**Write-Up for "Reverse this Linux executable"**

**Author:** Mubarak Mikail  
**Category:** Reverse Engineering  
**Challenge:** Analyze and reverse a Linux ELF binary to extract a flag.

**Description**

The challenge involves analyzing a Linux ELF executable that has been packed with UPX (Ultimate Packer for Executables). The task is to reverse-engineer the binary to extract the flag.

**Step-by-Step Solution**

**1. File Analysis**

Start by identifying the binary type:

file out

Output:

out: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, no section header

**Analysis:**

* The file is a **64-bit Linux ELF executable**.
* It is **statically linked**, meaning all required libraries are included in the binary.
* The message **"no section header"** strongly suggests that the binary is packed, likely to obscure its original structure.

**2. Detect UPX Packing**

To confirm the binary is packed with UPX, use the strings command:

strings out | grep -i "packed"

Output:

$Info: This file is packed with the UPX executable packer http://upx.sf.net $

This confirms the binary was packed with UPX.

**3. Install UPX**

Ensure UPX is installed on the system to unpack the binary. Use the following commands to install UPX on Ubuntu:

sudo apt update

sudo apt install upx-ucl

Verify the installation:

upx --version

**4. Unpack the Binary**

To unpack the binary, use:

upx -d out

Output:

Ultimate Packer for eXecutables

Copyright (C) 1996 - 2024

UPX 4.2.2 Markus Oberhumer, Laszlo Molnar & John Reiser Jan 3rd 2024

File size Ratio Format Name

-------------------- ------ ----------- -----------

877724 <- 336512 38.34% linux/amd64 out

Unpacked 1 file.

The binary has been successfully unpacked, increasing its size and restoring the original section headers.

**5. Analyze the Unpacked Binary**

After unpacking, verify the file structure:

file out

Check the ELF headers:

readelf -h out

These steps confirm that the binary is now in a readable and analyzable state.

**6. Extract the Flag**

Use the strings command to extract readable text from the binary:

strings out

Output (truncated for clarity):

**Phân tích chuỗi hex**

Các chuỗi bắt đầu bằng:

* **7069636fH**
* **4354467bH**
* Và tiếp nối với các chuỗi khác như:
  + 5539585fH
  + 556e5034H
  + 636b314eH
  + 365f4231H
  + 6e345269H
  + 33535f36H
  + 66663936H
  + 3465667dH

Rõ ràng, đây là một chuỗi được mã hóa dưới dạng **hexadecimal**, có thể là một **flag CTF**.

**Cách giải mã chuỗi hex**

1. Gộp các chuỗi hex lại thành một chuỗi duy nhất:

plaintext

7069636f4354467b5539585f556e5034636b314e365f42316e34526933535f36666639363465667d

1. Dùng lệnh echo để giải mã:

bash

echo "7069636f4354467b5539585f556e5034636b314e365f42316e34526933535f36666639363465667d" | xxd -r -p

1. Kết quả sẽ hiển thị chuỗi đã được giải mã. Ví dụ:

picoCTF{...}

**Flag**

picoCTF{U9X\_UnP4ck1N6\_B1n4Ri3S\_6ff964ef}

.