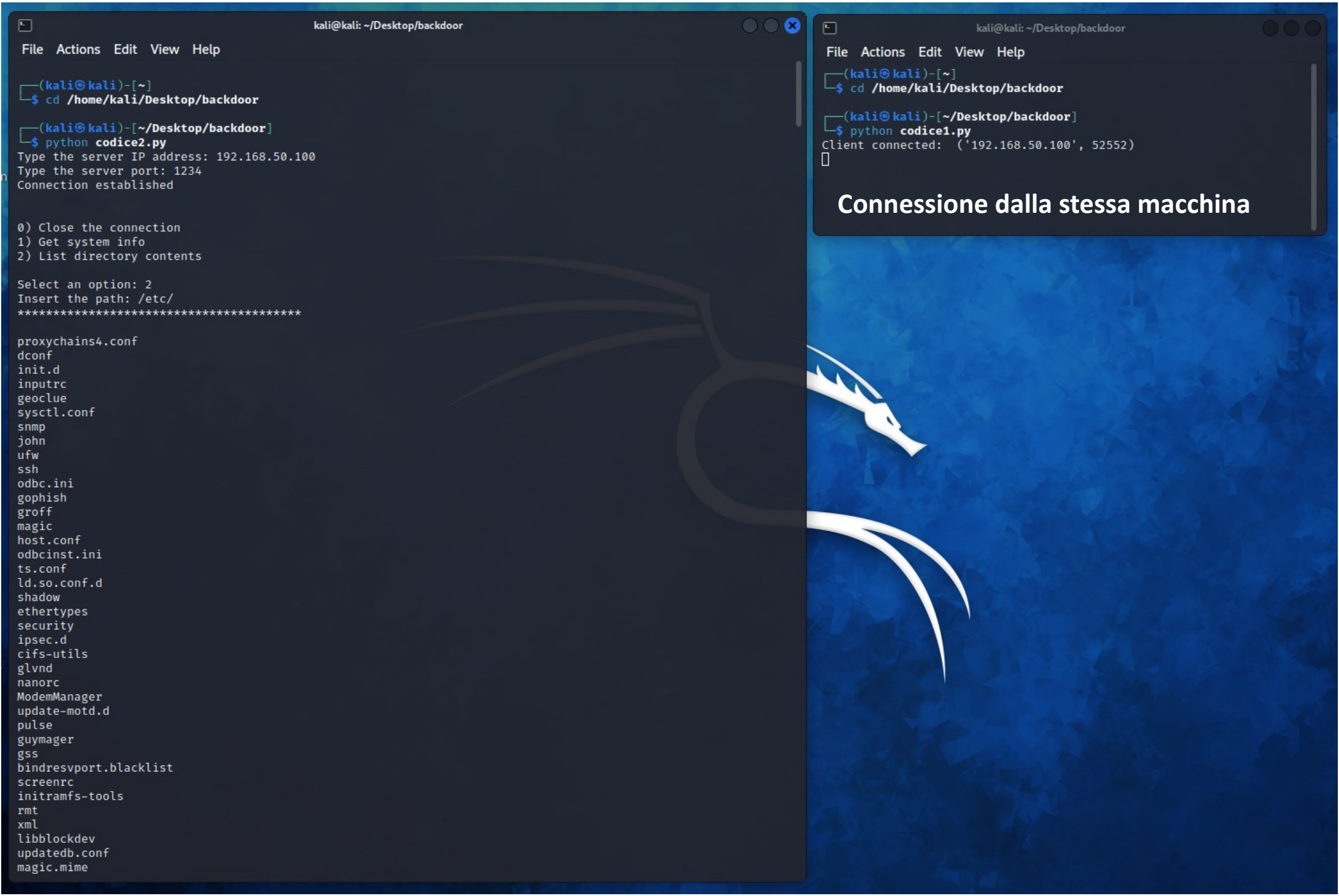
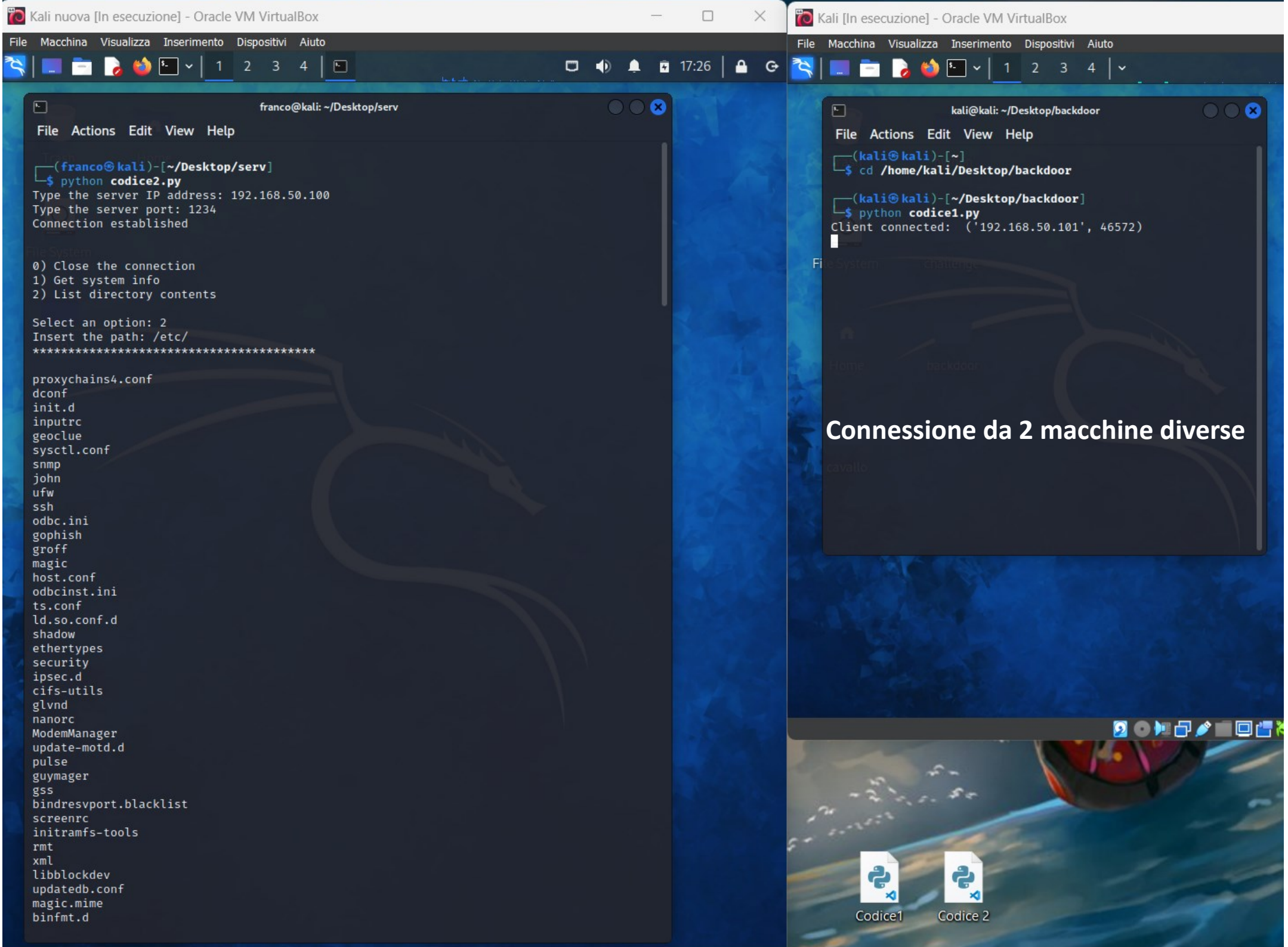
S3L2 | BACKDOOR | DIFFERENZA TRA I DUE CODICI | TEST DEL CODICE

Una backdoor è una vulnerabilità intenzionalmente inserita in un sistema software per consentire l'accesso non autorizzato o la manipolazione da parte di terzi. La backdoor rappresenta una minaccia grave, perché consente a utenti malintenzionati di trapassare le normali misure di sicurezza e ottenere un accesso non autorizzato al sistema, avendo cosi accesso a dati sensibili, per poi eseguire attacchi dannosi o sfruttare il sistema per scopi malevoli senza essere rilevati.
La presenza di backdoor può compromettere la sicurezza e l'integrità di sistemi informatici, rendendoli esposti a varie forme di exploit e violazioni della privacy.

Nell'esercizio di oggi abbiamo due codici che rappresentano un esempio di un server e un client che comunicano tramite il socket.
Il server fornisce informazioni di sistema e una lista di file in una directory specifica, mentre il client interagisce con il server attraverso un menu di opzioni.
La principale differenza è che il server esegue un loop per gestire connessioni multiple, mentre il client esegue un menu interattivo per consentire all'utente di selezionare le opzioni desiderate in modo più flessibile.
Inoltre, il client richiede all'utente di inserire manualmente l'indirizzo IP e la porta del server, mentre nel server questi valori sono fissati nel codice, infatti andiamo a modifica l'indirizzo IP della nostra macchina e la porta e proviamo a lanciare il programma.


kali@kali: ~/Desktop/backdoor
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/Desktop/backdoor
┌──(kali㉿kali)-[~/Desktop/backdoor]
└─$ python codice2.py
Type the server IP address: 192.168.50.100
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: /etc/
****
proxychains4.conf
dconf
init.d
inputrc
geoclue
sysctl.conf
snmp
john
ufw
ssh
odbc.ini
gophish
groff
magic
host.conf
odbcinst.ini
ts.conf
ld.so.conf.d
shadow
ethertypes
security
ipsec.d
cifs-utils
glvnd
nanorc
ModemManager
update-motd.d
pulse
guymager
gss
bindresvport.blacklist
screenrc
initramfs-tools
rmt
xml
libblockdev
updatedb.conf
magic.mime
kali@kali: ~/Desktop/backdoor
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/Desktop/backdoor
┌──(kali㉿kali)-[~/Desktop/backdoor]
└─$ python codice1.py
Client connected: ('192.168.50.100', 52552)
Connessione dalla stessa macchina


Kali nuova [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
17:26
franco@kali: ~/Desktop/serv
File Actions Edit View Help
┌──(franco㉿kali)-[~/Desktop/serv]
└─$ python codice2.py
Type the server IP address: 192.168.50.100
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: /etc/
****
proxychains4.conf
dconf
init.d
inputrc
geoclue
sysctl.conf
snmp
john
ufw
ssh
odbc.ini
gophish
groff
magic
host.conf
odbcinst.ini
ts.conf
ld.so.conf.d
shadow
ethertypes
security
ipsec.d
cifs-utils
glvnd
nanorc
ModemManager
update-motd.d
pulse
guymager
gss
bindresvport.blacklist
screenrc
initramfs-tools
rmt
xml
libblockdev
updatedb.conf
magic.mime
binfmt.d
Kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali: ~/Desktop/backdoor
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/Desktop/backdoor
┌──(kali㉿kali)-[~/Desktop/backdoor]
└─$ python codice1.py
Client connected: ('192.168.50.101', 46572)
Connessione da 2 macchine diverse
Codice1
Codice 2