Relazione sul Programma di Simulazione di UDP Flood

Obiettivo

L'obiettivo di questo progetto è stato quello di sviluppare un programma in Python in grado di simulare un attacco **UDP Flood**. Un attacco UDP Flood consiste nell'invio massivo di pacchetti UDP verso una macchina target, sovraccaricandola e potenzialmente interrompendo il suo normale funzionamento. Il programma consente all'utente di specificare l'IP della macchina target, la porta UDP in ascolto, e il numero di pacchetti da inviare, ciascuno di 1 KB di dimensione.

Funzionamento del Programma

Il programma si compone principalmente delle seguenti fasi:

1. **Input dell'Utente**:
   - Il programma utilizza il modulo `argparse` per richiedere tre input da parte dell'utente:
     - L'indirizzo IP della macchina target.
     - La porta UDP della macchina target su cui inviare i pacchetti.
     - Il numero di pacchetti da inviare.
2. **Creazione di un Pacchetto UDP**:
   - Una volta ricevuti gli input, il programma crea un pacchetto UDP della dimensione di **1 KB** (1024 byte).
   - Il modulo `random` viene utilizzato per generare un pacchetto contenente **dati casuali**, tramite la funzione `random._urandom(1024)`, che garantisce la creazione di una sequenza casuale di byte.
3. **Invio dei Pacchetti**:
   - Utilizzando il modulo `socket`, il programma crea un socket UDP.
   - In un ciclo `for`, il programma invia i pacchetti generati al target, uno alla volta. Ogni pacchetto contiene esattamente 1 KB di dati.
   - Per ogni pacchetto inviato, il programma stampa un messaggio per indicare l'avanzamento dell'attacco.
4. **Chiusura del Socket**:
   - Al termine dell'invio dei pacchetti, il socket viene chiuso per liberare le risorse utilizzate.

Descrizione Tecnica del Codice

Il programma è suddiviso in due sezioni principali:

- **udp_flood(target_ip, target_port, num_packets)**: Questa è la funzione principale del programma, che esegue l'UDP flood. Riceve come input l'indirizzo IP del target, la porta UDP e il numero di pacchetti da inviare.
- **argparse**: Questo modulo consente di inserire comodamente i parametri da riga di comando (target IP, porta, e numero di pacchetti).

Il codice è stato progettato per essere facilmente eseguibile da riga di comando, con un'interfaccia semplice e intuitiva. Ad esempio, eseguendo il comando:

```
python UDP.py 192.168.50.152 137
```

Verranno inviati 1000 pacchetti da 1 KB ciascuno all'indirizzo IP `192.168.50.152` sulla porta UDP `137`.

Componenti Utilizzati

1. **Modulo `socket`**: È stato utilizzato per la creazione e gestione delle connessioni UDP. Il socket UDP è un meccanismo di trasmissione "connectionless", dove i pacchetti vengono inviati senza la necessità di stabilire una connessione stabile tra il client e il server.
2. **Modulo `random`**: Viene utilizzato per generare byte casuali che formano il contenuto di ciascun pacchetto inviato. Questo simula l'invio di dati reali, sebbene i dati in questo caso siano casuali.
3. **Modulo `argparse`**: Utilizzato per acquisire gli argomenti da riga di comando, rendendo l'interfaccia del programma più flessibile e configurabile dall'utente.

Uso Responsabile

L'attacco UDP Flood è una tecnica che può essere utilizzata in contesti legali, ad esempio per testare la resistenza di un proprio sistema o per valutare la capacità di difesa di un'infrastruttura di rete. **Non deve essere utilizzato per attacchi illegali o senza il consenso del proprietario del sistema target**, poiché ciò può violare diverse leggi, incluse quelle relative agli attacchi di tipo denial of service (DoS).

Conclusioni

Questo progetto ha permesso di simulare un attacco **UDP Flood** in un ambiente controllato utilizzando il linguaggio Python. Il programma offre una base flessibile per comprendere come funziona l'invio massivo di pacchetti UDP e i potenziali impatti su un sistema bersaglio. Tuttavia, va utilizzato con grande attenzione e solo in scenari in cui si ha pieno controllo sull'ambiente di destinazione.