HackNight

Reverse Engineering

2/16/2023

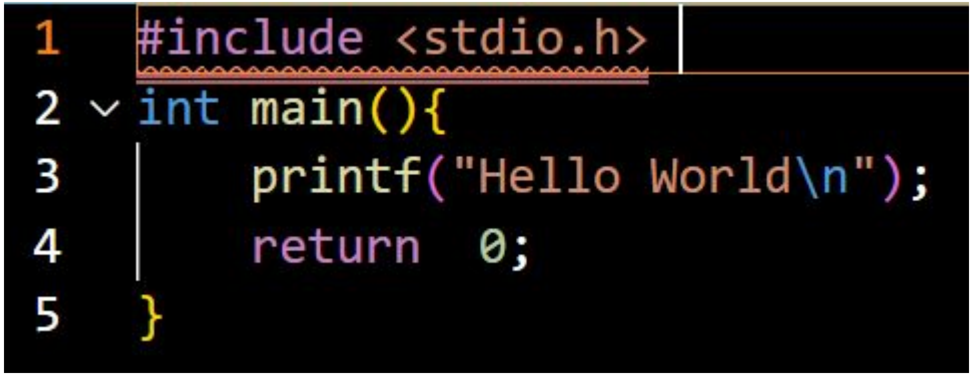
OSIRIS

What is Reverse Engineering

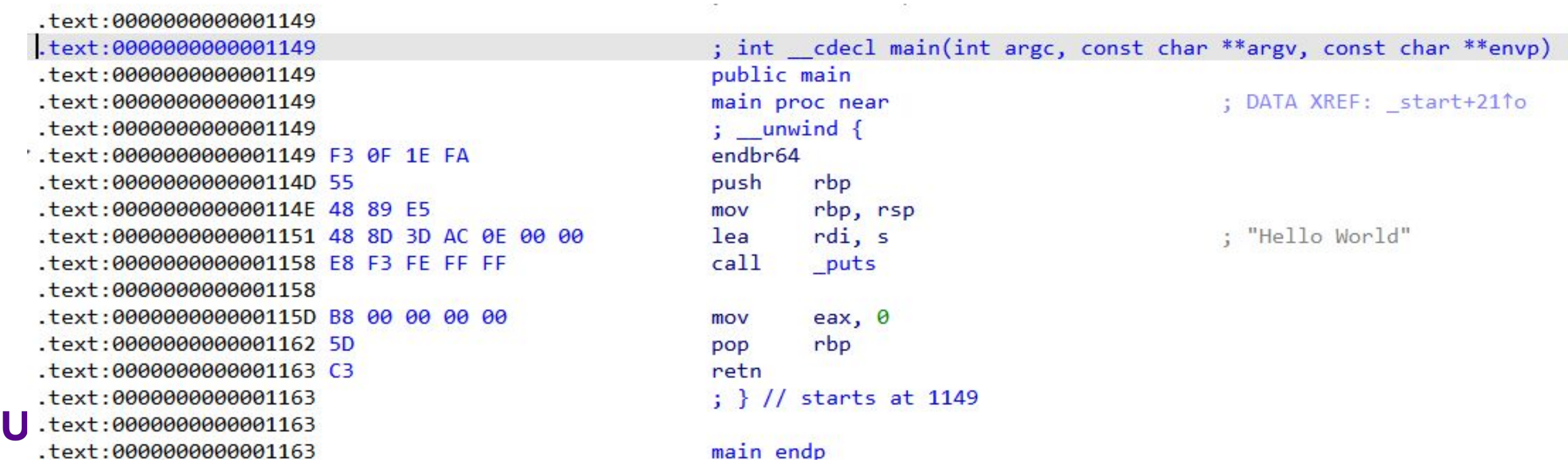
- A process or method in which one deduces:
- How a product is made
- What is the purpose of the product
- Why it is made

Reverse Engineering Computer Softwares

- Software is made from source code
- Source codes are in (hopefully) simple English or an understandable language
- Softwares are…



```c
#include <stdio.h>
int main(){
    printf("Hello World\n");
    return  0;
}
```



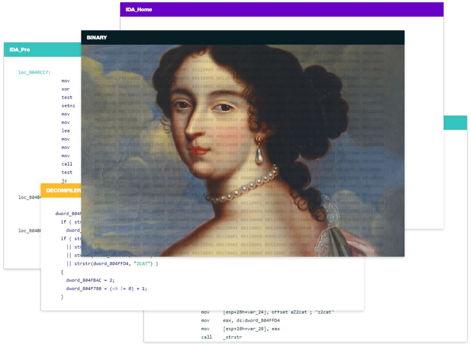
```
.text:0000000000001149
.text:0000000000001149                                  ; int __cdecl main(int argc, const char **argv, const char **envp)
.text:0000000000001149                                  public main
.text:0000000000001149                                  main proc near                          ; DATA XREF: _start+21↑o
.text:0000000000001149                                  ; __unwind {
.text:0000000000001149 F3 0F 1E FA                      endbr64
.text:000000000000114D 55                               push    rbp
.text:000000000000114E 48 89 E5                         mov     rbp, rsp
.text:0000000000001151 48 8D 3D AC 0E 00 00             lea     rdi, s                          ; "Hello World"
.text:0000000000001158 E8 F3 FE FF FF                   call    _puts
.text:0000000000001158
.text:000000000000115D B8 00 00 00 00                   mov     eax, 0
.text:0000000000001162 5D                               pop     rbp
.text:0000000000001163 C3                               retn
.text:0000000000001163                                  ; } // starts at 1149
.text:0000000000001163
.text:0000000000001163                                  main endp
```

How do we make it simpler?

With These Tools

Binary Ninja

A.K.A. Binja, free trial available, commercial license pricey but very powerful. Disassembly contains all of low, Medium, and High level IL



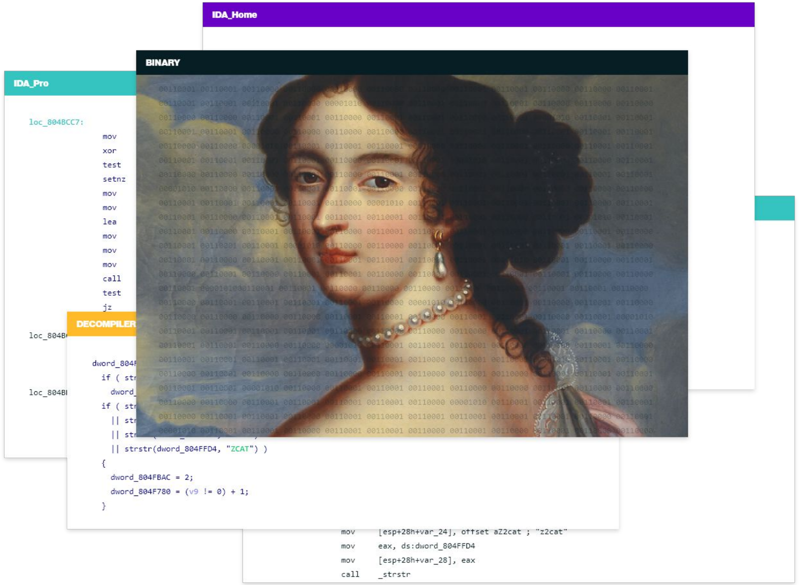
IDA

Charges an immense amount of money for a license, commonly cracked. OG disassembler with a wide variety of plugins

Ghidra

Completely free disassembler made by NSA, plugins are continuously being made by the community. (Though it runs on JVM)

https://cloud.binary.ninja/



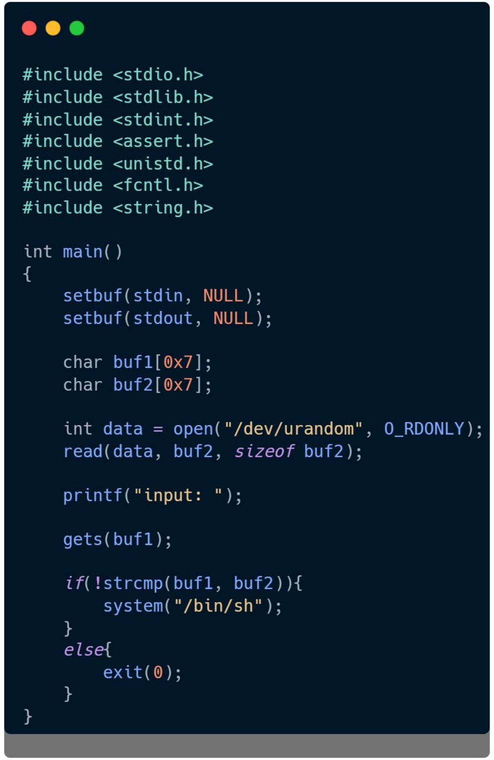
```
loc_804BCC7:
            mov
            xor
            test
            setnz
            mov
            mov
            lea
            mov
            mov
            mov
            call
            test
            jz

loc_804B

loc_804B
```

```
dword_804F
  if ( str
    dword_
  if ( str
    || str
    || str
    || strstr(dword_804FFD4, "ZCAT") )
  {
    dword_804FBAC = 2;
    dword_804F780 = (v9 != 0) + 1;
  }
```

```
mov     [esp+28h+var_24], offset aZ2cat ; "z2cat"
mov     eax, ds:dword_804FFD4
mov     [esp+28h+var_28], eax
call    _strstr
```

https://hex-rays.com/ida-pro/

https://ghidra-sre.org/



```c
#include <stdio.h>
#include <stdlib.h>
#include <stdint.h>
#include <assert.h>
#include <unistd.h>
#include <fcntl.h>
#include <string.h>

int main()
{
    setbuf(stdin, NULL);
    setbuf(stdout, NULL);

    char buf1[0x7];
    char buf2[0x7];

    int data = open("/dev/urandom", O_RDONLY);
    read(data, buf2, sizeof buf2);

    printf("input: ");

    gets(buf1);

    if(!strcmp(buf1, buf2)){
        system("/bin/sh");
    }
    else{
        exit(0);
    }
}
```

Find The Vul

Smash Your Brain

What's the payload

Smash Your Brain

What's the length of shortest payload?

Smash Your Brain

What’s the shortest payload

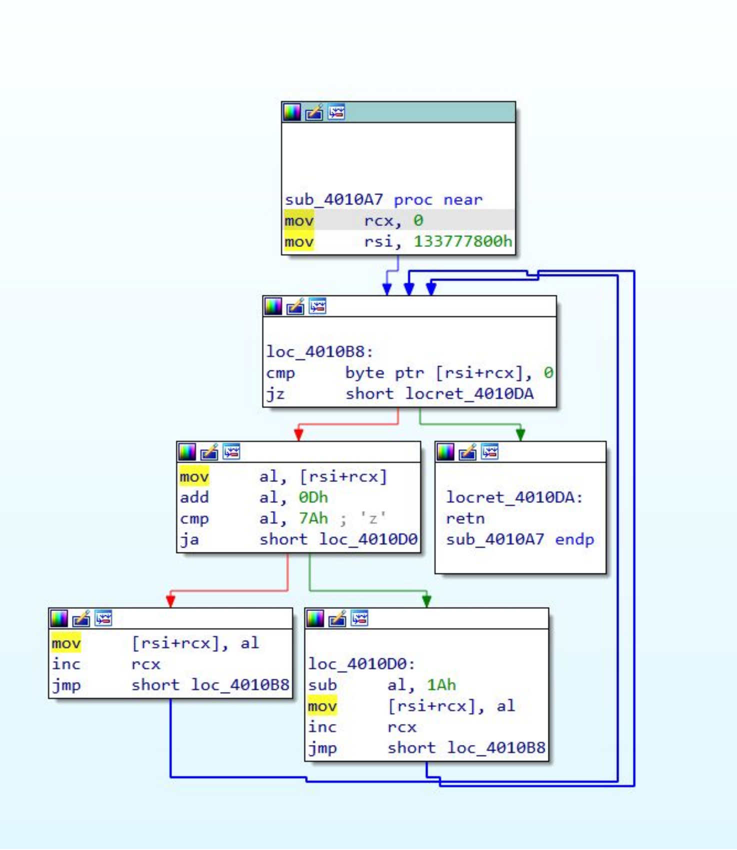
Smash Your Brain

What's the shortest but not stable payload

Asm
Code
Rev

Would you like to read the source code or binary?

Practice challenge - tor
https://drive.google.com/file/d/17XLgWqx3f0d_JLLYhRLiIRCGaY2oHlt4/view?usp=sharing



```
sub_4010A7 proc near
mov     rcx, 0
mov     rsi, 133777800h

loc_4010B8:
cmp     byte ptr [rsi+rcx], 0
jz      short locret_4010DA

mov     al, [rsi+rcx]
add     al, 0Dh
cmp     al, 7Ah ; 'z'
ja      short loc_4010D0

locret_4010DA:
retn
sub_4010A7 endp

mov     [rsi+rcx], al
inc     rcx
jmp     short loc_4010B8

loc_4010D0:
sub     al, 1Ah
mov     [rsi+rcx], al
inc     rcx
jmp     short loc_4010B8
```

NYU

Q&A

What can we do with Reversing & Pwning?

- Pwn your homework programs
- Hack the Routers
- Hack the Vehicles (https://keenlab.tencent.com/en/)
- Hack the Satellite (https://hackasat.com/)