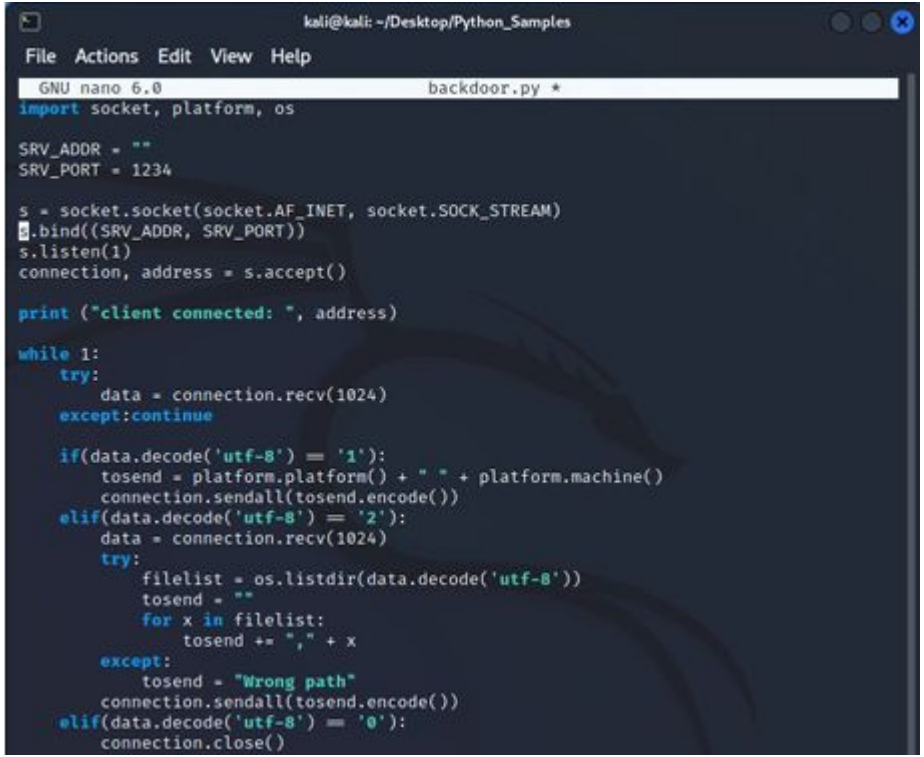
Backdoor

Traccia:

L'esercizio di oggi consiste nel commentare/spiegare questo codice che fa riferimento ad una backdoor. Inoltre spiegare cos'è una backdoor.



Questo server è in ascolto su una porta specificata (SRV_PORT) per le connessioni in entrata.
A seconda dei dati ricevuti, esegue diverse azioni:

l socket viene associato a un indirizzo IP e a una porta specificati con bind((SRV_ADDR, SRV_PORT)).
In attesa di connessioni: Il server inizia ad ascoltare sulla porta specificata con listen(1) e attende che un client si connetta con accept().
Gestione delle connessioni: Una volta stabilita una connessione con un client, viene visualizzato un messaggio di "client connnected" insieme all'indirizzo del client.
Il ciclo principale nel server entra in un ciclo (while 1) in cui riceve i dati dal client
Elaborazione dei dati: In base ai dati ricevuti, il server può rispondere in tre modi:

- Se riceve '1', invia al client le informazioni su piattaforma e sistema.
- Se riceve '2', riceve un messaggio contenente un percorso e invia al client la lista nella directory specificata.
- Se riceve '0', chiude la connessione corrente e aspetta una nuova connessione.

La backdoor

La backdoor o (porta sul retro) è una seconda via di accesso non documentata per ottenere l'accesso a un sistema, bypassando normali procedure di autenticazione o sicurezza. Questa può essere intenzionalmente installata da un amministratore di sistema legittimo per scopi di manutenzione o di supporto, ma può anche essere sfruttata malevolmente dai blackhat.