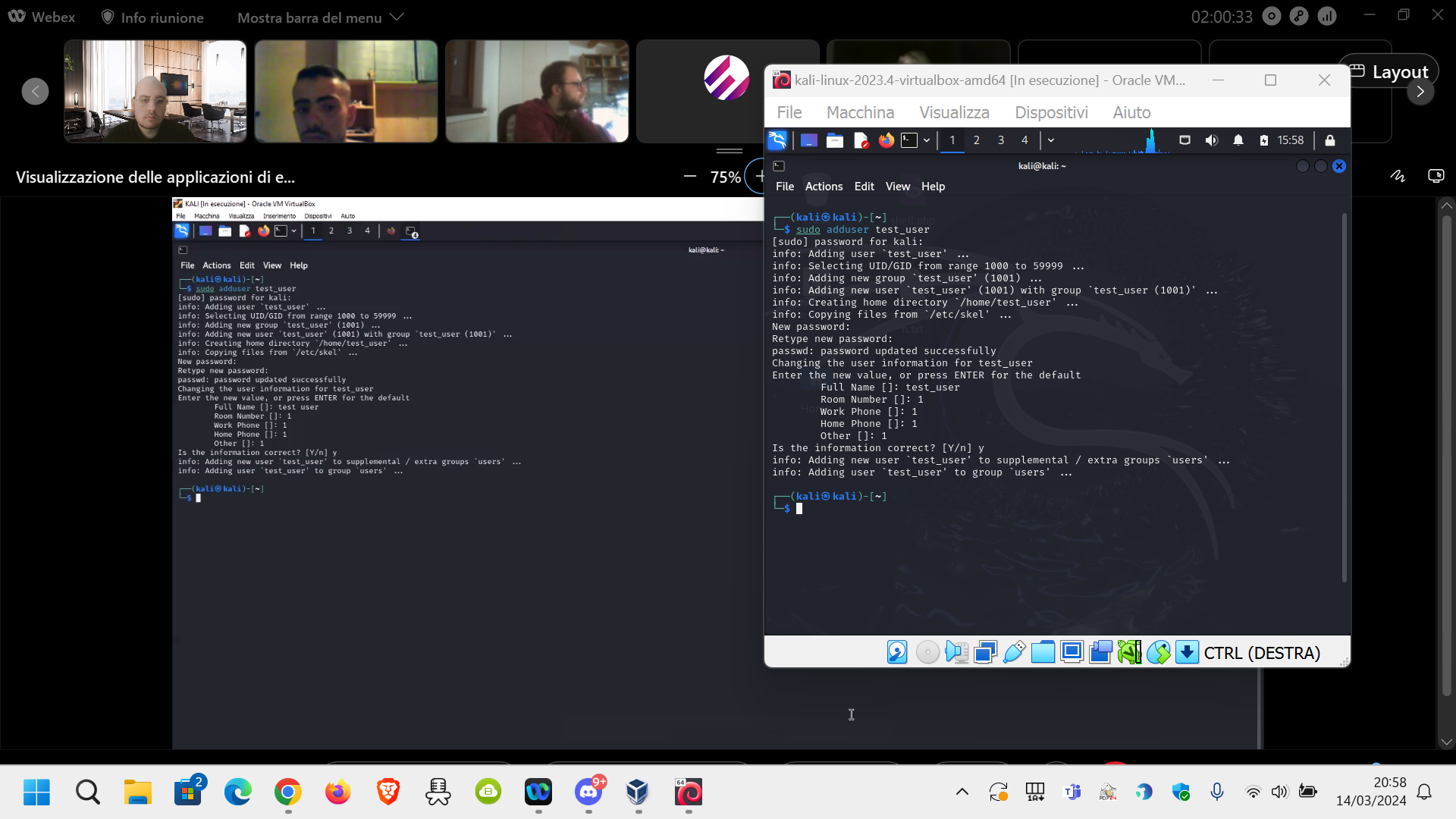
ESERCIZIO W14D4

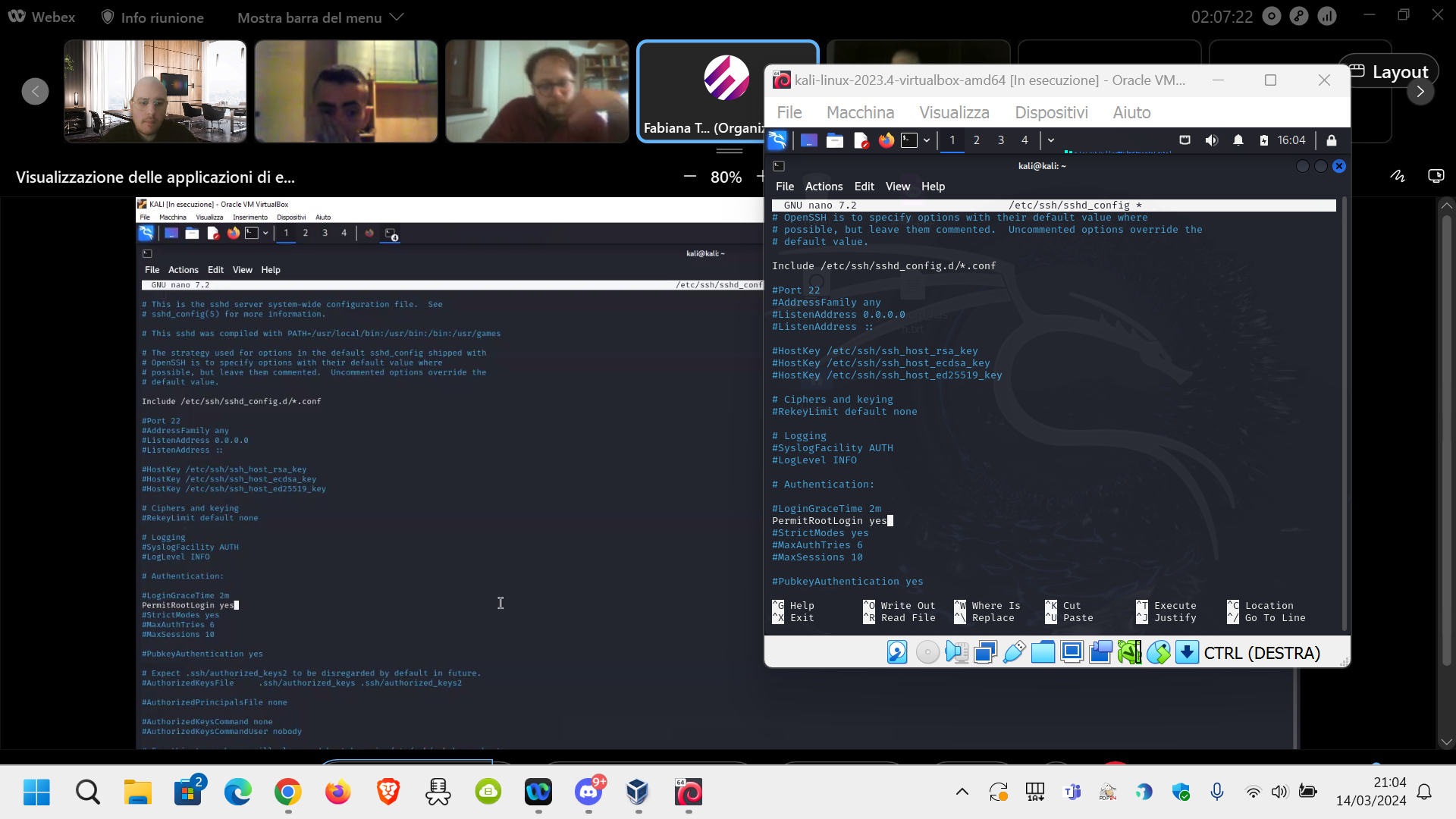
**Report dell'Esercizio di Configurazione e Cracking SSH con Hydra**

Nell'esercizio di oggi, abbiamo affrontato due obiettivi principali: fare pratica con Hydra per craccare l'autenticazione dei servizi di rete e consolidare le conoscenze dei servizi stessi tramite la loro configurazione. L'esercizio è stato suddiviso in due fasi.

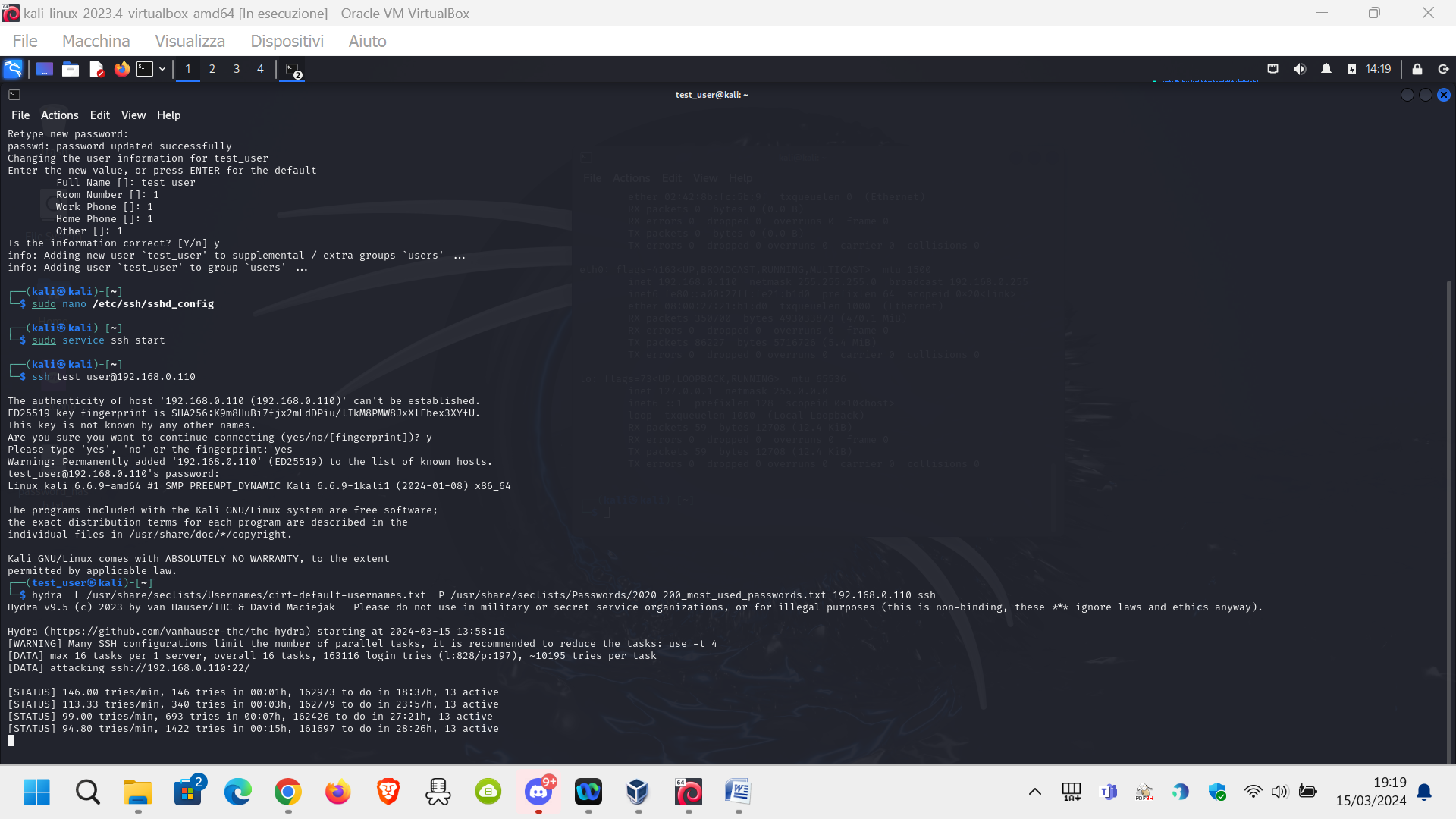
**Fase 1: Configurazione di SSH su Kali Linux**

1. **Creazione di un nuovo utente su Kali Linux**: Abbiamo utilizzato il comando **sudo adduser test\_user** per creare un nuovo utente chiamato "test\_user".



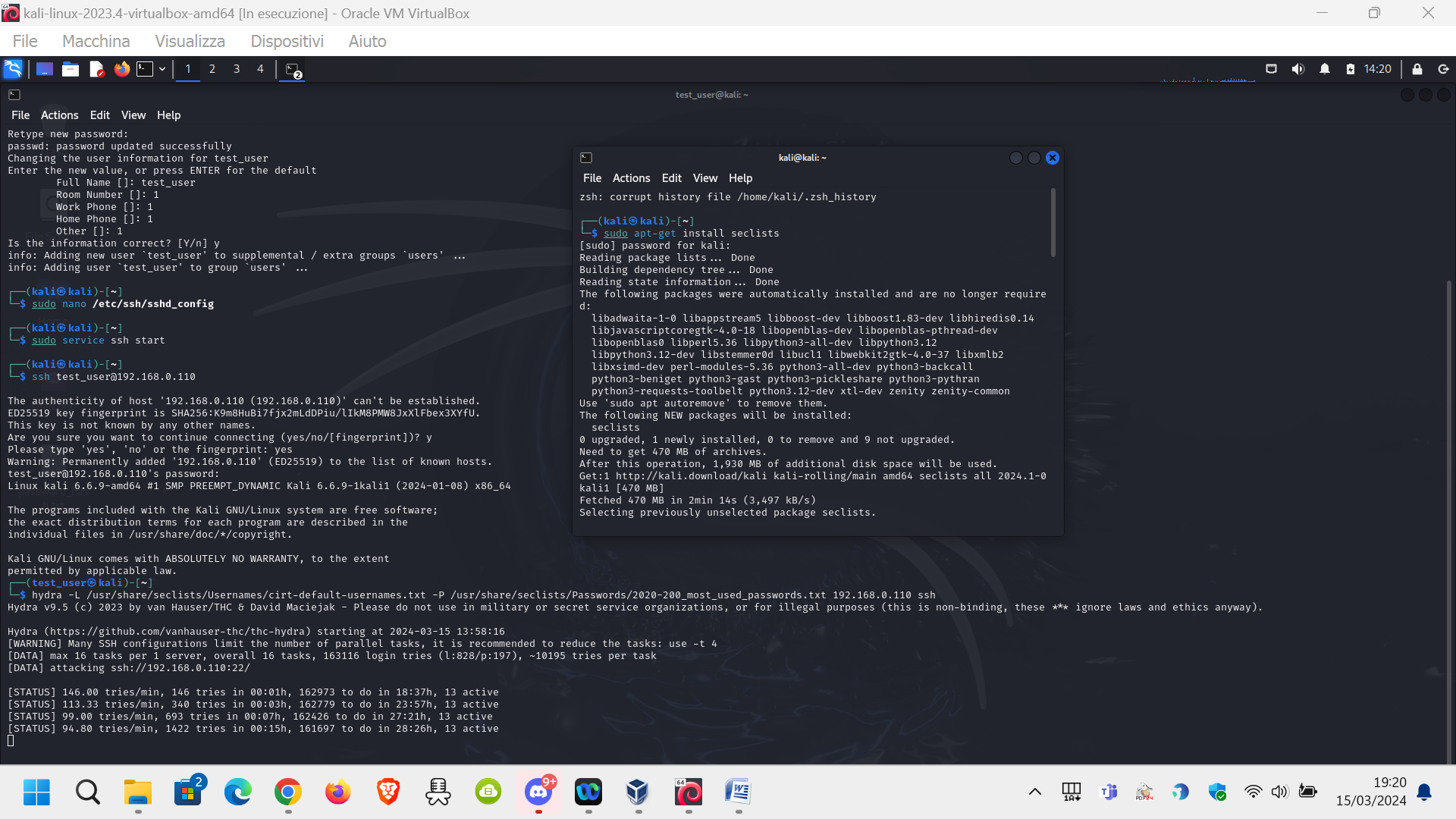


1. **Configurazione della password iniziale**: Abbiamo assegnato una password iniziale "testpass" all'utente appena creato.
2. **Attivazione del servizio SSH**: Abbiamo avviato il servizio SSH utilizzando il comando **sudo service ssh start**.
3. **Verifica dell'accesso SSH**: Abbiamo testato la connessione SSH per l'utente appena creato eseguendo il comando **ssh test\_user@ip\_kali**, sostituendo "ip\_kali" con l'indirizzo IP della nostra macchina Kali. Se le credenziali inserite sono corrette, abbiamo ricevuto il prompt dei comandi dell'utente "test\_user" sulla nostra Kali.



**Fase 2: Cracking dell'autenticazione SSH con Hydra**

1. **Installazione di seclists**: Prima di procedere con l'attacco di forza bruta, abbiamo installato seclists utilizzando il comando **sudo apt install seclists**.

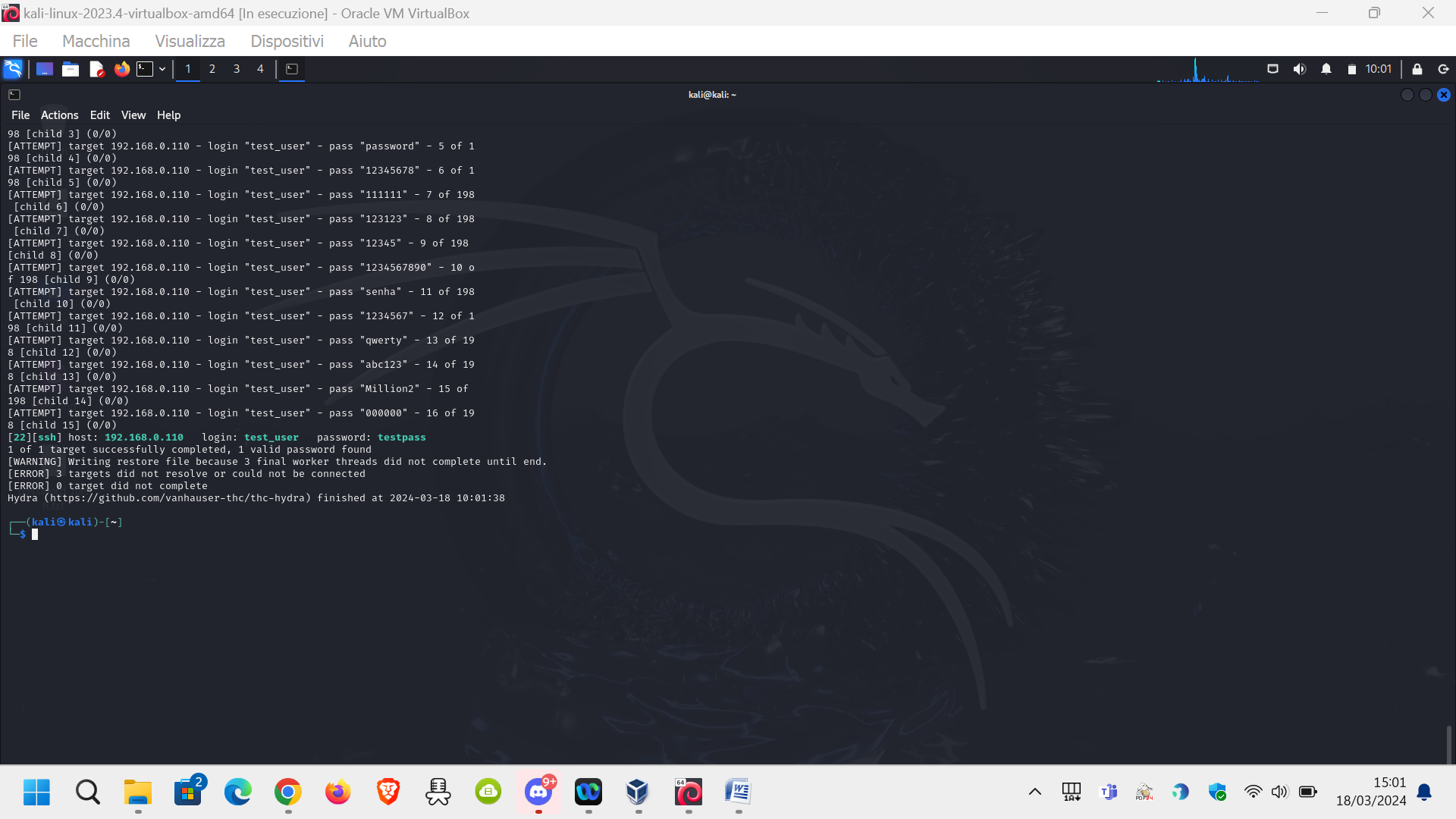


1. **Utilizzo di Hydra per l'attacco di forza bruta**: Abbiamo utilizzato Hydra per eseguire un attacco di forza bruta contro l'autenticazione SSH. La sintassi del comando Hydra è stata illustrata come segue:

cssCopy code

hydra -l username\_list -P password\_list IP\_kali ssh

Dove abbiamo sostituito "username\_list" e "password\_list" con le wordlist scaricate e "IP\_kali" con l'indirizzo IP della nostra macchina Kali. E quindi: **hydra -V -l test\_user -P /usr/share/seclists/Passwords/2020-200\_most\_used\_passwords.txt 192.168.0.110 ssh**



Durante l'esercizio, abbiamo potuto osservare il processo di configurazione di un servizio (SSH) e la successiva esecuzione di un attacco di forza bruta per craccare l'autenticazione. Questo ci ha fornito una maggiore comprensione dei servizi di rete e delle loro vulnerabilità potenziali.

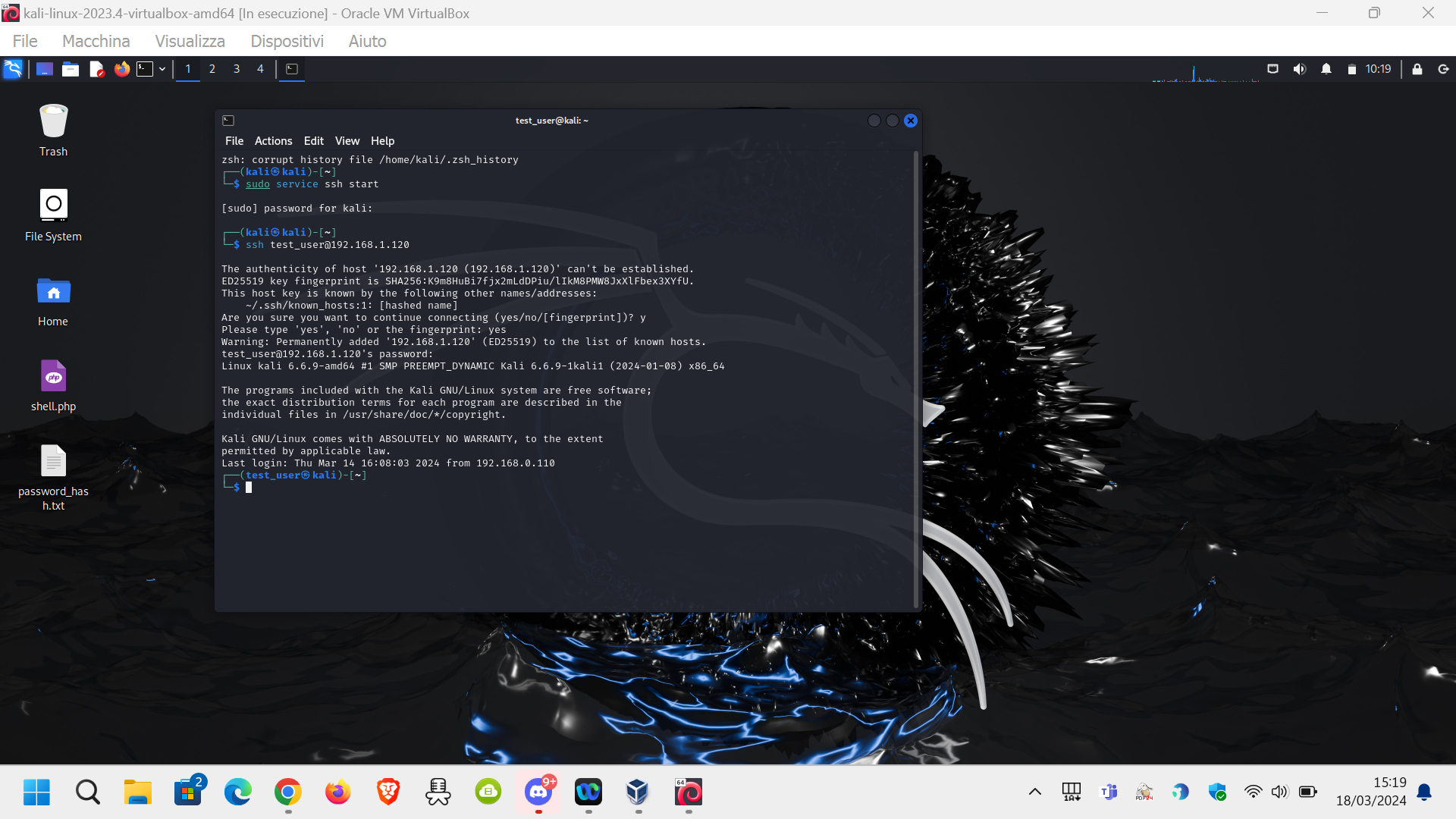
**Esercizio su SSH e FTP da Kali a Kali**

**Obiettivo:** L'obiettivo di questa parte dell'esercizio era esplorare e utilizzare i protocolli SSH e FTP per la comunicazione tra due sistemi Kali Linux all'interno di una rete interna.

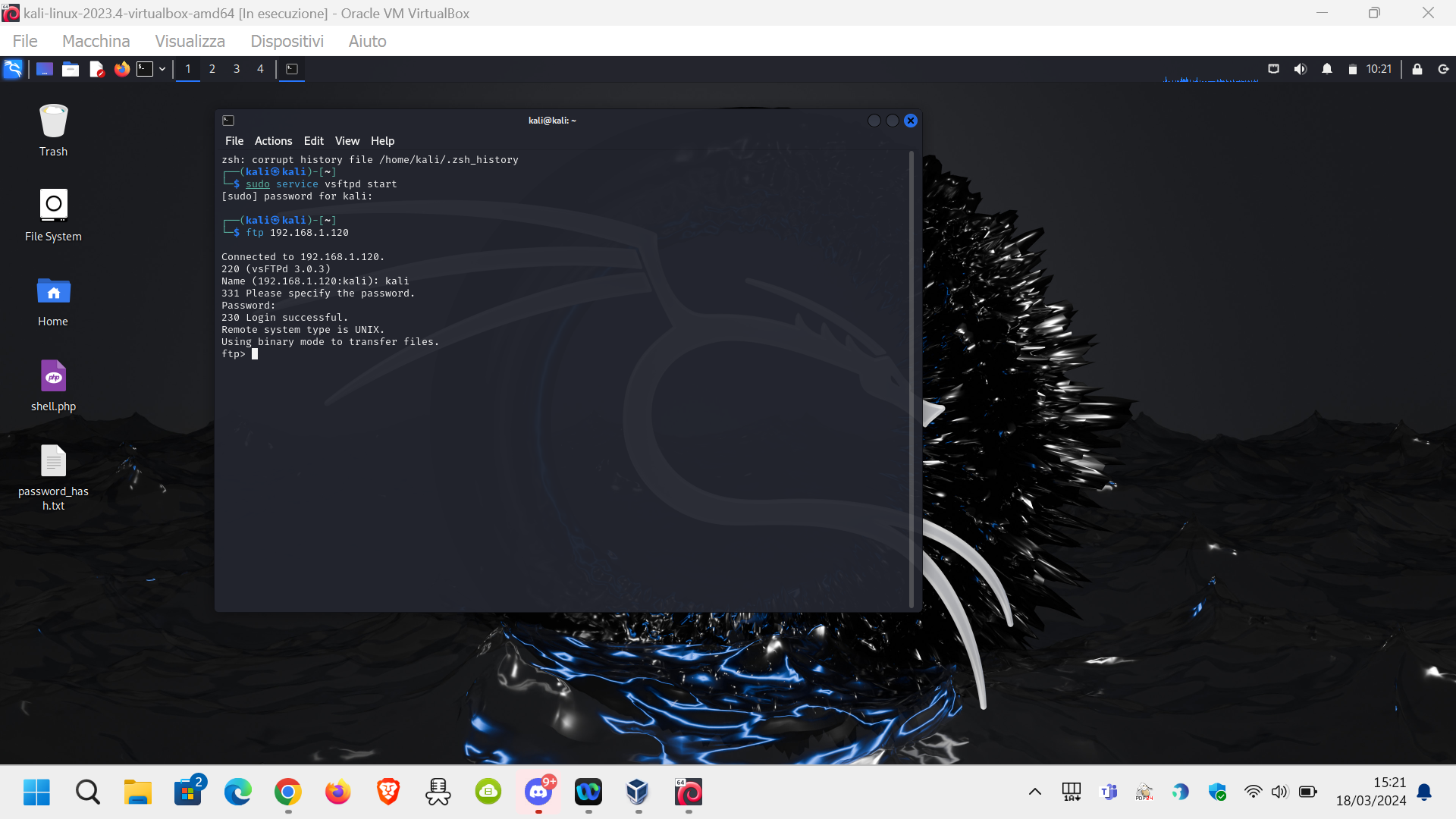
**Procedure eseguite:**

1. Configurazione dell'interfaccia di rete su entrambi i dispositivi Kali per la comunicazione nella stessa rete interna.
2. Avvio del servizio SSH sul dispositivo di destinazione.
3. Connessione tramite SSH utilizzando l'account utente "test\_user" sul dispositivo di destinazione.
4. Avvio del servizio FTP sul dispositivo di destinazione.
5. Tentativo di connessione FTP utilizzando l'account utente "test\_user" sul dispositivo di destinazione.

**Risultati:**



* La connessione SSH è stata stabilita con successo utilizzando l'account utente "test\_user". Il servizio SSH era attivo e funzionante sulla porta predefinita 22.
* Successivamente, il servizio FTP è stato correttamente avviato e la connessione FTP è stata stabilita con successo utilizzando l'account utente "kali".



**Conclusioni:** In conclusione, abbiamo avuto successo nel connetterci tramite SSH e FTP tra due dispositivi Kali Linux nella stessa rete interna.