Để kiểm tra xem một tệp có bị **nén, đóng gói (packed) hoặc bị anti-reverse (unpacked) hay không**, bạn có thể sử dụng một số phương pháp sau.

**🔹 1. Kiểm tra với file**

Lệnh này giúp bạn kiểm tra xem tệp có chứa dấu hiệu của **UPX, packed sections** hay không:

file crackme100

👉 Nếu tệp bị nén, kết quả có thể xuất hiện như:

crackme100: ELF 64-bit LSB executable, dynamically linked, stripped, packed with UPX

➡️ Nếu có chữ **"packed with UPX"**, nghĩa là tệp đã bị **nén bằng UPX**.

**🔹 2. Kiểm tra bằng strings**

Nếu tệp bị nén hoặc đóng gói, lệnh strings sẽ trả về rất ít chuỗi có thể đọc được.

strings crackme100 | less

👉 Nếu chỉ có **một vài chuỗi lộn xộn**, khả năng cao là nó đã bị **packed**.

**🔹 3. Kiểm tra entropy (độ hỗn loạn của dữ liệu)**

Nếu tệp bị nén hoặc đóng gói, nó sẽ có entropy cao (gần 8.0). Dùng ent để kiểm tra:

ent crackme100

👉 Nếu entropy **cao hơn 7.5**, khả năng lớn là tệp đã bị **nén hoặc packed**.

**🔹 4. Sử dụng checksec để xem cấu trúc bảo vệ**

Nếu tệp có bảo vệ **PIE, RELRO, NX, Canaries**, nó có thể đã được bảo vệ chống reverse.

checksec --file=crackme100

**🔹 5. Dùng binwalk để tìm dấu hiệu packer**

binwalk crackme100

Nếu có dấu hiệu của **UPX, ASPack, Armadillo**, nghĩa là tệp đã bị đóng gói.

**🔹 6. Nếu nghi ngờ UPX, thử giải nén**

Nếu file hoặc binwalk phát hiện UPX, bạn có thể thử giải nén:

upx -d crackme100

👉 Nếu giải nén thành công, tệp đã bị **nén bằng UPX**.

**🔹 7. Dùng radare2 để kiểm tra section**

Mở tệp bằng radare2:

r2 -AA crackme100

Sau đó, kiểm tra các section:

iS

🔹 Nếu có **section lạ như .upx0, .upx1 hoặc thiếu .text**, tệp có thể đã bị **packed**.

**🛠 Kết luận**

🔹 **Tệp có bị packed hay không?** → Kiểm tra với file, strings, ent, binwalk.  
🔹 **Nếu là UPX?** → Dùng upx -d để giải nén.  
🔹 **Nếu nghi ngờ packer khác?** → Dùng radare2, binwalk để phân tích sâu hơn.

🚀 **Bạn có thể thử chạy các lệnh trên và gửi kết quả để tôi phân tích giúp bạn!**