Backdoors

Cos’è una backdoor

Una "backdoor" (porta sul retro, in italiano) è un termine informatico che si riferisce a una vulnerabilità intenzionale o a un meccanismo nascosto in un sistema software o hardware che consente l'accesso non autorizzato o il controllo del sistema da parte di utenti non autorizzati. In pratica, una backdoor è un modo segreto per bypassare le normali procedure di autenticazione o sicurezza di un sistema.

Le backdoor possono essere create a scopo legittimo, ad esempio per consentire l'accesso remoto a scopo di manutenzione o monitoraggio da parte degli sviluppatori o degli amministratori di sistema. Tuttavia, se una backdoor viene sfruttata da persone non autorizzate o se è presente senza il consenso degli utenti, può rappresentare una minaccia alla sicurezza e alla privacy.

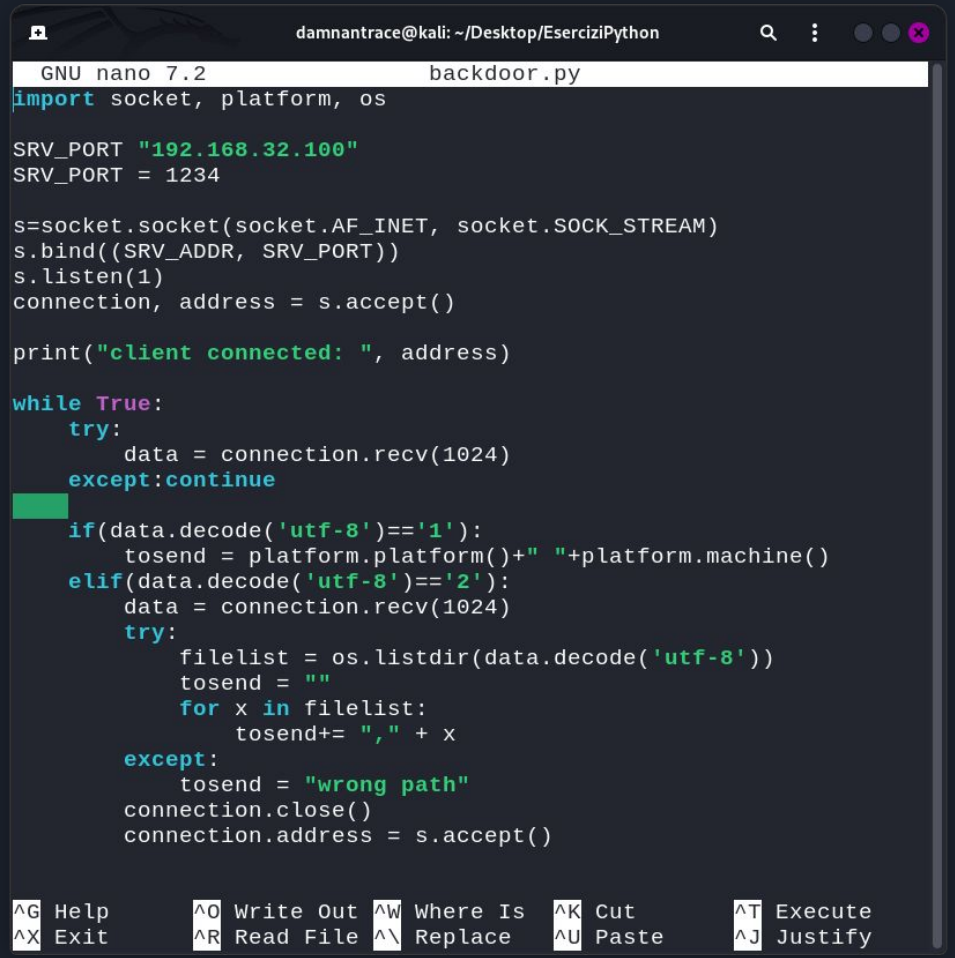
Le backdoor possono essere implementate in vari modi, come codice nascosto in un'applicazione, una porta di accesso nascosta o una funzionalità di controllo remoto non documentata. Il rilevamento e la gestione delle backdoor sono importanti nel contesto della sicurezza informatica, poiché possono essere sfruttate da attaccanti malevoli per compromettere la sicurezza di un sistema.

Codice 1

Il primo codice è una backdoor, crea un server socket che ascolta sulla porta 1234.

Quando un client si connette al server, il server accetta la connessione e stampa l'indirizzo del client. Successivamente, il server entra in un ciclo infinito in cui riceve i dati dal client.

Se il client invia il messaggio "1", il server risponde con una stringa che contiene il nome della piattaforma e la macchina su cui viene eseguito il codice. Se il client invia il messaggio "2", il server riceve un percorso di directory dal client e restituisce una stringa che contiene i nomi dei file nella directory specificata. Se il percorso non è valido, il server restituisce la stringa "wrong path"



Codice 2

Il secondo codice è il client da utilizzare per accedere alla backdoor della slide precedente.

Questo script prende in input indirizzo IP e porta del server a cui si vuole connettere, avvia la connessione e chiede all'utente cosa vuole fare:
0) per chiudere il programma e la connessione
1) ottenere le informazioni di sistema del server
2) restituire il contenuto di una directory del server inserita dall'utente