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.

www.cyber.org.il/networks/SynFloodSample.pcap

קרדיט לקובץ ההסנפה: www.pcapr.net

הדרכה:

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:
    ...
```

טיפ:
ניתן לקבל את הזמן המדויק שבו פקטה התקבלה באמצעות השדה time.
לדוגמה pkt.time.

בהצלחה!