S3/L5

ATTACCO DOS

TRACCIA

Gli attacchi di tipo Dos, ovvero denial of services, mirano a saturare le richieste di determinati servizi rendendoli così indisponibili con
conseguenti impatti sul business delle aziende.
L’esercizio di oggi è scrivere un programma in Python che simuli un UDP flood, ovvero l’invio massivo di richieste UDP verso una
macchina target che è in ascolto su una porta UDP casuale.

Requisiti:

- Il programma deve richiedere l’inserimento dell’IP target.
- Il programma deve richiedere l’inserimento della porta target.
- La grandezza dei pacchetti da inviare è di 1 KB per pacchetti
- Il programma deve chiedere all’utente quanti pacchetti da 1 KB inviare.

01

Questo codice Python implementa un attacco di tipo UDP flood attraverso l'uso di socket e thread multipli. Innanzitutto, il programma importa le librerie necessarie come ***socket*** per la comunicazione di rete, random per la generazione di dati casuali, e ***threading*** per gestire più operazioni simultaneamente. È utilizzato anche ***colorama*** per colorare l'output per migliorarne l'accessibilità.

CODE

02

Nella funzione ***udp_flood(target_ip, target_port, num_packets)***, viene creato un ***socket UDP (socket.SOCK_DGRAM)*** per inviare pacchetti di dati. Viene generato un byte array di 1KB di dati casuali che verranno inviati ripetutamente al target specificato attraverso il metodo sendto.
Se l'invio ha successo per il numero desiderato di pacchetti, viene stampato un messaggio verde di completamento dell'attacco; altrimenti, viene gestito qualsiasi eccezione mostrando un messaggio di errore in rosso.

03

Nella funzione ***main()***, l'utente inserisce l'indirizzo IP e la porta del target, oltre al numero di pacchetti da inviare e il numero di thread da utilizzare per l'attacco. Se i valori inseriti sono validi, il programma divide equamente il numero di pacchetti tra i thread creati, ognuno dei quali esegue la funzione ***udp_flood*** in parallelo.
Al termine dell'attacco, il programma aspetta che tutti i thread completino prima di terminare.

THREADING

Utilizzare il threading nel contesto di uno script di attacco di tipo UDP flood significa creare più thread per inviare pacchetti contemporaneamente (allo stesso tempo) piuttosto che in sequenza (uno dopo l'altro).
Questo simula “un'inondazione” di pacchetti più intensa verso il bersaglio, rendendo l'attacco potenzialmente più efficace aumentando il volume e la velocità dei pacchetti inviati.

Vantaggi dell'uso del threading in un attacco UDP flood:

- **Invio parallelo**: Più thread funzionano in parallelo, ciascuno inviando pacchetti contemporaneamente.
- **Aumento dell’invio**: Un maggior numero di pacchetti può essere inviato in un periodo di tempo più breve perché più thread lavorano simultaneamente
- **Attacco più efficace**: Aumentando il numero di pacchetti inviati per unità di tempo, l'attacco può potenzialmente sopraffare il bersaglio in modo più efficace.

Utilizzando questa tecnica, l'attacco riesce a sfruttare meglio le risorse disponibili e a generare un traffico più elevato verso il bersaglio, aumentando così le probabilità di successo nell'intasare e disturbare il servizio.