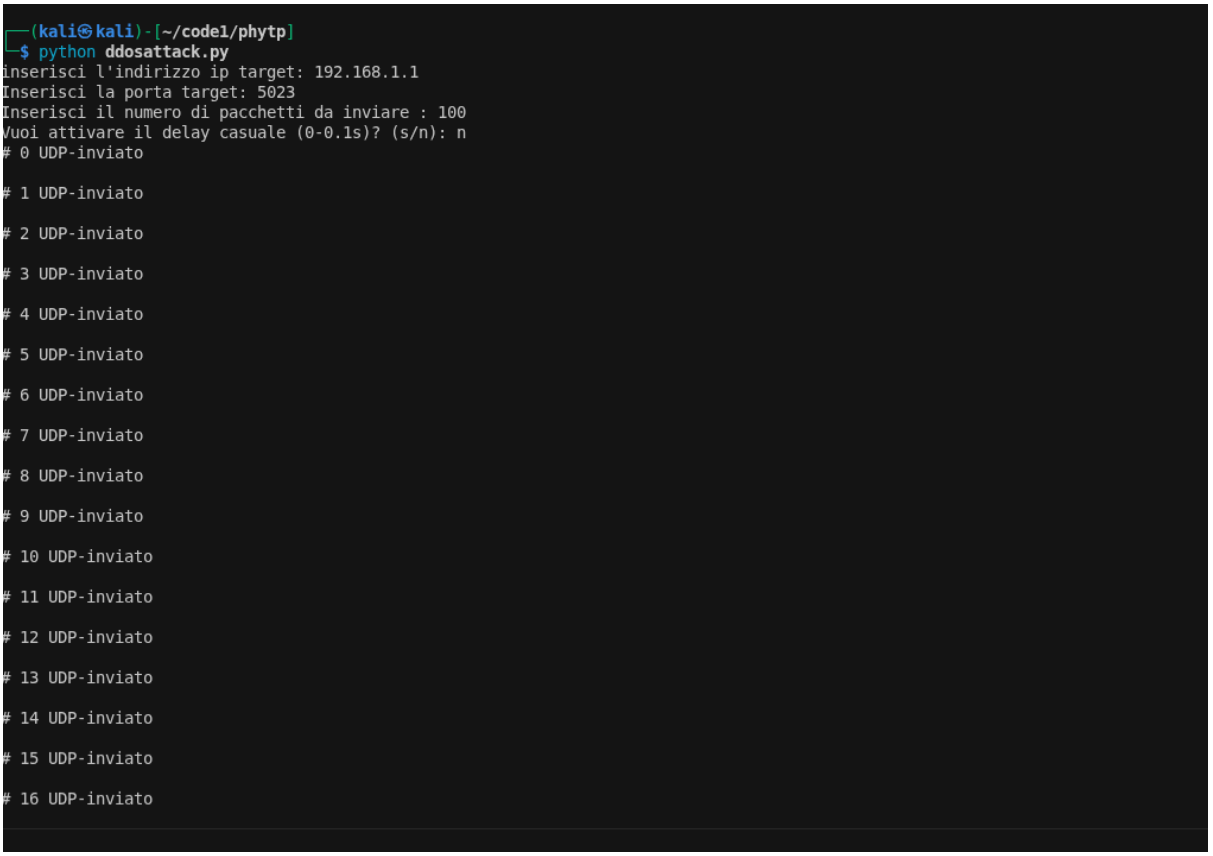
Report DDos Flood

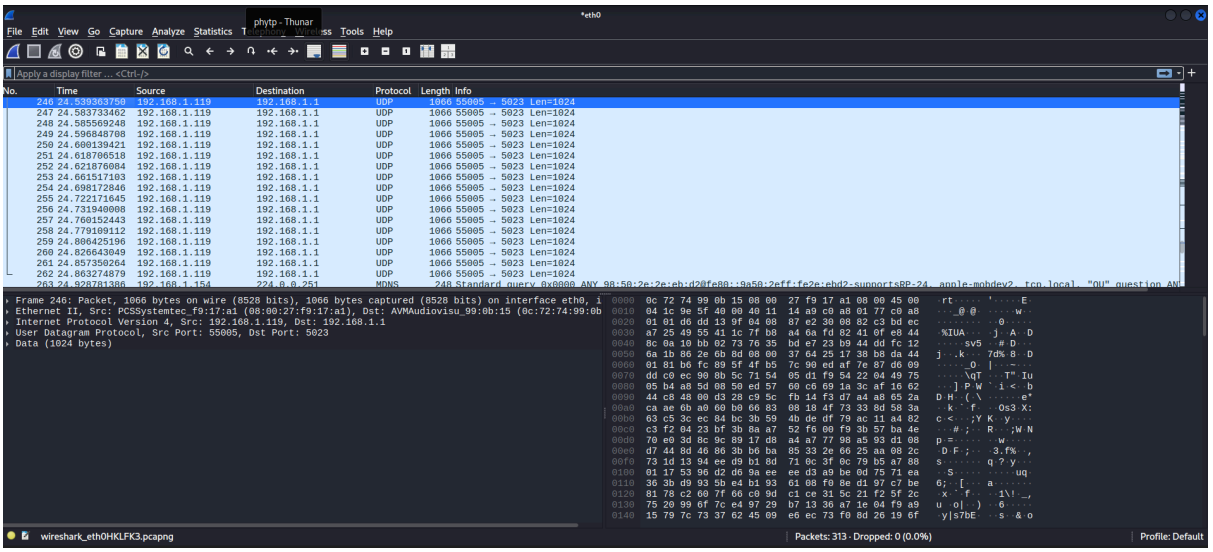
Studente :Pancrazio Giuzio Data:06/02/26

Traccia: Gli attacchi di tipo DDoS, ovvero Distributed 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 (nel nostro caso un DoS. Requisiti:-Il programma deve richiedere l'inserimento dell'IP target (input)-Il programma deve richiedere l'inserimento della porta target (input)-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 (input)

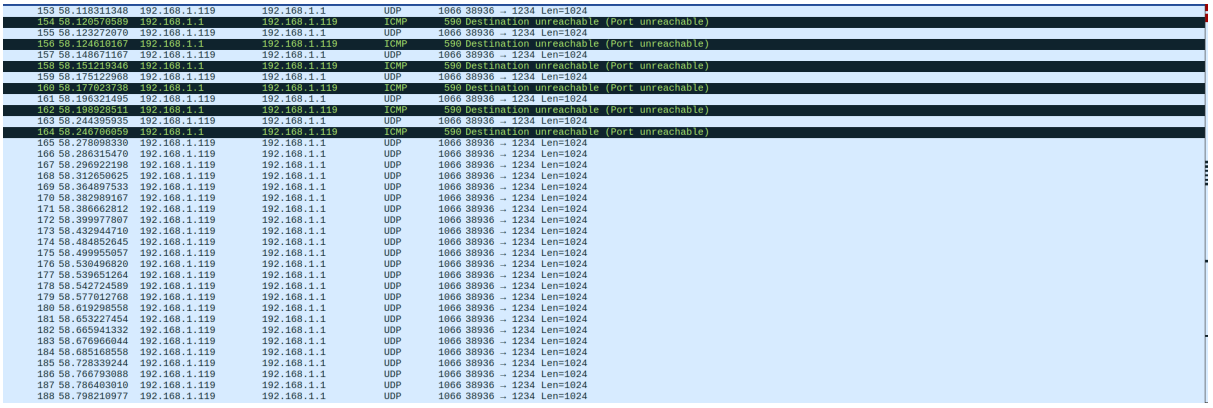
Svoglimento :
Lo scritp in python creato mirava a generare dei pacchetti udp in maniera randomica , (il facoltativo permetteva una latenza sempre randomica in mezzo)
per generare questo script le prime librerie importanti da utilizzare sono state RANDOM ,SOCKET e TIME per il facoltativo che abbiamo implementato nel codice.
Lo script si trova in allegato e come si puo'notare le fasi della costruzione sono state spiegate con il# commentando le funzioni .
a differenza di utilizzare il loopback in questo caso ho provato a floodare la mia stessa rete , in quanto avrei avuto un responso prima di mettere su un server virtuale.



come si puo’ vedere il flood ha funzionato e tramite wireshark ho catturato i pacchetti ricevuti,



sotto propongo un ‘altra immagine catturata sempre con wireshark



come si puo’ notare nei primi sei pacchetti il router risponde quindi l’host è raggiungibile ma la porta è chiusa, nei pacchetti successivi ,invece si vede proprio come il nostro attacco vada a segno in quanto il router non riesce ad elaborare le risposte ICMP prima fornite elaborando comunque le richieste ,ma avendone troppe non riesce a dare risposta.
NB:nella seconda immagine cambia la porta di ricezione ma il principio rimane lo stesso.