Consegna S6/L3

Marco Falchi

Introduzione e consegna

Gli attacchi DDoS (Distributed Denial of Service) sono azioni mirate a sovraccaricare un sistema, rendendo i servizi indisponibili per gli utenti legittimi. Questo esercizio simula un attacco UDP Flood, dove pacchetti UDP vengono inviati in massa verso una macchina target.

L'obiettivo è stato costruire un programma in Python per:

1. Scansionare le porte di un target.
2. Eseguire un attacco UDP Flood su una porta specifica.

Funzionalità del Programma

Scansione delle Porte

- Identifica le porte aperte su un IP specificato dall'utente.
- Utilizza il protocollo TCP per rilevare i servizi in ascolto.
- Mostra tutte le porte aperte trovate.

Attacco UDP Flood

- Invia pacchetti UDP di dimensioni configurabili verso una porta selezionata.
- Permette di scegliere il numero di pacchetti da inviare.
- Fornisce un'interfaccia grafica per una facile gestione.

Struttura del Programma

Il programma è diviso in due sezioni principali:

Scansione delle Porte

L'utente inserisce l'IP target.

Il programma esegue una rapida scansione delle porte.

Le porte aperte vengono visualizzate in un elenco.

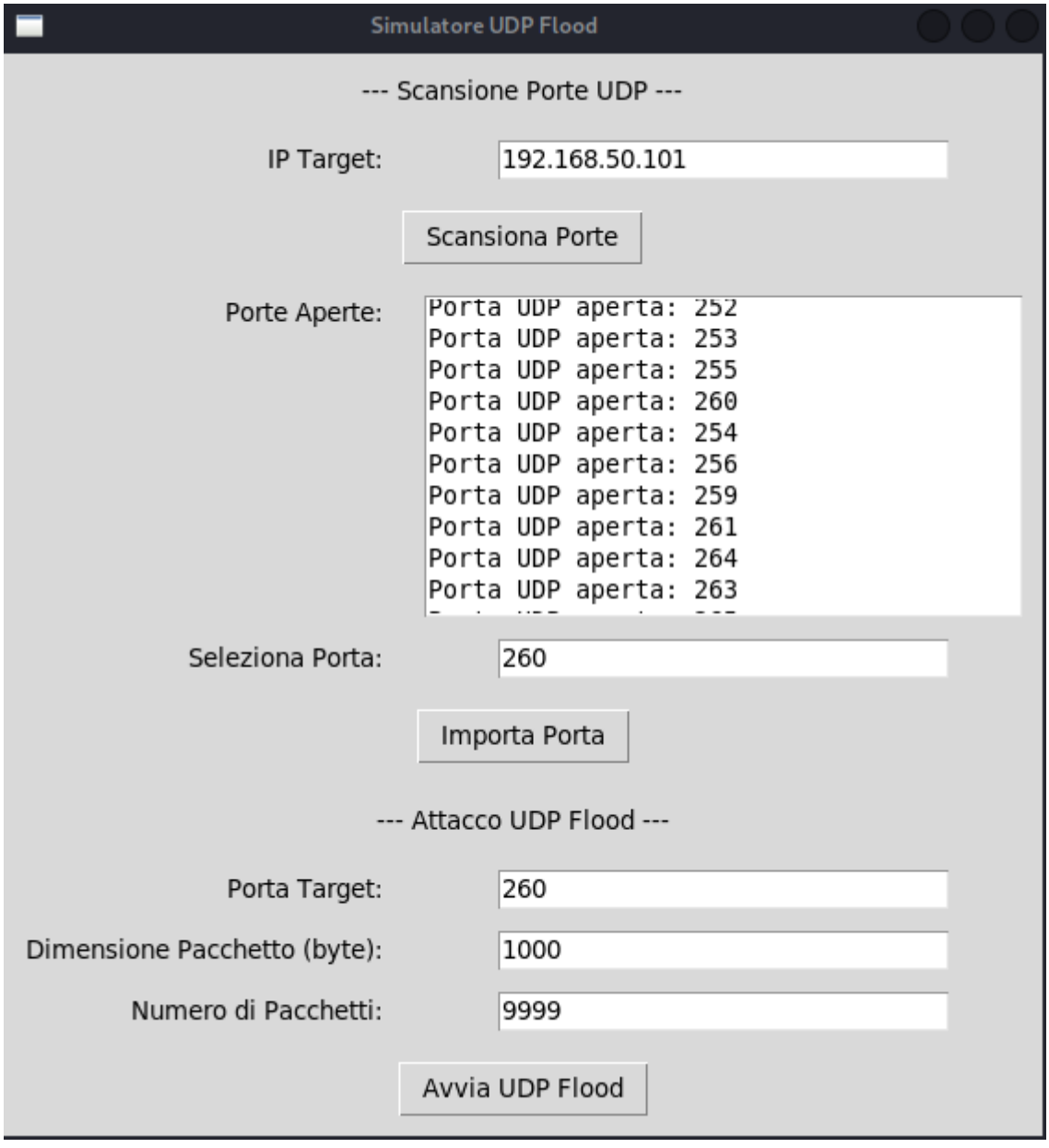
L'utente può selezionare una porta dall'elenco per l'attacco.

Attacco UDP Flood

L'utente specifica:

- IP target (importabile dalla sezione precedente).
- Porta target.
- Dimensione dei pacchetti (default: 1024 byte).
- Numero di pacchetti da inviare.

2. **Il programma invia pacchetti verso il target usando un socket UDP.**



Come Testare il Programma

Utilizzare un ambiente sicuro come una macchina virtuale con Metasploitable2, come nel nostro caso.

Verifica del Traffico UDP

Per assicurarsi che i pacchetti arrivino al target:

1. Ho usato una funzione di ascolto e monitoraggio del traffico come tcpdump:

sudo tcpdump -i eth0 udp port <PORTA>

2. Controlla che i pacchetti UDP siano visibili nel traffico catturato.