Compito di oggi:

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

Una "backdoor" è una via di accesso segreta o nascosta in un sistema informatico, software o dispositivo che consente a un utente autorizzato o non autorizzato di aggirare le normali procedure di autenticazione e ottenere l'accesso al sistema o alle sue funzionalità in modo non intenzionale. In altre parole, una backdoor è una porta secondaria che bypassa le normali misure di sicurezza.

Le backdoor possono essere deliberate o accidentali.

Le **backdoor deliberate** sono spesso create da sviluppatori di software o da individui malevoli per scopi nefasti. Ad esempio, un malware potrebbe installare una backdoor in un sistema per consentire agli hacker di accedere e controllare il sistema senza il consenso dell'utente legittimo.

Le **backdoor accidentali** possono verificarsi a causa di errori di programmazione o di configurazione. Questi errori possono creare vulnerabilità non intenzionali che possono essere sfruttate da terze parti per ottenere accesso non autorizzato.

Le backdoor possono comportare diversi pericoli, a seconda di come vengono utilizzate e implementate. Ecco alcuni dei principali rischi associati alle backdoor:

1. Accesso non autorizzato:

• La backdoor fornisce un accesso non autorizzato al sistema o al software in cui è implementata. Questo può permettere a un attaccante di compromettere la sicurezza del sistema, accedere a dati sensibili o eseguire azioni dannose.

2. Violenza della privacy:

• Se una backdoor è utilizzata malevolmente, può essere impiegata per monitorare le attività degli utenti senza il loro consenso. Ciò può portare a gravi violazioni della privacy, con conseguente accesso indebito a informazioni personali e riservate.

3. Attacchi mirati:

• Le backdoor possono essere utilizzate come parte di attacchi mirati, in cui gli attaccanti sfruttano questa via di accesso segreta per condurre operazioni di spionaggio, furto di informazioni aziendali o governative, o sabotaggio.

4. Danni ai dati e alle risorse:

• Gli utenti malevoli possono utilizzare backdoor per danneggiare o cancellare dati critici, interrompere le operazioni di sistema o causare danni irreparabili alle risorse digitali.

5. Diffusione di malware:

• Le backdoor sono spesso utilizzate come parte di malware più ampi. Una volta che una backdoor è installata su un sistema, può essere sfruttata per l'introduzione di ulteriori malware o per facilitare l'espansione di una minaccia informatica.

6. Minaccia persistente avanzata (APT):

 Le backdoor sono spesso coinvolte in attacchi APT, in cui gli attaccanti cercano di mantenere l'accesso non rilevato per lunghi periodi. Ciò può consentire loro di raccogliere informazioni sensibili nel tempo e di eseguire azioni dannose senza essere scoperti.

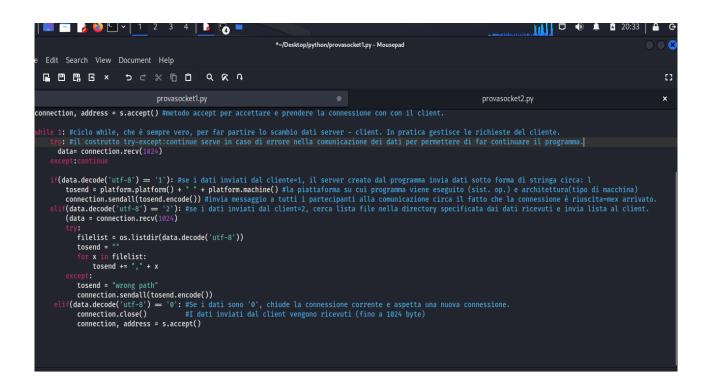
7. Rischi legali e reputazionali:

 L'installazione di backdoor può comportare conseguenze legali significative per gli sviluppatori di software o per coloro che implementano tali meccanismi senza il consenso degli utenti. Inoltre, può danneggiare la reputazione di un'organizzazione o di un individuo.

CODICI

Il primo programma è un semplice server che permette l'ingresso tramite una backdoor (porta 1234) alla macchina client che utilizzerà il codice 2 per vedere la tipologia del sistema operativo oppure il contenuto della directory che si immette.

Codice server



Codice client

```
□ • • 20:54
 📉 🔲 🛅 🍃 🍏 🕒 🗸 1 2 3 4 | 🖪 🍖 🖿
                                                                                                                                                                                                                                 ~/Desktop/python/provasocket2.py - Mousepad
 provasocket1.py
  1 import socket ##modulo importati per sfruttarne le funzionalità
  2 SRV_ADDR =input("Type the server IP address: ") #dichiarazione delle variabili del server richieste all'utente: Ip e porta del server 4 SRV_PORT =int(input("Type the server port: "))
 6 def print_menu():
7     print("""\n\n0) Close the connection
8 1) Get system info
9 2) List directory contents""")
 11 my_sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM) #creazione del socket che si mette in ascolto tramite IP:porta
12 my_sock.connect((SRV_ADDR, SRV_PORT)) #il socket si connette con il server attraverso la coppia IP:po
                                                                                       #il socket si connette con il server attraverso la coppia IP:porta
                                                                 #viene stampato a video il fatto che la connessione è stabilita. #viene stampato a video il menù delle opzioni.
 14 print("Connection 15 print_menu()
         nt("Connection established")
15 print_mer
17 while 1:
18 messa
19 20 if(me
21 r
22 z
23 i
24 25 elife
26 27
         message = input("\n-Select an option: ")
                                                                 #questo blocco serve a gestire le scelte dell'utente.
#Se utente sceglie=0, invia il messaggio al server per chiudere la connessione e termina il programma.
          if(message = 0):
    my_sock.sendall(message.encode())
    my_sock.close()
          elif(message = "1"):
    my_sock.sendall(message.encode())
    data = my_sock.recv(1024)
```

