Lo scopo di questo codice è quello di stabilire una connessione ad una backdoor tramite le socket, in questo caso la backdoor sulla porta 1234.

Il codice inizia con l'import di 3 librerie quali socket, platform e os.

La libreria socket ci permette di creare e gestire le connessioni di rete, inviando e ricevendo pacchetti.

La libreria platform ci permette di ricevere informazioni sulla macchina su cui viene eseguito.

La libreria os ci permette di eseguire operazione sul file system, gestire file e directory.

Dichiariamo poi delle variabili quali SRV_ADDR e SRV_PORT che sono inizializzate rispettivamente con "" e 1234.

Nelle righe successive inizializziamo un socket che chiamiamo s e gli diamo come parametri AF_INET e SOCK_STREAM, così stiamo specificando che il socket deve utilizzare IPv4 ed una connessione TCP.

Utilizziamo il metodo .bind() che ci permette di collegarlo alla porta e all'indirizzo IP che gli passiamo come parametri, in questo caso: s.bind(SRV_ADDR, SRV_PORT)

Successivamente usiamo s.listen(1) che ci permette di configurare il socket per ascoltare sulla porta che abbiamo indicato. Il numero fra parentesi indica il numero massimo di connessioni in coda.

A riga 8 poi ritroviamo il metodo accept(), che restituisce l'oggetto socket che utilizzeremo per lo scambio dati e l'IPv4 del client.

Apriamo poi un ciclo while con condizione True (1) ovvero un loop e con il try-except ignora qualsiasi tipo di errore e continua con il ciclo. Riceviamo in questo caso i dati dal client inserendoli nella variabile data con la riga di codice 'data = connectio.recv(1024).

Nel caso in cui i dati che riceviamo siano uguali '1',il server invia al client il nome della piattaforma e il tipo di macchina utilizzando le funzioni fornite dalla libreria platform

Nel caso in cui i dati che riceviamo siano uguali a '2' il server riceve ulteriori dati dal client, rappresentanti il percorso di una directory. Successivamente, cerca i file nella directory specificata utilizzando la funzione os.listdir(), e se la directory è valida, invia al client una lista di file presenti in essa.

Nel caso in cui i dati che riceviamo siano uguali a '0' il server chiude la connessione corrente e rimane in attesa di una nuova connessione.

Una backdoor è una vulnerabilità intenzionalmente introdotta o una porta secondaria nascosta all'interno di un sistema informatico, di un'applicazione software o di un dispositivo, che consente l'accesso non autorizzato o non inteso al sistema. Le backdoor possono essere utilizzate da hacker,

sviluppatori di software o amministratori di sistema per ottenere un accesso segreto al sistema, bypassando i normali controlli di sicurezza.

Possono essere usate per scopi legittimi, come il supporto da remoto degli sviluppatori, ma possono anche essere utilizzate per attività illegali come il furto dei dati.