

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.

The screenshot shows a graphical user interface for a 'Simulatore UDP Flood' (UDP Flood Simulator). The window has a title bar with the text 'Simulatore UDP Flood' and standard macOS window controls. The interface is divided into two main sections: '--- Scansione Porte UDP ---' and '--- Attacco UDP Flood ---'.

--- Scansione Porte UDP ---

- IP Target:** A text input field containing '192.168.50.101'.
- Scansiona Porte:** A button to initiate the port scan.
- Porte Aperte:** A list box displaying the results of the scan, showing 11 open UDP ports: 252, 253, 255, 260, 254, 256, 259, 261, 264, and 263.
- Seleziona Porta:** A text input field containing '260'.
- Importa Porta:** A button to import the selected port.

--- Attacco UDP Flood ---

- Porta Target:** A text input field containing '260'.
- Dimensione Pacchetto (byte):** A text input field containing '1000'.
- Numero di Pacchetti:** A text input field containing '9999'.
- Avvia UDP Flood:** A button to start the flood attack.

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.

```
09:02:26.608744 IP 192.168.50.100.38926 > 192.168.50.101.260: UDP, length 1000
09:02:26.609200 IP 192.168.50.100.50010 > 192.168.50.101.260: UDP, length 1000
09:02:26.609534 IP 192.168.50.100.40108 > 192.168.50.101.260: UDP, length 1000
09:02:26.610211 IP 192.168.50.100.50927 > 192.168.50.101.260: UDP, length 1000
09:02:26.610446 IP 192.168.50.100.60014 > 192.168.50.101.260: UDP, length 1000
09:02:26.610916 IP 192.168.50.100.50203 > 192.168.50.101.260: UDP, length 1000
09:02:26.611201 IP 192.168.50.100.58706 > 192.168.50.101.260: UDP, length 1000
09:02:26.611682 IP 192.168.50.100.36444 > 192.168.50.101.260: UDP, length 1000
09:02:26.612025 IP 192.168.50.100.33976 > 192.168.50.101.260: UDP, length 1000
09:02:26.613497 IP 192.168.50.100.46356 > 192.168.50.101.260: UDP, length 1000
09:02:26.613831 IP 192.168.50.100.49186 > 192.168.50.101.260: UDP, length 1000
09:02:26.614084 IP 192.168.50.100.51476 > 192.168.50.101.260: UDP, length 1000
09:02:26.614651 IP 192.168.50.100.42734 > 192.168.50.101.260: UDP, length 1000
09:02:26.615083 IP 192.168.50.100.49527 > 192.168.50.101.260: UDP, length 1000
09:02:26.615221 IP 192.168.50.100.38588 > 192.168.50.101.260: UDP, length 1000
09:02:26.615683 IP 192.168.50.100.57678 > 192.168.50.101.260: UDP, length 1000
09:02:26.616570 IP 192.168.50.100.46614 > 192.168.50.101.260: UDP, length 1000
09:02:26.616712 IP 192.168.50.100.34273 > 192.168.50.101.260: UDP, length 1000
09:02:26.616958 IP 192.168.50.100.48004 > 192.168.50.101.260: UDP, length 1000
09:02:26.617399 IP 192.168.50.100.52637 > 192.168.50.101.260: UDP, length 1000
09:02:26.617988 IP 192.168.50.100.41179 > 192.168.50.101.260: UDP, length 1000
09:02:26.617990 IP 192.168.50.100.33456 > 192.168.50.101.260: UDP, length 1000
09:02:26.618494 IP 192.168.50.100.44702 > 192.168.50.101.260: UDP, length 1000
09:02:26.618626 IP 192.168.50.100.42362 > 192.168.50.101.260: UDP, length 1000
```