Zad. 5

niedziela, 14 maja 2023 12:36

Zadanie 5. Zmodyfikuj opcje kompilacji programu «ropex» w pliku «Makefile». Najpierw zleć kompilatorowi dodanie **kanarków** (ang. *canary*) włączając opcję «-fstack-protector». Pokaż, że program wykrywa **uszkodzenie stosu** (ang. *stack smashing*). Posługując się debuggerem gdb zaprezentuj, że przy każdym uruchomieniu programu wartość kanarka jest inna. Następnie usuń opcję wymuszającą *statyczną konsolidację* «-static» i dodaj opcję «-fpie», aby umożliwić **randomizację rozkładu przestrzeni adresowej** (ang. *Address Space Layout Randomization*). Pokaż, że adres *gadżetu* o nazwie «gadget» jest inny przy każdym uruchomieniu programu. Następnie dodaj opcję kompilacji «-z noexecstack», która zapisuje w pliku ELF informacje o tym, że procesor nie powinien próbować wykonywać zawartości stosu. Przy pomocy programu «pmap» zweryfikuj, że istotnie stos uruchomionego programu «ropex» nie jest wykonywalny.

Czemu każde z zastosowanych wyżej zabezpieczeń utrudnia zadanie atakującemu?

Uwaga! Debugger gdb może wyłączyć ASLR przeprowadzaną przez konsolidator dynamiczny, aby ułatwić sobie pracę.

```
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ gcc -o ropex2 -fstac
k-protector ropex.c gadget.o
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ ls
data.c  even.s    lazy      odd.o   ropex.c      ropex.o    start.map
data.s  gadget.o  lazy.c    odd.s   ropex.in     start      start.o
even.c  gadget.s  Makefile  ropex   ropex.in.txt  start.c    start.s
even.o  input.in  odd.c     ropex2  ropex.map    start.lds
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ ./ropex2 input.in
gadget at 0x557fac60c2a6
{@
*** stack smashing detected ***: terminated
Aborted (core dumped)
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$
```

wykrywa

```
code:x86:64
   0x5555555551d7 <echo+36>        mov    %rbx, %rdi
   0x5555555551da <echo+39>        call   0x555555555030 <puts@plt>
   0x5555555551df <echo+44>        mov    0x38(%rsp), %rax
→  0x5555555551e4 <echo+49>        sub    %fs:0x28, %rax
   0x5555555551ed <echo+58>        jne    0x5555555551f5 <echo+66>
   0x5555555551ef <echo+60>        add    $0x40, %rsp
   0x5555555551f3 <echo+64>        pop    %rbx
   0x5555555551f4 <echo+65>        ret
   0x5555555551f5 <echo+66>        call   0x555555555040 <__stack_chk_fail@plt>
```

inne kanarki, bo inna różnica

```
$rax   : 0x28a4de3ddfd7c57b
```

vs

```
$rax   : 0xd7805b9a446d357b
```

inne

```
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ ./ropex
gadget at 0x55a75364a258
q
q
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ ./ropex
gadget at 0x556ab099e258
a
a
```

z flagą

z flagą

```
00007ffdd6c07000    132K rw---   [ stack ]
```

vs

```
00007ffdfeaaa000    132K rwx--   [ stack ]
```

bez

./ropex & + pmap [PID] ↗