DEFINIZIONE DI BACKDOOR:

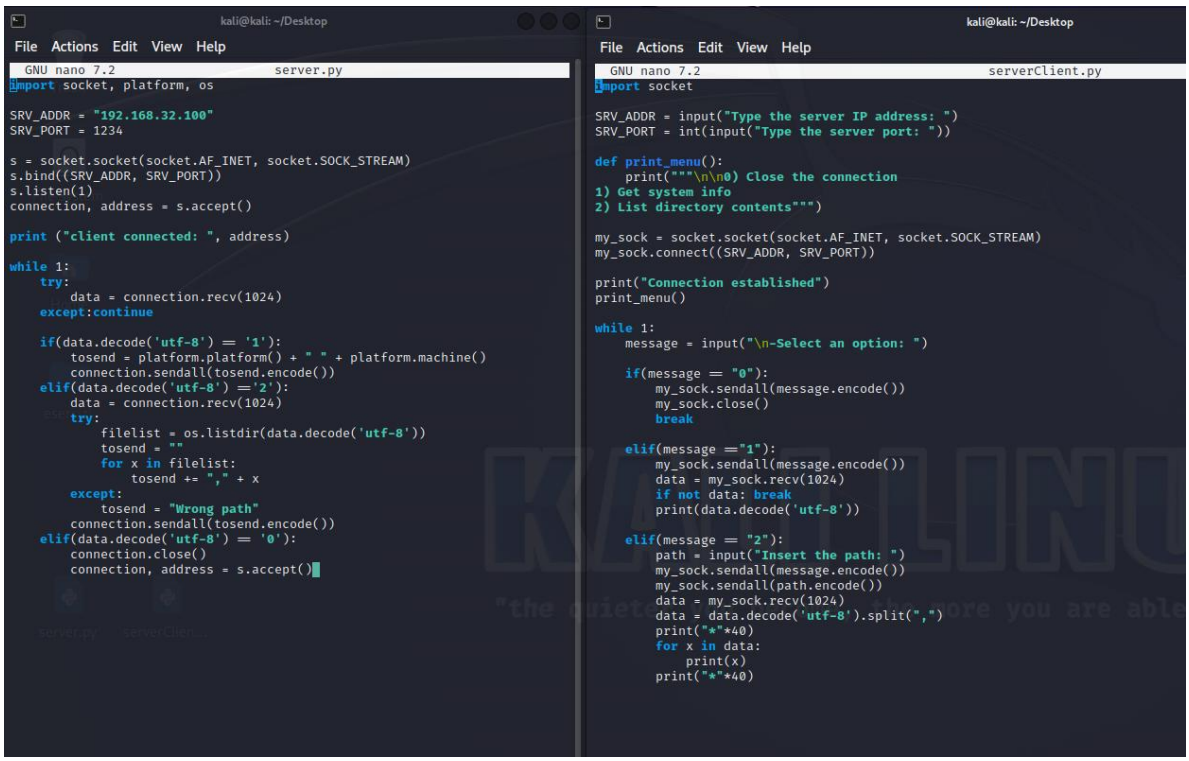
una backdoor è come una porta segreta nascosta in un sistema informatico o un software che permette a qualcuno di accedere o controllare il sistema senza autorizzazione. Spesso, questa porta segreta viene creata o sfruttata da BLACK HAT o da chi ha accesso al sistema per scopi nefasti. È una vulnerabilità che mette a rischio la sicurezza del sistema. Ecco alcune caratteristiche comuni delle backdoor:

1. **Accesso nascosto:** consente al blackhat di accedere al sistema o all'applicazione senza che l'utente se ne accorga.
2. **Controllo remoto:**i blackhat usano queste porte per eseguire comandi, rubare dati o effettuare altre azioni.
3. **Persistenza:** Le backdoor cercano di rimanere nascoste nel sistema il più a lungo possibile. Possono essere progettate per sopravvivere a riavvii del sistema e ad aggiornamenti software.
4. **Evasione delle difese:** i blackhat usano queste porte per evitare di essere rilavati da software di sicurezza, firewall e antivirus.
5. **Scopo malevolo:** Le backdoor sono spesso utilizzate per, come il furto di dati, il monitoraggio delle attività degli utenti o la compromissione del sistema.

Anche gli sviluppatori usano queste porte per cose tipo manutenzione o accessi di emergenza. Però l'abuso puo portare a problemi di sicurezza.

Per evitare gli attacchi atraverso le backdoor si possono usare password piu robuste, i firewall, e l'uso di politiche di accesso piu severe. Ed è importante formare gli utenti nella consapevolezza della sicurezza per evitare accessi non autorizzati nel sistema.

Codici di kali, dove il socket, crea un server, e crea un client



Dimostrazione