S3-L2

Leandra

Backdoor

Una "backdoor" è una via di accesso che bypassa le normali procedure di autenticazione o sicurezza.

Le backdoor possono assumere diverse forme e possono essere implementate a livello hardware o software. In genere, sono progettate per evitare la rilevazione, consentendo a chi le conosce di ottenere un accesso non autorizzato senza essere notati.

CODICE 1

Nel codice 1, è stato creato come backdoor personale. In essa vengono importati tre diversi programmi: socket fornisce funzionalità per la comunicazione di rete; platform fornisce una interfaccia per informazioni specifiche sulla piattaforma su cui il tuo programma Python sta girando; os fornisce una serie di funzioni che permettono al tuo programma Python di interagire con il sistema operativo sottostante.

Infatti, in esso ci sono due variabili, una con l'indirizzo IP del PC dove vogliamo mettere il servizio in ascolto, ossia il nostro, ed una con una porta che poi useremo per la connessione.

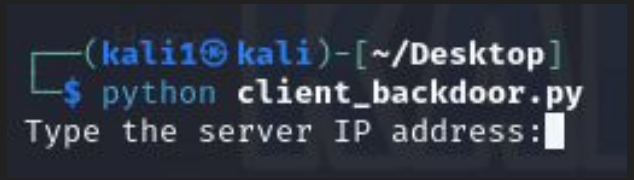
La connessione utilizzata è di tipo TCP, e siccome è stato specificato il binding la backdoor è in grado di ascoltare.

CODICE 1

Se la condizione 1 è verificata viene creato un nuovo oggetto tosend che contiene la concatenazione della piattaforma e dell'architettura del sistema, separati da uno spazio.

CODICE 2

Il codice 2 è stato creato per un utente. Difatti, è possibile scorgere due opzioni diverse; ossia, l’opzione numero 1, ottenere informazione del sistema e opzione numero 2, la lista delle directory.


(kali1㉿kali)-[~/Desktop]
$ python client_backdoor.py
Type the server IP address:


(kali1㉿kali)-[~/Desktop]
$ python backdoor.py