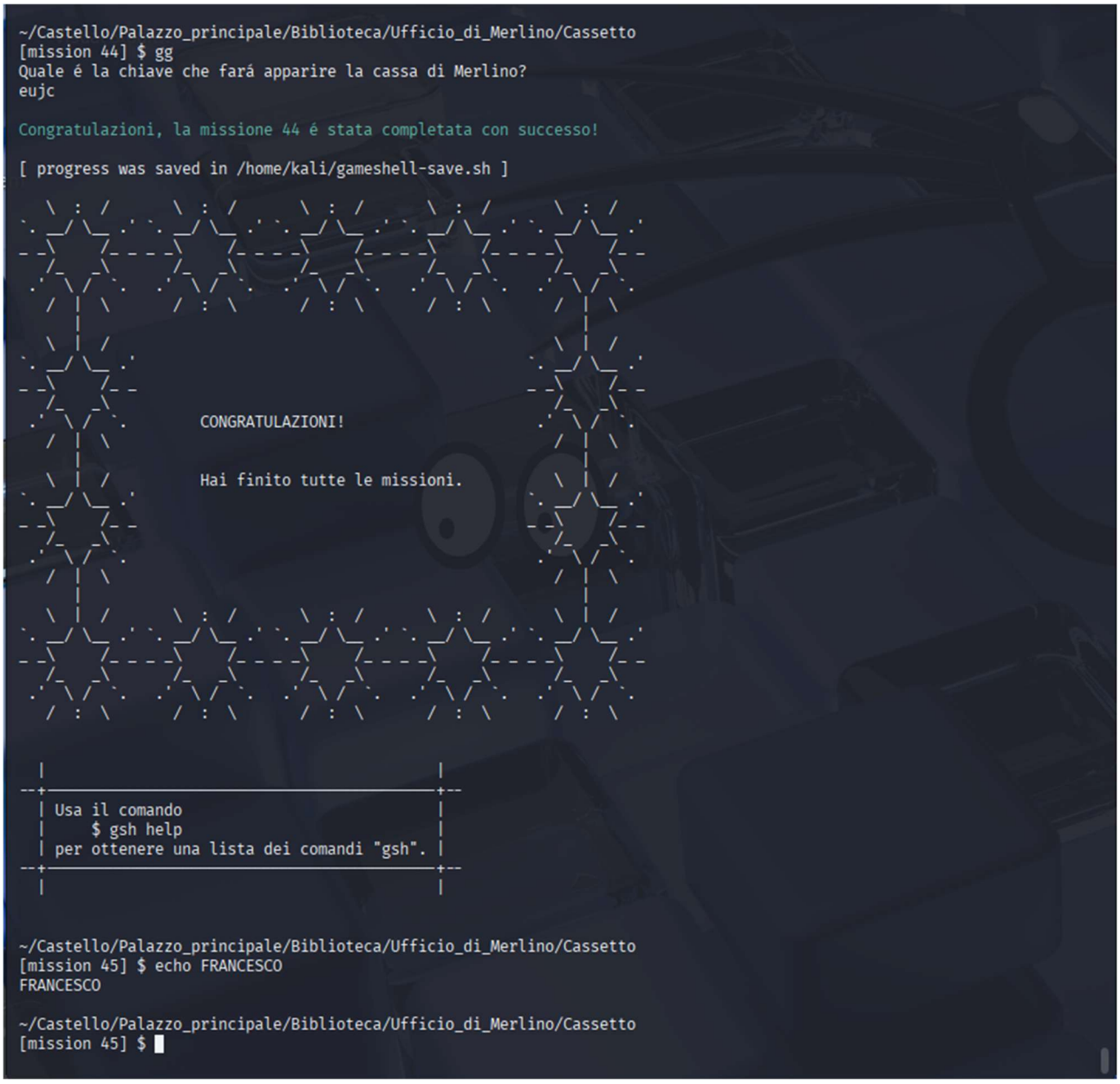
CONSEGNA W8D4

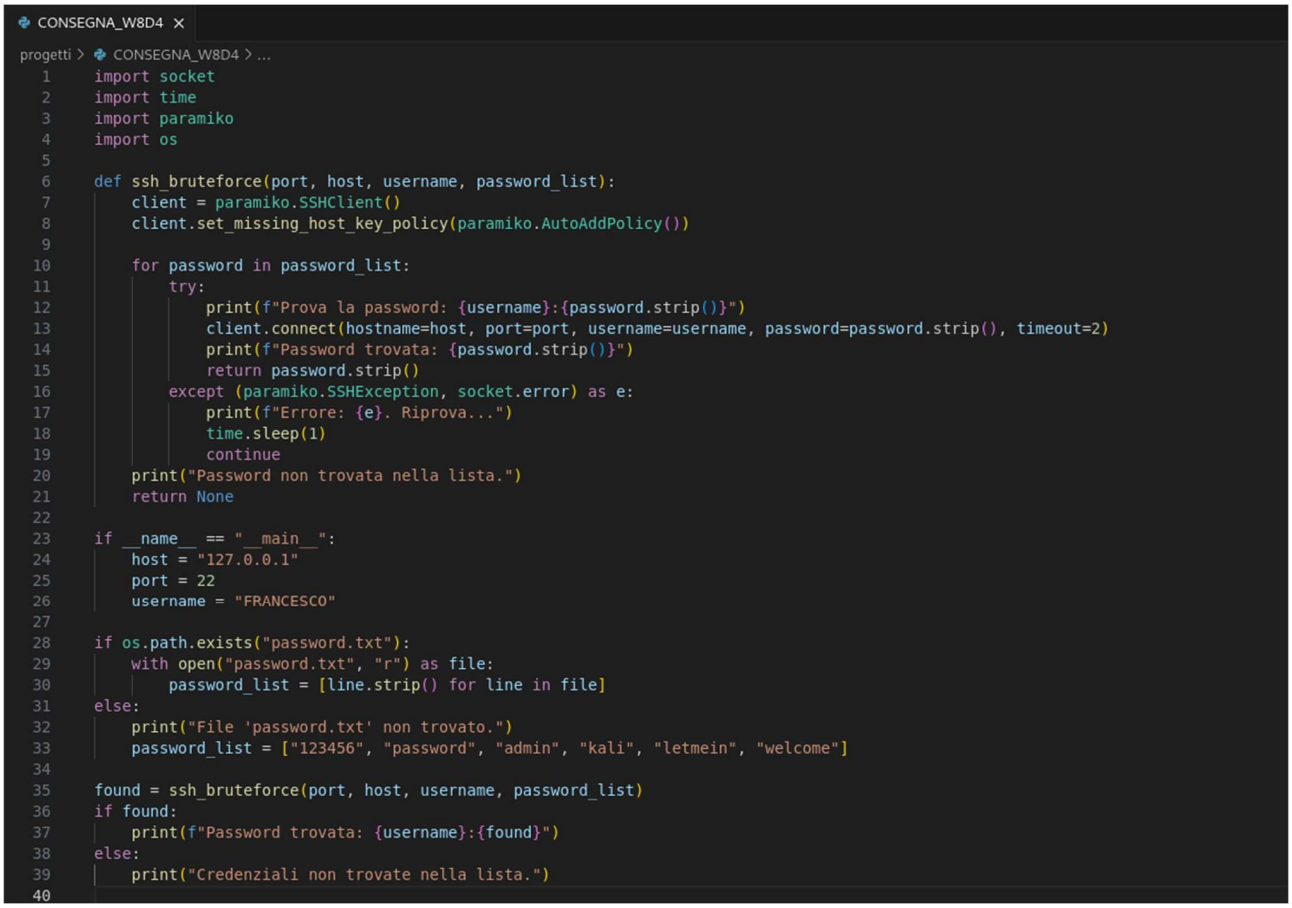
PT.1 GAMESHELL

È un “programma” pensato per per insegnare l’uso della shell. È un vero e proprio gioco da terminale ambientato in un mondo fantasy. I comandi che l’esperienza ti fa allenare sono quelli per spostarsi tra le cartelle, tutto quello che riguarda i file (creare, spostare, modificare, leggerli), modificare i permessi, la gestione dei processi, la ricerca dei file e come ottimizzare i tempi (ad esempio nello screen sotto si può vedere come invece di “gsh check” tramite il comando “alias” per svolgere la stessa funzione basta digitare “gg”).



PT.2 SCRITTURA DI UN PROGRAMMA CHE PERMETTE UN ATTACCO BRUTE-FORCE

Abbiamo creato un tool che prova ad accedere ad un server SSH provando una lista di password. Avevamo la possibilità di scegliere se farlo usando Python o C. Ho scelto di farlo in Python.



1) Ho iniziato con l'importare le varie librerie:

- Socket: usata per intercettare errori di rete
- Time: usato per misurare la durata dell'attacco
- Paramiko: utile per gestire le connessioni SSH
- Os: usato per verificare se una cartella o un file esiste

2) Definiamo la funzione principale che prova a connettersi tramite SSH usando una lista di password

3) Configurazione del client SSH. Creando un oggetto "SSHClient" e gli diamo il comando di accettare chiave sconosciute

4) Andiamo a creare un loop sulle password

5) Tentativi di connessioni. Provando a farlo connettere con le varie password e restituendoci i vari tentativi

6) Gestione degli errori.

- Ogni volta che la password è errata ci restituisce il messaggio "password errata"
- Per eventuali errori di rete ci restituisce l'errore e interrompe il processo

7) Creazione del blocco principale “if __name__ == “__main__” ci assicura che il codice venga eseguito solo se il file è avviato direttamente

8) Parametri di connessione. Specifichiamo l’indirizzo IP; la porta SSH e l’username da testare

9) Lettura del file delle password. Diamo il comando che fa aprire il file “password.txt” e creiamo una lista di password

10) Esecuzione del brute-force

11) Stampa del risultato. Dove o vengono restituite le credenziali nel caso fossero corrette o altrimenti viene comunicato il fallimento.

Con l’ultimo screen vado a mostrare come si comporta il codice in caso di utilizzo.