EPICODE

Esercizio S3 – L4

L'esercizio di oggi consiste nel commentare/spiegare questo codice che fa riferimento ad una backdoor. Inoltre, spiegare cos’è una backdoor.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Qui sopra il codice completo

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

1. Nella prima riga di codice si importa il modulo socket che fornisce funzionalità per la rete in Python.
2. Nella seconda riga scritta si definisce la prima variabile, ovvero l’indirizzo ip che fungerà da server. L’indirizzo ip dev’essere pubblico.
3. Nella terza riga scritta si definisce la seconda variabile, ovvero la porta su cui ci si metterà in ascolto.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

1. La prima riga dell’immagine crea un socket utilizzando la funzione socket.socket(). Il primo parametro socket.AF\_INET specifica che si tratta di un socket di tipo IPv4, e il secondo parametro socket.SOCK\_STREAM specifica che si tratta di un socket TCP.
2. s.bind() associa l’ip con la porta. In questo modo il server è in ascolto su quell’ip e su quella porta per le connessioni in ingresso.
3. s. listen(1) mette il socket in ascolto. L’1 indica che si accetta una sola connessione in entrata alla volta.
4. connection è il nuovo socket creato per comunicare con il client, e address contiene l'indirizzo IP e la porta del client. Si accetta una comunicazione in entrata utilizzando accept(). Questo metodo blocca il programma finché non viene stabilita una connessione da un client.
5. Print (“client connected: “, address) stampa un messaggio per indicare che un client è stato connesso e visualizza l’indirizzo del client.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

1. Si apre un ciclo while 1, dove 1 sta per True. Ovvero un ciclo while infinito.
2. Inizia un blocco di codice in cui si gestiscono delle eventuali eccezioni.
3. Utilizza recv(1024) per ricevere dati dal client, con una dimensione massima di 1024 byte alla volta.
4. Se durante la ricezione dei dati si verifica un’eccezione il programma continua a ricevere.
5. Si decodificano i dati ricevuti in utf-8 e verifica se sono uguali a 1.
6. Se è così prepara una stringa da inviare contenente il nome della piattaforma e della macchina.
7. Invia la stringa in formato utf-8.
8. Se i dati ricevuti sono uguali a 2, allora riceve ulteriori dati dalla connessione.
9. Un altro blocco di gestione delle eccezioni.
10. Ottiene la lista dei file nella directory specificata dai dati ricevuti.
11. Prepara la risposta con una stringa vuota.
12. Concatena il nome di ciascun file alla stringa di risposta separandoli con virgole.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

1. Se si verifica un’eccezione durante il tentativo di ottenere la lista dei file imposta la stringa di risposta a “Wrong path” e la invia.
2. Se i dati ricevuti sono uguali a zero chiude la connessione.
3. Accetta una nuova connessione.

Una backdoor è, metaforicamente, l’entrata sul retro di una rete.  
Nasce dall’esigenza dei programmatori/sviluppatori di non dover accedere con utente e password in ogni dispositivo di una rete quando si deve, per esempio, fare degli aggiornamenti (si pensi ad una grande rete aziendale con centinaia di dispostivi). Trattandosi di un’entrata secondaria è molto meno difesa. Per questo possono essere spesso sfruttate dai criminali informatici per entrare nelle reti aggirando i sistemi di difesa.