PRATICA S3L2 – Giorgio Trovesi

Spiegare cosa è una backdoor e illustrare l'utilizzo dei 2 codici presenti nella traccia.

La backdoor o "Porta sul retro" è uno strumento che permette l'accesso da remoto ad un sistema informatico bypassando l'autenticazione.

Può essere pericolosa se usata da criminali informatici per ottenere informazioni sensibili, il controllo remoto o per effettuare attacchi.

Nell'ambito del Penetration Testing viene utilizzata dopo la privilege escalation e permette di non dover ripetere la fase degli expolit.

Primo codice

Nella parte iniziale codice viene creato il socket tramite la funzione *socket, bind* e *listen* ; con la funzione *accept* per autorizzare la connessione che servirà a recuperare le informazioni.

La seconda parte del codice gestisce i comandi che dovrà eseguire in base all'input ricevuto dal client:

1. Se il client invia "1" tramite le funzioni *platform* e *machine* raccoglierà informazioni riguardanti sistema operativo, versione e architettura del processore (32 o 64bit);
2. Se il client invia "2" tramite la funzione *listdir* otterrà una lista di tutti i file contenuti in una determinata directory;
3. Se il client invia "0" la connessione si interromperà.

Secondo codice

Dopo aver inserito l'indirizzo IP e la porta alla quale ci si vuole connettere, all'utente verrà visualizzato un menú con 3 scelte:

1. Con "0" interromperà la connessione tramite la funzione *close*;
2. Con "1" riceverà le informazioni raccolte dalle funzioni *platform* e *machine*;
3. Con "2" gli verrà chiesto di inserire il path nel quale vuole che venga usata la funzione *listdir* e successivamente riceverà le informazioni richieste.