PWN College

Session 20

Atousa Ahsani

References: https://pwn.college/, https://guyinatuxedo.github.io/

Bad Seed

H3 Time

H3 Time

- It is a **64-bit dynamically** linked binary, with a **stack canary**, non executable **stack**, and no **PIE**.

```
→  h3_time file time
time: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked,
 interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=
4972fe3e2914c74bc97f0623f0c4643c40300dab, not stripped
→  h3_time checksec time
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

- We can see that it prompts us to guess a number.

```
→  h3_time ./time
Welcome to the number guessing game!
I'm thinking of a number. Can you guess it?
Guess right and you get a flag!
Enter your number: 15935728
Your guess was 15935728.
Looking for 560750746.
Sorry. Try again, wrong guess!
```

H3 Time

- So we can see it generates a **random number** using the ***rand*** function. It then prompts us for input using ***scanf*** with the ***%u*** format string stored in *DAT_00400bbc* (double click on *DAT_00400bbc* in the assembly to see it).
- Then it checks if the two number are the same, and if they are it will run the ***giveFlag*** function which when we look at it, we can see that it reads prints out the flag file from */home/h3/flag.txt* .

```
undefined8 main(void)

{
  time_t tVar1;
  long in_FS_OFFSET;
  uint local_18;
  uint local_14;
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  tVar1 = time((time_t *)0x0);
  srand((uint)tVar1);
  local_14 = rand();
  puts("Welcome to the number guessing game!");
  puts("I\'m thinking of a number. Can you guess it?");
  puts("Guess right and you get a flag!");
  printf("Enter your number: ");
  fflush(stdout);
  __isoc99_scanf(&DAT_00400bbc,&local_18);
  printf("Your guess was %u.\n",(ulong)local_18);
  printf("Looking for %u.\n",(ulong)local_14);
  fflush(stdout);
  if (local_14 == local_18) {
    puts("You won. Guess was right! Here\'s your flag:");
    giveFlag();
  }
  else {
    puts("Sorry. Try again, wrong guess!");
  }
  fflush(stdout);
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return 0;
}
```

H3 Time

- So we need to figure out what the output of the ***rand*** function will be.
- Thing is the **output** of the ***rand*** function is **not** actually **random**. The output is based of a value called a **seed**, which it uses to determine what number sequence to generate.
- So if we can get the **same seed**, we can get rand to generate the same sequence of numbers. Looking at the decompiled code, we see that it uses the **current time** as a **seed**.

```
tVar1 = time((time_t *)0x0);
srand((uint)tVar1);
local_14 = rand();
```

```
void giveFlag(void)

{
  FILE *__stream;
  long in_FS_OFFSET;
  char local_118 [264];
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  memset(local_118,0,0x100);
  __stream = fopen("/home/h3/flag.txt","r");
  if (__stream == (FILE *)0x0) {
    puts("Flag file not found!  Contact an H3 admin for assistance.");
  }
  else {
    fgets(local_118,0x100,__stream);
    fclose(__stream);
    puts(local_118);
  }
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return;
}
```

H3 Time

rand()

- The function ***rand***() is used to generate the **pseudo random number**. It returns an **integer** value and its range is from ***0*** to ***rand_max*** which is granted to be at least 32767.

srand()

- The function ***srand***() is used to **initialize** the generated pseudo random number by ***rand***() function. It does not return anything.

How srand() and rand() are related to each other?

- ***srand***() sets the **seed** which is used by ***rand*** to generate "random" numbers.
- If you don't call ***srand*** before your first call to rand, it's as if you had called ***srand(1)*** to set the seed to one.

H3 Time

- Source code of ***rand*** and ***srand*** in stdlib:

```
void srand(unsigned int seed) {
  holdrand = (long) seed;
}

int rand() {
  return (((holdrand = holdrand * 214013L + 2531011L) >> 16) & 0x7fff);
}
```

H3 Time

- So if we just write a simple **C** program to use the **current time** as a **seed**, and output generated random and **redirect** the output to the target, we will solve the challenge.

```c
#include <stdio.h>
#include <stdlib.h>
#include <stdint.h>
#include <time.h>

int main()
{
    uint32_t rand_num;
    srand(time(0));
    rand_num = rand();
    printf("%d\n", rand_num);
}
```

H3 Time

- Then we just need to compile and run it.
-
```
→  h3_time gcc solve.c
→  h3_time ./a.out | ./time
Welcome to the number guessing game!
I'm thinking of a number. Can you guess it?
Guess right and you get a flag!
Enter your number: Your guess was 1479347496.
Looking for 1479347496.
You won. Guess was right! Here's your flag:
Flag file not found!  Contact an H3 admin for assistance.
```
- We can see that it is solved. It didn't print the flag since the file */home/h3/flag.txt* does not exist, however it prints out an error message seen in the *giveFlag* function so we know that we solved it.