Introdução à engenharia reversa de códigos maliciosos

Marcus Botacin[1]

[1]Depto. de Informática - UFPR
mfbotacin@inf.ufpr.br

Outubro de 2017

Tópicos

Tópicos

Material do curso

Disponível no Github

- git clone `https://github.com/marcusbotacin/Malware.Reverse.Intro.git`

Arquivos Suspeitos

Quais são os arquivos de interesse ?

- Diretório Files/Suspicious.Files/

Arquivos Suspeitos

O comando file

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Suspicious.Files$ file 0 10 1
0:  PNG image data, 300 x 168, 8-bit colormap, non-interlaced
10: PDF document, version 1.5
1:  ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, inter
ldID[sha1]=9321ea5eeeaa6628e8ac634972fa0cc0f3b88402, not stripped
```

- **ELF:** formato executável.
- **64-bit:** tamanho da palavra.
- **LSB:** endianess.
- **x86-64:** Arquitetura.
- **SYSV:** System V ABI.
- **dynamically linked:** tipo de ligação com bibliotecas.
- **not stripped:** `gcc -g`

Quebrando senha I

Qual a senha do arquivo ?

- Diretório Files/Password/

Quebrando senha I

Hexdump -C

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Password$ hexdump -C pass
00000000  7f 45 4c 46 02 01 01 00  00 00 00 00 00 00 00 00  |.ELF............|
00000010  02 00 3e 00 01 00 00 00  50 05 40 00 00 00 00 00  |..>.....P.@.....|
00000020  40 00 00 00 00 00 00 00  88 1a 00 00 00 00 00 00  |@...............|
00000230  01 00 00 00 00 00 00 00  2f 6c 69 62 36 34 2f 6c  |......../lib64/l|
00000240  64 2d 6c 69 6e 75 78 2d  78 38 36 2d 36 34 2e 73  |d-linux-x86-64.s|
00000250  6f 2e 32 00 04 00 00 00  10 00 00 00 01 00 00 00  |o.2.............|
00000060  f8 01 00 00 00 00 00 00  f8 01 00 00 00 00 00 00  |................|
```

Quebrando senha I

Strings

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Password$ strings -n 8 pass
/lib64/ld-linux-x86-64.so.2
libc.so.6
__isoc99_scanf
__stack_chk_fail
__libc_start_main
__gmon_start__
GLIBC_2.7
GLIBC_2.4
GLIBC_2.2.5
[]A\A]A^A_
Password:
this is the password
You've got it
Nooooope
```

WEB

Quais IPs e URLs são referidos ?

- Diretório Files/Network

WEB

Strings + Python regex

```
IP_regex = r'[0-9]+(?:\.[0-9]+){3}'
mail_regex = r"([^@|\s]+@[^@]+\.[^@|\s]+)"
```

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Network$ strings net | python net.py
['ld-linux-x86-64.so']
['libc.so']
['192.168.0.1']
['https://localhost:80']
me@me.com
```

ASM

Quais funções foram compiladas ?

- Diretório Files/inspect.me/

ASM

Objdump

```
objdump -d inspect.me

0000000000400566 <f1>:
  400566:   55                      push   %rbp
  400567:   48 89 e5                mov    %rsp,%rbp
  40056a:   89 7d fc                mov    %edi,-0x4(%rbp)
  40056d:   89 75 f8                mov    %esi,-0x8(%rbp)
  400570:   8b 55 fc                mov    -0x4(%rbp),%edx
  400573:   8b 45 f8                mov    -0x8(%rbp),%eax
  400576:   01 d0                   add    %edx,%eax
  400578:   5d                      pop    %rbp
  400579:   c3                      retq

000000000040057a <f2>:
  40057a:   55                      push   %rbp
  40057b:   48 89 e5                mov    %rsp,%rbp
  40057e:   89 7d fc                mov    %edi,-0x4(%rbp)
  400581:   89 75 f8                mov    %esi,-0x8(%rbp)
  400584:   8b 45 fc                mov    -0x4(%rbp),%eax
  400587:   2b 45 f8                sub    -0x8(%rbp),%eax
  40058a:   5d                      pop    %rbp
  40058b:   c3                      retq

000000000040058c <main>:
  40058c:   55                      push   %rbp
  40058d:   48 89 e5                mov    %rsp,%rbp
  400590:   bf 34 06 40 00          mov    $0x400634,%edi
  400595:   e8 96 fe ff ff          callq  400430 <puts@plt>
```

Libs

Quais funções foram ligadas I ?

- Diretório Files/Calls.1/

Libs

Objdump -T

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Calls.1$ objdump -T calls

calls: formato do arquivo elf64-x86-64

DYNAMIC SYMBOL TABLE:
0000000000000000      DF *UND*  0000000000000000  GLIBC_2.2.5 puts
0000000000000000      DF *UND*  0000000000000000  GLIBC_2.2.5 __libc_start_main
0000000000000000  w   D  *UND*  0000000000000000              __gmon_start__
0000000000000000      DF *UND*  0000000000000000  GLIBC_2.2.5 fork
```

Libs

Quais funções foram ligadas II ?

- Diretório Files/Calls.2/

Packing (UPX)

Diretório Files/Pack/

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Pack$ make 1
gcc hello.c -o hello
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Pack$ make check
upx -l hello
upx: hello: NotPackedException: not packed by UPX
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Pack$ make 2
gcc hello.c -static -o hello
upx -1 hello
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Pack$ make check
upx -l hello
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2013
UPX 3.91        Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 2013

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    912704 ->    401564   44.00%  linux/ElfAMD   hello
```

Libs

De volta a Files/Calls.2/

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Calls.2$ strace ./calls
execve("./calls", ["./calls"], [/* 66 vars */]) = 0
mmap(0x800000, 2995983, PROT_READ|PROT_WRITE|PROT_EXEC, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, 0, 0) = 0x800000
readlink("/proc/self/exe", "/home/marcus/Documentos/Malware."..., 4096) = 65
brk(0x24961c0)                          = 0x24961c0
clone(child_stack=0, flags=CLONE_CHILD_CLEARTID|CLONE_CHILD_SETTID|SIGCHLD, child_tidptr=0x2495b50) = 1311
fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 11), ...}) = 0
World
write(1, "Hello\n", 6Hello
```

Traços dinâmicos

Quais funções são chamadas ?

- Diretório Files/trace.me/

Traços dinâmicos

Evasão de ptrace

```
if(ptrace(PTRACE_TRACEME)==-1)
{
    exit(0);
}
```

Traços dinâmicos

Mais traços de funções

- Diretório Files/Calls.3/

Traços dinâmicos

ltrace

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Calls.3$ ltrace ./mylibs
__libc_start_main(0x400526, 1, 0x7fffea012398, 0x400550 <unfinished ...>
puts("malware"malware
)                                                                    = 8
```

Traços dinâmicos

Mais traços de funções

- Diretório Files/Calls.4/

Traços dinâmicos

Ligação estática x dinâmica

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Calls.4$ ltrace ./mylibs
Couldn't find .dynsym or .dynstr in "/proc/2302/exe"
malware
```

Debugging

GDB

- Breakpoint
- Info registers
- Next, Step, Stepi
- display/i $pc
- disassemble foo()

Debugging

O que há escondido no arquivo ?

- Diretório Files/Hidden/

Debugging

Chamando funções

```
marcus@tux:~/Documentos/Malware.Reverse.Intro/Files/Hidden$ gdb -q hidden
Lendo símbolos de hidden...(no debugging symbols found)...concluído.
(gdb) b main
Ponto de parada 1 at 0x40053b
(gdb) run
Starting program: /home/marcus/Documentos/Malware.Reverse.Intro/Files/Hidden/hidden

Breakpoint 1, 0x000000000040053b in main ()
(gdb) call malicious()
I'm a malware
$1 = 14
```

Quebrando senha II

Qual a senha do arquivo ?

- Diretório Files/crack.me/

Binary patching

HT Editor

```
400692 !    call        wrapper_601030_400520
400697 !    test        eax, eax
400699 !    jnz         loc_4006a5
40069b !    mov         edi, strz_Oh_Yeah__40075a
4006a0 !    call        wrapper_601018_4004f0
4006a5 !
```

```
400692 !    call        wrapper_601030_400520
400697 !    test        eax, eax
400699 !    nop
40069a !    nop
40069b !    mov         edi, strz_Oh_Yeah__40075a
4006a0 !    call        wrapper_601018_4004f0
```

Desafios

O que fazem os binários ?

- Diretório Files/Challenges