PWN College

Session 21

Atousa Ahsani

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

Bad Seed

HSCTF 2019 Tuxtalkshow

HSCTF'19: Tuxtalkshow

- It is a **64-bit dynamically** linked binary, with a **stack canary**, non executable **stack**, and enabled **PIE**.

```
→  hsctf19_tuxtalkshow file tuxtalkshow
tuxtalkshow: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically
linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=8c0d2b94392e01fecb
4b54999cc8afe6fa99653d, for GNU/Linux 3.2.0, not stripped
→  hsctf19_tuxtalkshow checksec tuxtalkshow
[*] '/home/atousa/PWNCollegeCourse_TMU/21/hsctf19_tuxtalkshow/tuxtalkshow'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
```

- When we run it, it prompts us for a number.

```
→  hsctf19_tuxtalkshow ./tuxtalkshow
Welcome to Tux Talk Show 2019!!!
Enter your lucky number: 1234
```

HSCTF'19: Tuxtalkshow

- So we can see, it starts off by scanning in the contents of ***flag.txt*** to *local_228*.

```
int iVar1;
time_t tVar2;
basic_ostream *this;
long in_FS_OFFSET;
int local_290;
int local_28c;
int local_288;
int local_284;
undefined4 local_280;
undefined4 local_27c;
undefined4 local_278;
undefined4 local_274;
undefined4 local_270;
undefined4 local_26c;
int local_268 [4];
undefined4 local_258;
undefined4 local_254;
basic_string local_248 [32];
basic_istream local_228 [520];
long local_20;

local_20 = *(long *)(in_FS_OFFSET + 0x28);
basic_ifstream((char *)local_228,0x1020b0);
tVar2 = time((time_t *)0x0);
srand((uint)tVar2);
                /* try { // try from 0010127e to 001012c0 has its CatchHandler @ 00101493 */
this = operator<<<std--char_traits<char>>
                ((basic_ostream *)cout,"Welcome to Tux Talk Show 2019!!!");
operator<<((basic_ostream<char,std--char_traits<char>> *)this,endl<char,std--char_traits<char>>);
operator<<<std--char_traits<char>>((basic_ostream *)cout,"Enter your lucky number: ");
operator>>((basic_istream<char,std--char_traits<char>> *)cin,&local_290);
```

```
                    s_flag.txt_001020b0
001020b0 66 6c 61      ds         "flag.txt"
         67 2e 74
         78 74 00
```

HSCTF'19: Tuxtalkshow

- Proceeding that we see that it initializes an ***int*** array with size entries, although the decompilation only shows ***four***. Looking at the assembly code shows us the rest.

```
001012c1  MOV     dword ptr [local_280 + RBP],0x79
001012cb  MOV     dword ptr [local_27c + RBP],0x12c97f
001012d5  MOV     dword ptr [local_278 + RBP],0x135f0f8
001012df  MOV     dword ptr [local_274 + RBP],0x74acbc6
001012e9  MOV     dword ptr [local_270 + RBP],0x56c614e
001012f3  MOV     dword ptr [local_26c + RBP],0xffffffe2
001012fd  MOV     EAX,dword ptr [local_280 + RBP]
00101303  MOV     dword ptr [local_268 + RBP],EAX
00101309  MOV     EAX,dword ptr [local_27c + RBP]
0010130f  MOV     dword ptr [local_264 + RBP],EAX
00101315  MOV     EAX,dword ptr [local_278 + RBP]
0010131b  MOV     dword ptr [local_260 + RBP],EAX
00101321  MOV     EAX,dword ptr [local_274 + RBP]
00101327  MOV     dword ptr [local_25c + RBP],EAX
0010132d  MOV     EAX,dword ptr [local_270 + RBP]
00101333  MOV     dword ptr [local_258 + RBP],EAX
00101339  MOV     EAX,dword ptr [local_26c + RBP]
0010133f  MOV     dword ptr [local_254 + RBP],EAX
```

```
local_280 = 0x79;
local_27c = 0x12c97f;
local_278 = 0x135f0f8;
local_274 = 0x74acbc6;
local_270 = 0x56c614e;
local_26c = 0xffffffe2;
local_268[0] = 0x79;
local_268[1] = 0x12c97f;
local_268[2] = 0x135f0f8;
local_268[3] = 0x74acbc6;
local_258 = 0x56c614e;
local_254 = 0xffffffe2;
local_28c = 0;
while (local_28c < 6) {
  iVar1 = rand();
  local_268[(long)local_28c] = local_268[(long)local_28c] - (iVar1 % 10 + -1);
  local_28c = local_28c + 1;
}
local_288 = 0;
local_284 = 0;
while (local_284 < 6) {
  local_288 = local_288 + local_268[(long)local_284];
  local_284 = local_284 + 1;
}
if (local_288 == local_290) {
  basic_string();
                    /* try { // try from 00101419 to 00101448 has its CatchHandler @ 0010147f */
  operator>><char,std--char_traits<char>,std--allocator<char>>(local_228,local_248);
  this = operator<<<char,std--char_traits<char>,std--allocator<char>>
                     ((basic_ostream *)cout,local_248);
  operator<<((basic_ostream<char,std--char_traits<char>> *)this,endl<char,std--char_traits<char>>)
  ;
  ~basic_string((basic_string<char,std--char_traits<char>,std--allocator<char>> *)local_248);
}
~basic_ifstream((basic_ifstream<char,std--char_traits<char>> *)local_228);
if (local_20 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
  __stack_chk_fail();
}
return 0;
```

HSCTF'19: Tuxtalkshow

- Also we can see that it uses ***time*** as a **seed**. Proceeding that it performs an algorithm where it will generate **random numbers** (using time as a seed) to **edit** the values of array, then accumulate all of those values and that is the number we are supposed to guess.
- Since the rand function is directly based off of the **seed**, and since the seed is the time, we know what values the **rand function** will output.
- Thus we can just write a simple C program that will simply use **time** as a **seed**, and just generate the same number that the target wants us to guess. With that, we can solve the challenge!

HSCTF'19: Tuxtalkshow

```c
int main()
{
    int array[6];
    int i, output;
    uint32_t randVal, ans;
    srand(time(0));

    array[0] = 0x79;
    array[1] = 0x12c97f;
    array[2] = 0x135f0f8;
    array[3] = 0x74acbc6;
    array[4] = 0x56c614e;
    array[5] = 0xffffffe2;
    i = 0;
    while (i < 6){
        randVal = rand();
        array[i] = array[i] - ((randVal % 10) - 1);
        i += 1;
    }
    i = 0;
    output = 0;
    while (i < 6){
        output = output + array[i];
        i += 1;
    }
    printf("%d\n", output);
}
```

HSCTF'19: Tuxtalkshow

- We just need to compile and run the exploit code, and redirect the result to the target.

```
→  hsctf19_tuxtalkshow cc solve.c -o solve
→  hsctf19_tuxtalkshow ./solve
234874826
→  hsctf19_tuxtalkshow ./solve | ./tuxtalkshow
Welcome to Tux Talk Show 2019!!!
Enter your lucky number: flag{i_need_to_think_of_better_flags}
```