המרכז לחינוך סייבר
CYBER EDUCATION CENTER

סין - Flood

גורמים זדוניים מנסים לבצע עלינו Denial of service (מניעת שירות) באמצעות מתקפת SYN-Flood. המתקפה מגיעה ממספר רב של כתובות IP.

נבחרתם לעמוד בראש צוות המגינים- לרשותכם קובץ הסנפה שהוקלט תוך כדי המתקפה. עליכם לכתוב סקריפט פייתון שמזהה את כתובות ה-IP של התוקפים ושומר אותם לקובץ.

https://data.cyber.org.il/networks/SYNflood.pcapng

שימו לב:

1. בתוך סקריפט הפייתון שלכם, השתמשו בסקאפי על מנת לנתח את הפקטות
2. סקאפי יכול לקרוא קבצי pcap באמצעות הפקודה rdpcap. לדוגמה:

```
pcapFile = rdpcap("SynFloodSample.pcap")
```

3. לאחר מכן ניתן לעבור על הפקטות באמצעות לולאת for כגון:

```
for pkt in pcapFile:
    ...
```

בהצלחה!

קרדיט לקובץ ההסנפה - https://blog.packet-foo.com/