```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.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 programma socket*

*In questo esercizio andiamo a vedere come un attaccante può ascoltare una conversazione fra due persone collegate a una porta conoscendo almeno l'indirizzo IP di una delle due persone. Tutto ciò è possibile tramite il socker, un tool pre-impostato su kali.*

*Il programma inizia con l'importazione dei vari delle varie librerie che andremo a utilizzare, ovvero* ***socket,platform e os.***

*Successivamente viene impostato l'indirizzo IP interessato(in questo caso vuoto perche il programma è eseguibile con qualsiasi IP) e la porta di riferimento; viene utilizzata questa specifica porta perchè precedentemente l'attaccante è riuscito a inserire un Trojan all'interno di una delle macchine che comunicano, questo malware è stato programmato proprio per passare inosservato al computer attaccato e per aprire la porta desiderata cosi da consentire l'accesso.*

*Con il comando socket.socket viene creato il socket con delle specifiche particolari:*

- *Con AF_INET specifichiamo che vogliamo un socket con indirizzo IPv4*
- *Con SOCK_STREAM invece specifichiamo che vogliamo una connessione di tipo TCP*

*A seguire vengono usati i comandi:*

- *s.bind((SRV_ADDR, SRV_PORT)) per collegare il socker all'IP desiderato e alla porta utilizzata per l'ascolto.*
- *s.listen(1) per configurare il socket sulla coppia IP:PORTA; il numero tra parentesi tonde sta a indicare il numero di connessioni in coda.*
- *s.accept() è il metodo di accettazione delle connessioni in entrata.*

*Infine abbiamo un ciclo while infinito, poichè è stato inserito il valore true(1) e sappiamo bene che il ciclo while in phython continua all'infinito se sempre vero.*

## *Cos'è una Backdoor?*

*La backdoor(definita come malware) in questo programma è proprio la porta 1234 utilizzata perche, come spiegato piu in alto, è stata aperta da un malware inserito proprio dall'attaccante precedentemente. Questa backdoor non permette solo di spiare la conversazione, ma permette anche di entrare all'interno del computer indisturbato.*

*Esistono vari tipi di backdoor:*

- *Trojan: Fingono di essere file benigni ma contengono funzioni dannose(come il cavallo di Troia, da qui il nome Trojan).*
- *Backdoor Integrale: Sono backdoor impossibili da chiudere, create sotto forma di account predefiniti.*
- *Reverse Shell:è una tecnica per eseguire comandi sulla macchina della vittima; la particolarità di questo attacco è che la connessione si origina dal sistema infetto verso l'attaccante, al quale viene dato poi accesso alla shell dei comandi.*
- *Botnet: Sono attacchi di massa, eseguiti su larga scala(ad esempio attacchi di DDOS).*

## *Come difendersi?*

- *Limitare i privilegi, cercando di prevenire l'infiltrazione di attaccanti e ospiti sgradevoli.*
- *Firewall ben settati forniscono un buono scudo, bloccando connessioni provenienti da web server sospetti.*
- *Tenere sempre aggiornate applicazioni di ogni genere.*
- *Antivirus completi con regolare monitoraggio sono regole base contro qualsiasi tipo di attacco, anche questi.*
- *Creando un honeypot, per far cadere nella trappola tutti coloro che proveranno a insidiarsi nel computer tramite backdoor.*