0x0000

a great fool in my life i have been
have squandered till pallid and thin
hung my head in shame
and refused to take blame
for the darkness i know i've let win

j knapp

VulnCatcher:
Fun with Programmatic Debugging

atlas

atlas@r4780y.com

http://atlas.r4780y.com

0x0100 What is it?

- Debugging other processes from your (my) favorite language
- Accessing and Influencing CPU and Memory state of a process in a programmatic fashion
  - Logic and other language contructs

0x0101 What can we do?

- Live Patching? Fun with Hex
  - LivePatch
- Live Dumping?
  - LiveOrganTransplant
- Process Grep?
  - Visi's memgrep
- Vampyre Jack SSHD
  - In progress by drb and myself

0x0102 What can we do?

- everything else that GDB or Olly can do, only better
- interactive python debugger
  - especially nice with *searchMemory()* and *traceme()*

0x0200 Vulnerabilities

- what can we do to encourage vulns to suddenly appear?
  - fuzzing on its own is so ghetto!
- rather, what can we watch/do to catch indications of vulnerability?

0x0300 Buffer Overflows?

- custom Breakpoints at key functions
- at break:
  - Stack-Analysis for Parameters
  - Buffer-Analysis for Size

0x0301 vtrace attach

```
from vtrace import *
me = getTrace()
me.attach(<pid>)
me.addBreakpoint(MemcpyBreaker(me))
me.setMode("RunForever", True)
me.run()
```

0x0302 memcpy()

- memccpy()/mempcpy()/memmove()
  - check length of dest (%ESP + 0x4)
    - HEAP (malloc), check length field immediately before the pointer to the dest
      - heapptr - 4
    - Stack, check distance to RET
      - (%ebp + 4) – dest
  - compare with Copy Size (%ESP + 0xc)

0x0303 MemcpyBreaker

```
class MemcpyBreaker(BreakpointPublisher):
  def __init__(self):
    ...
  def notify(self, event, trace):
    eip=trace.getProgramCounter()
    esp=trace.getRegisterByName('esp')
    ebp=trace.getRegisterByName('ebp')
    copylen=trace.readMemoryFormat((esp + 0xc),AddrFmt)[0]
    retptr =trace.readMemoryFormat((esp + 0x0),AddrFmt)[0]
    dest   =trace.readMemoryFormat((esp + 0x4),AddrFmt)[0]
    src    =trace.readMemoryFormat((esp + 0x8),AddrFmt)[0]
    destlen = 0
    if (copylen >= destlen):
       self.publish(BOFException(...))
```

0x0400 EBP-FREE SUBS?

- some subs don't start new stack frames using %ebp
  - Windows Libraries
- trouble measuring stack buffer length

0x0401 EBP-FREE SUBS?

- some disassembly required...
- possible solutions:
  - Initial ESP Offset for Stack Allocation
  - Stack Backtrace for RET
  - Sub Epilog Analysis
    - ret $0x34
    - add $0x34, %esp
  - Sub Tracing for %esp Mods
    - 'til ret do us part
    - or jmp

0x0500 strcpy()/strncpy()

- strcpy – compare length of source and destination
  - dest (%ESP + 0x4)
  - source (%ESP + 0x8)

0x0501 strcpy()/strncpy()

- strncpy – compare length of copy (size_t) to destination
  - dest (%ESP + 0x4)
  - size_t (%ESP + 0xc)

0x0502 strcat()/strncat()

- similar to strcpy/strncpy
- copies source and destination together
- difficult for coders to get right! (ie. often exploitable)
- best to look into logic surrounding strcat() limiting the size of both buffers

0x0600 printf()

- vfprinf covers printf and fprintf in Linux
- what's on the stack for format string?
  - %ESP + 0x8
- does it live in a likely spot?
  - Heap? Stack? .rodata?
- parse format string
  - are there “%” characters in it?

0x0601 sprintf()

- vsprintf covers sprintf in Linux
- what's on the stack for format string?
  - %ESP + 0x8
- does it live in a likely spot?
  - Heap? Stack? .rodata?
- parse format string
  - are there “%” characters in it?
  - how long of a string can we create?

0x0602 snprintf()

- vsnprintf covers snprintf in Linux
- what's on the stack for format string?
  - %ESP + 0x8
- does it live in a likely spot?
  - Heap? Stack? .rodata?
- parse format string
  - are there “%” characters in it?
  - how long will the format string allow?
  - how long **can** we write? (%ESP + 0xc)

0x0700 scanf/sscanf/fscanf

- parse format string
- are there any “%s”?
- if so, where are we storing them?
  - must check each string
    - %45s against a buffer with 32 bytes

0x0800 gets()/fgets()

- lol.
- Just alert. Period.

0x0801 getc()/fgetc()

- loop for getc
- how big is the loop?
- simpler just to identify in disassembly and write up... analysis for which loop mechanism is used is more complex than just eye-balling it.

0x0900 memchr()/memrchr()

- check size_t against length of string as in memcpy
- may be used to look past a buffer as a potential target or source of data

0x0a00 rep stos/rep movs

- special case.
- need to disassemble code to hook these.
  - Set breakpoint one instruction before
  - stepi() to reach start of opcode
  - Check %ECX against buffer length

0x0b00 Format Strings

- used with printf/scanf families
- %c = 1 byte
- %* = * bytes (depends on the size)
- %#d = at **least** # bytes, possibly more!
- See man page for scanf or printf for more

0x0c00 Are there more?

- you tell me!
- programmatic debugging fresh turf for new ideas.
- “The force runs strong in your family... Pass on what you have learned...”

0x0d00 choops

- hola y gracias amigos
  - Dios
  - jewel
  - bug
  - ringwraith
  - menace
  - 1@stplace
  - invisigoth and K