

Per arrivare a mettere una “backdoor” bisogna prima superare delle fasi

- informazione
- cerca porta
- exploit
- mantenimento privilegi

The screenshot displays a terminal window titled "kali@kali: ~/Desktop/python". The terminal shows the execution of a Python script named "provasocket.py".

```
File Actions Edit View Help
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()
```

The user enters the following commands:

```
kali@kali:~/Desktop/python]
$ nano provasocket.py
kali@kali:~/Desktop/python]
$ nano provasocket.py
kali@kali:~/Desktop/python]
$ python provasocket.py
```

The output shows a traceback error:

```
*Traceback (most recent call last):
  File "/home/kali/Desktop/python/provasocket.py", line 9, in <module>
    connection, address = s.accept()
                                ^^^^^^^^^^
FileNotFoundError: [Errno 2] No such file or directory: 'socket.socket'

File "/usr/lib/python3.11/socket.py", line 294, in accept
    fd, addr = self._accept()
               ^^^^^^^^^^^^
KeyboardInterrupt
```

The user then runs the command:

```
kali@kali:~/Desktop/python]
$ python provasocket.py
```

The output shows:

```
client connected: ('192.168.1.14', 39086)
```

Fungendo in poche parole da server è configurato per ascoltare su un indirizzo vuoto ("") e la porta 1234 ed entra quindi in un loop infinito (while 1) in cui aspetta di ricevere comandi dal client. I comandi vengono ricevuti tramite `connection.recv(1024)` e decodificati.

```
kali@kali: ~/Des
File Actions Edit View Help
-Select an option: 2
Insert the path: kali/home/Desktop
*****
Wrong path
*****
-Select an option: 0

(kali@kali)-[~/Desktop/python]
$ pwd
/home/kali/Desktop/python

(kali@kali)-[~/Desktop/python]
$ python porta.py
Type the server IP address: 192.168.1.14
Type the server port: 1234
Connection established

0) Close the connection
1) Get system info
2) List directory contents

-Select an option: 2
Insert the path: /home/kali/Desktop/python
^CTraceback (most recent call last):
  File "/home/kali/Desktop/python/porta.py", line 35, in <module>
    data = my_sock.recv(1024)
KeyboardInterrupt

(kali@kali)-[~/Desktop/python]
$ python porta.py
Type the server IP address: 
```

Il codice che hai fornito è un esempio di un'applicazione client-server semplice utilizzando socket in Python. Questo tipo di applicazione consente a un client di stabilire una connessione a un server e inviare comandi al server, che a sua volta risponde ai comandi del client. Sembra che il client sia progettato per interagire con un server remoto in modo da eseguire comandi specifici e ricevere risposte.