# ESERCITAZIONE S3L2

Una backdoor è concettualmente simile a una vulnerabilità intrinseca o a un accesso non autorizzato, inserito intenzionalmente nel software di un sistema informatico. In altri termini è come possedere una chiave di riserva che consente l'accesso al sistema senza rilevamenti apparenti.

Va notato che, sebbene talvolta le backdoor siano integrate per scopi legittimi, come la facilitazione delle operazioni di manutenzione da parte degli sviluppatori, il loro utilizzo improprio o la compromissione accidentale di tali accessi possono portare a gravi minacce per la sicurezza informatica. Pertanto, è di cruciale importanza implementare adeguate misure di sicurezza per mitigare il rischio di accessi indesiderati al sistema.

La pericolosità di una backdoor deriva principalmente dalla sua capacità di aprire un varco non autorizzato e impercettibile in un sistema informatico. Le ragioni di tale minaccia sono diverse e includono:

- Accesso Incontrollato: Una backdoor consente l'accesso al sistema bypassando i normali controlli di sicurezza. Questo significa che chiunque sia in grado di sfruttarla può entrare nel sistema senza essere rilevato, aprendo la strada a possibili abusi.

- Potenziale di Danneggiamento: Una volta che un individuo o un gruppo ha accesso tramite la backdoor, possono manipolare dati, installare software dannoso o danneggiare il sistema. Le conseguenze di tali azioni possono essere gravi, soprattutto se coinvolgono informazioni cruciali o sistemi vitali.

- Violazione della Riservatezza: Le backdoor possono essere utilizzate per raccogliere informazioni sensibili senza il consenso degli utenti. Questo costituisce una minaccia significativa alla privacy.

- Persistenza Nascosta: Le backdoor sono spesso progettate per rimanere attive nel sistema a lungo termine senza essere rilevate. Ciò complica l'individuazione e la mitigazione della minaccia, poiché gli attaccanti possono mantenere l'accesso senza essere scoperti.

- Utilizzo Su Larga Scala: Se una backdoor viene distribuita su più sistemi, gli attaccanti possono compromettere simultaneamente numerosi utenti. Questo amplifica notevolmente l'impatto della minaccia, aumentando il numero di vittime potenziali.

In sintesi, la pericolosità di una backdoor risiede nella sua abilità di introdurre un accesso non autorizzato e impercettibile, aprendo la strada a una serie di attività dannose che minacciano la sicurezza e l'integrità dei sistemi informatici.

*CODICE 1*

Il primo codice permette l'ascolto con socket tcp su un indirizzo e una porta specifici.

Definendo l'ip e la porta da ascoltare ci permette di stabilire una connessione con il client, stampando un messaggio di collegamento e ricevendo i dati.

Se il dato ricevuto è "1", invia al client informazioni sul sistema operativo e sul dispositivo.

Se il dato è "2", si ricevono ulteriori dati, cercando nella directory e invia la lista.

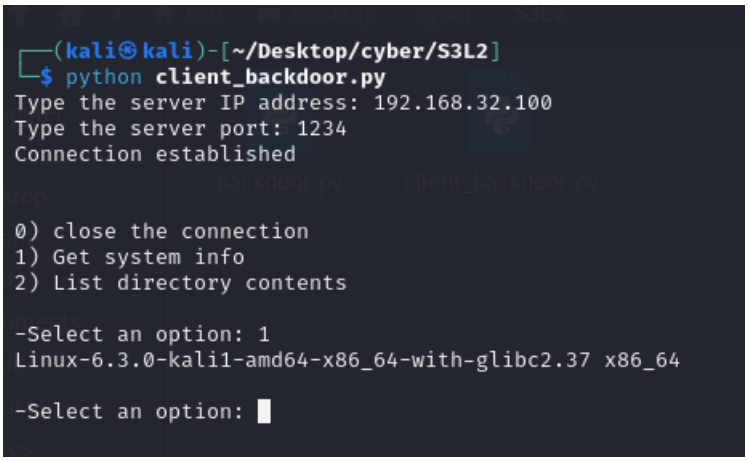
Se il dato è "0", chiude la connessione e ne accetta una nuova.

*CODICE 2*

Il secondo codice permette di inserire l'ip del server e la porta.

Dando in input 0, chiude la connessione.

Dando in input 1, permette di mandare un messaggio con le informazioni sul sistema operativo




Mettendo 2 invece, si manda un messaggio con path, che restituisce le informazioni sulla directory.