Mission Name

StrangerStrings

Background

Claire and Ethan leave Paris, heading to Euphea in Shanghai - Their transport is hijacked, changing course to an unknown destination. Ethan has to battle the autopilot of the Sky-Cage. He successfully hacks into the system. But doesn't stop the ambush. Dr.Pinche encourages Ethan to run a simulator to check if bug works perfect.

Technical High-Level Overview

A Windows PE binary is provided to the player. The goal of this challenge is to identify encrypted strings, acting as a simulator to catch the bug. Taking into account the level of this challenge, player should use a tool named *floss* from FireEye due to RC4 encryption was used to hide the “bug”. This tool eases the analysis of encrypted strings with any encryption knowledge or reversing capacities.

Short Description

You´re going to act as a simulator to catch the bug. For this purpose, you must analyse a Windows PE binary to locate encrypted strings.

Mission Description

You´re going to act as a simulator to catch the bug. For this purpose, you must analyse a Windows PE binary to locate encrypted strings. Once you see the main string, please insert the number. We know your level in terms of reversing, so use a specific tool located in your computer to achieve it.

Location

MOZAMBIQUE - SHAX - DR PINCHE

Tools

- floss

Questions

How many Unicode strings were you able to find?

- 2

Which compiler was used?

- GNU Compiler

Which language was used to compile it?

- C

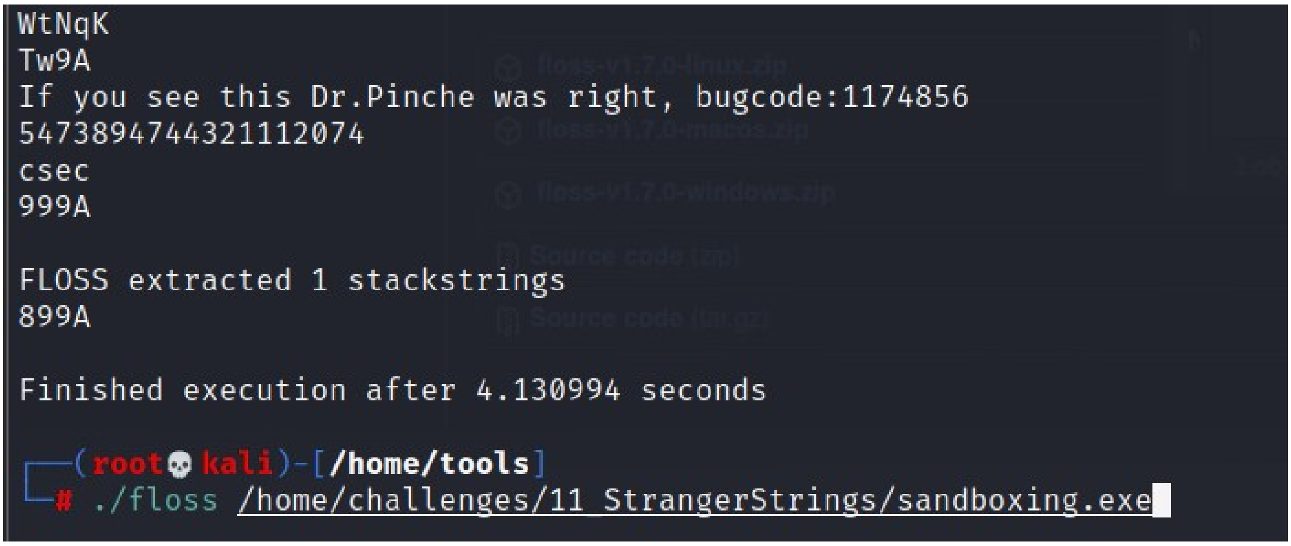
Hints

1. Inside the binary, there´s an encrypted string
2. The encryption method is RC4.
3. Use the tool FLOSS to decrypt it.

Write Up

Linux Method

Run ./floss /home/Challenges/11_StrangerStrings/sandboxing.exe from /homt/tools

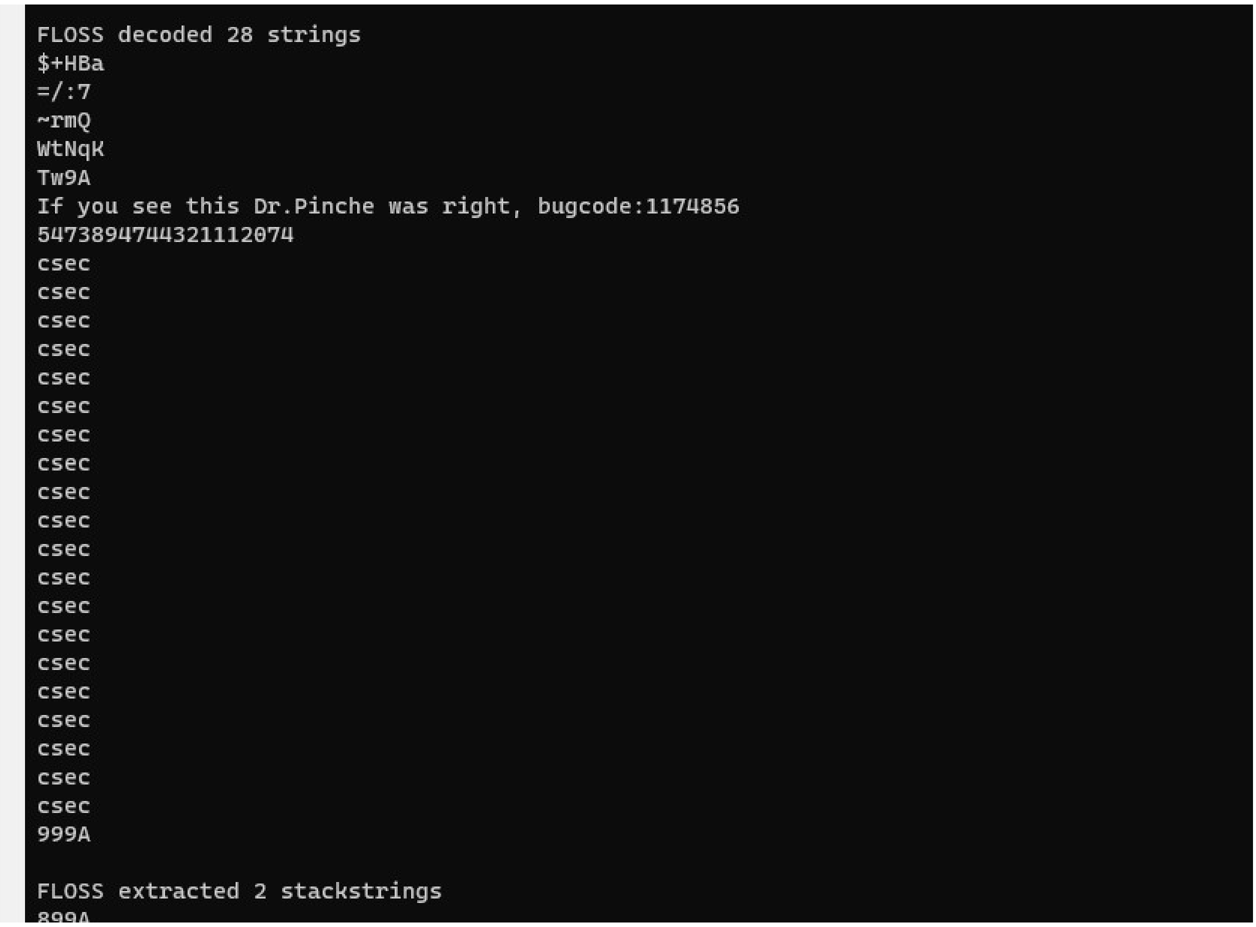


```
WtNqK
Tw9A
If you see this Dr.Pinche was right, bugcode:1174856
5473894744321112074
csec
999A

FLOSS extracted 1 stackstrings
899A

Finished execution after 4.130994 seconds

┌──(root💀kali)-[/home/tools]
└─# ./floss /home/challenges/11_StrangerStrings/sandboxing.exe
```

Figure 1

Windows Method

First of all player must locate the necessary tool inside his own computer, **Floss**. Then, execute to get all strings including encrypted strings:



```
FLOSS decoded 28 strings
$+HBa
=/:7
~rmQ
WtNqK
Tw9A
If you see this Dr.Pinche was right, bugcode:1174856
5473894744321112074
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
csec
999A

FLOSS extracted 2 stackstrings
899A
```

Figure 2

Finally player will able to see a specific message: If you see this Dr.Pinche was right, bugcode: 1174856

Flag Information

flag{1174856}