CZ4067 CTF Pwn Challenges

By: Er Jun Jia

Introduction

These are a series of Pwn (Binary Exploitation) Challenges to practice your binary application exploitation techniques. Inside each challenge subfolder lies a `README.md` file as well as the challenge binary.

Player Setup

This section introduces the *recommended* environment and tools to solve the tutorial challenges.

Environment

- Mandatory: Tutorial challenges can only be completed on **Linux** Machines (**Binary files are Linux Executables**)
- Recommended Operating Systems:
  - `Kali Rolling - Kali Linux (2020.4) x64`
  - `Ubuntu 20.04.3 LTS`
- Recommended VM Manager:
  - `Oracle VM VirtualBox Manager`

  Guides to install Kali/Ubuntu. on VirtualBox can be found online. Some useful guide links are:
  - https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/
  - https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox#1-overview

Useful Tools

- GDB (https://www.gnu.org/software/gdb/)
  - Debug C programs
- Ghidra (https://ghidra-sre.org/)
  - Decompile and disassemble C programs to readable C code
- Python3
  - Pwntools (Python3 package - https://docs.pwntools.com/en/stable/)
    - Used to craft and send payloads to C programs locally or on the server

Executing the Binary

For example, the first challenge, `Don't Forget the Lyrics` has the challenge binary file name `lyrics_static`.

On a Linux Terminal:

1. Ensure you have permissions to run the file. `chmod 777 ./lyrics_static` will suffice
2. Run the file with `./lyrics_static`

Rules

- Depending on the difficulty of the challenge, challenge source code may be provided. Source code will be provided in a file named `{challengeName}_sample.c`.
  - These sample files contain majority of the original program, but exclude the `flag` as well as the function `d()`, which is used to decrypt and deobfuscate the flag stored on the program.
  - `d()` is **not part of the challenge scope**, and it is not necessary to reverse engineer any part of `d()` to obtain the flag
- You may have to use python scripting to solve some challenges. I have included a sample script (not the complete solution) for challenge `Escape Room 1` in the `./escape_room_1` directory titled `escape1_static_win_sample.py`.
- Try your best to complete the challenges yourselves before looking at the hints.
- Hints provided below are ROT-13 Encrypted, and only use them if you are stuck/lost.
- Flags only take the format CZ4067{ ... }

Good Luck and Have Fun!

Challenges

Don't Forget the Lyrics

Difficulty: Warmup

Source Code Provided?: Yes

Description

Rick Astley will never give you up... Can you find a way to not let him down?

Hint 1

Vf fpnas ihyarenoyr gb nal rkcybvgngvba?

Hint 2

Vs gur fbat vf hasnzvyvne, tbbtyr “Arire Tbaan Tvir lbh Hc” ol Evpx Nfgyrl

Hint 3

Jurer naq ubj vf gur ylevp inevnoyr vavgvnyvfrq? Pna lbh erjevgr gur ylevp inevnoyr guebhtu na biresybj?

Echo Chamber 1

Difficulty: Warmup

Source Code Provided?: Yes

Description

This cave seems to echo back whatever you shout into it. Mysteriously, if you shout in a certain *format*, the cave echoes back something else ... Spooky.

Hint 1

Gung cevags hfntr vf ybbxvat fhfcvpvbhf

Hint 2

Vf gur synt cbvagre fgberq ba gur fgnpx jura cevags vf rkrphgrq?

Hint 3

Gur synt cbvagre vf fbzrjurer ba gur fgnpx. Jvgu gur pbeerpg bssfrg, lbh fubhyq or noyr gb cevag bhg gur synt fgevat

---

Echo Chamber 2

Difficulty: Easy

Source Code Provided?: No

Description

The cave seems alot hollower now. I can’t seem to pin-*point* what is missing though. Maybe you can *point* it out for me?

Hint 1

Hayvxr Rpub Punzore 1, gurer vf ab synt cbvagre vavgvnyvfrq ba gur fgnpx sbe lbh. Pna lbh chg vg ba gur fgnpx lbhefrys?

Hint 2

Vs lbh'er univat qvssvphygl svaqvat gur synt cbvagre, V erpbzzraq qvffnfrzoyvat hfvat tqo

Hint 3

Qba'g sbetrg cnqqvat

Echo Chamber 3

Difficulty: Medium

Source Code Provided?: No

Description

Back to the cave again, but this time, the cave wants some PIE.

Hint 1

Eryngvir nqqerffvat naq bssfrgf ner fbzrgvzrf orggre guna nofbyhgr nqqerffrf

Hint 2

Fpevcgvat vf erpbzzraqrq sbe guvf punyyratr. V erpbzzraq gur cjagbbyf yvoenel vs lbh yvxr clguba

---

Escape Room 1

Difficulty: Easy

Source Code Provided?: Yes

Description

You're stuck in an Escape Room with no way out! Or is there?

Hint 1

Vs lbh arrq guvf pyhr, punaprf ner lbh unira'g 'trgf' gur ceboyrz lrg.

Escape Room 2

Difficulty: Medium

Source Code Provided?: No

Description

You're stuck in an Escape Room with no way out again! Seems like the secret code is 'dead' and 'cafe' ... Not sure how we plan on using these codes though.

Hint 1

Svaq gur evtug tnqtrgf gb fgber gur cnenzrgref!

Gotta Catch Them All

Difficulty: Easy

Source Code Provided?: Yes

Description

You've heard of Pikachu, but can you defeat Chikaphu? Just a warning, hitting him with the wrong attacks might heal him.

Hint 1

Jul jvyy lbh or nyybjrq gb urny uvz?

Roulette

Difficulty: Easy

Source Code Provided?: Yes

Description

Come try your luck at this new Roulette Table! Can you guess the correct number 7 times in a row?

Hint 1

Frrqf ner vzcbegnag ... Va tneqravat, naq va ebhyrggr znavchyngvba