Questo codice Python utilizza il modulo socket per accettare connessioni TCP e visualizzare i comandi inviati dal client attaccato.

andiamo ad analizzarlo riga per riga:

attiva i servizi socket attivati.
Definisce l'indirizzo del server (SRV_ADDR) come una stringa vuota e
seleziona la porta del server (SRV_PORT) come 1234.
Crea un socket (s) utilizzando il protocollo IPv4 e il protocollo di trasporto TCP (socket.SOCK_STREAM).
Associa il socket all'indirizzo e alla porta ed
Inizia ad “ascoltare” per le connessioni in entrata. “1” indica che il server accetterà una sola connessione alla volta.
Accetta una connessione in entrata e stampa l'indirizzo del client.
Entra in un loop con (while 1) per gestire i comandi inviati dal client.
Dentro il loop, tenta di ricevere dati dalla connessione del client
Se i dati ricevuti sono "1", visualizza una stringa contenente le informazioni prese dalla “macchina attaccata”
Se i dati ricevuti sono "2", tenta di ricevere ulteriori dati rispetto ai precedenti, invia un messaggio di errore se non riesce
Se i dati ricevuti sono "0", chiude la sessione attuale e accetta una nuova sessione.
infine fa visualizzare i dati ricevuti dal client e chiude la sessione al termine dell'esecuzione.
Questo codice implementa un server TCP (ipv4) che accetta connessioni, gestisce informazioni inviati da un client e fornisce risposte in base ai comandi ricevuti

BACKDOOR

Una backdoor è una vulnerabilità o un meccanismo segreto che permette l'accesso non autorizzato a un sistema, spesso bypassando i normali controlli di autenticazione; un' apertura di sicurezza non documentata o una funzionalità "segreta" non nota agli utenti.
Inoltre, una backdoor può essere inserita deliberatamente da un programmatore o da un attaccante malevolo.
Scavalcare misure di sicurezza: elude le misure di sicurezza, consentendo a un attaccante di superare i controlli di sicurezza e ottenere l'accesso al sistema.
Accesso remoto: Un'autorizzazione segreta che consente a un utente di accedere al sistema da una posizione remota
Manutenzione nascosta: consente agli amministratori di accedere a determinate risorse senza rivelare la presenza agli utenti.
Elevazione dei privilegi: permette a un utente di ottenere privilegi più elevati rispetto a quelli usuali.
Installazione di malware: può essere utilizzata per introdurre malware in un sistema senza essere rilevata, offrendo all'attaccante un accesso.