SPIEGAZIONE CODICE S3-L4

Import socket, platform, os Qui vengono inseriti tre moduli: socket che ci permette di accedere alle funzioni connect(), send() e recv(). platform che permette di leggere le caratteristiche hardware della macchina e la versione di python. os che ha diverse funzioni necessarie a far interagire il programma e il sistema operativo del computer

SVR_ADDR = “” Questa variabile indica l’indirizzo IP da ascoltare, non specificando alcun valore considererà tutti gli indirizzi IP disponibili

SVR_PORT = 1234 Questa variabile indica la porta su cui ascoltare
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM) Viene creato un oggetto socket dove il primo parametro corrisponde alla tipologia di indirizzo, in questo caso c’è AF_INET che indica gli indirizzi IPv4, il secondo parametro indica la tipologia di socket che vogliamo creare, SOCK_STREAM indica socket di tipo TCP

s.bind((SRV_ADDR, SRV_PORT)) Qui avviene l’associazione del socket, con .bind il socket viene legato all’indirizzo IP e alla porta specificati come variabili

s.listen(1) Qui con .listen si configura il socket(s) per mettere in ascolto il socket e prepararlo a ricevere connessioni in entrata, tra le parentesi viene indicato il backlog che indica il numero massimo di connessioni che verranno tenute in attesa prima che il sistema inizi a rifiutarne di nuove

connection, address = s.accept( ) Con s.accept() viene accettata una connessione, restituisce una tupla contenente due socket “connection” e “address”

print("client connected: ", address) Viene stampato l’indirizzo del client connesso

while 1:
try: Per eseguire il blocco di codice sotto
data = connection.recv(1024) Riceve fino a 1024 byte di dati dal socket connection
except:
continue Se except rileva errori esegue continue che fa ricominciare da capo il ciclo in questo modo vengono gestiti momentanei problemi di ricezione senza far terminare il server
if(data.decode('utf-8') == '1'): Il primo parametro di if decodifica I dati ricevuti dal formato byte in una stringa utilizzando la codifica UTF-8, if verifica se questi dati sono la stringa ‘1’
tosend = platform.platform() + " " + platform.machine() Se la condizione è vera crea una stringa contenente le informazioni sul sistema operativo e la macchina
connection.sendall(tosend.encode()) Codifica in formato byte la stringa da inviare con tosend.encode e la invia al socket con connection.sendall

```
elif(data.decode('utf-8') == ‘2'):
    data = connection.recv(1024)
    try:
        filelist = os.listdir(data.decode(‘utf-8') )
        tosend = ""
        for x in filelist:
            tosend += "," + x
    except:
      tosend = "Wrong path"
    connection.sendall(tosend.encode( ) )
```

Qui il se il client invia il la stringa ‘2’ il server questa volta tenterà invece di ricevere una stringa contenente un percorso di directory, poi risponderà con una lista dei file in quella directory. Se il percorso è errato risponde con “Wrong path”

```
elif(data.decode('utf-8') == '0'):
   connection.close()
   connection, address = s.accept()
```

Se il client invia la stringa ‘0’ il server chiude la connessione corrente e ne accetta una nuova ottenendo un nuovo socket connection e address questo permette al client di ricollegarsi

BACKDOOR

Le backdoor, letteralmente "porte sul retro", sono righe di codice informatico che permettono a un utente di accedere come amministratore a un computer o un sito web senza alcuna autorizzazione. Le backdoor quindi consentono a malintenzionati di entrare da remoto nel sistema informatico della vittima (nel quale è stata creata la backdoor), ottenendo così il controllo completo del sistema.
Le backdoor possono essere installate da malware, come i trojan, che sembrano software legittimi ma che, una volta eseguiti, forniscono accesso remoto al sistema infetto.

ALCUNE DIFFERENZE:

- Backdoor e Botnet:
  - Una backdoor rappresenta un singolo punto di accesso nascosto in un sistema specifico. Viene utilizzata per mantenere un accesso non autorizzato al sistema.
  - Una botnet, invece, è una rete di numerosi sistemi infetti e controllati collettivamente da un attaccante. La botnet è più sofisticata e viene spesso utilizzata per attacchi su larga scala.
- Trojan:
  - I trojan possono essere considerati come veicoli per la distribuzione di backdoor e per l'infezione iniziale di sistemi che verranno poi integrati in una botnet.