Ghidra + GDB + Pwntools

Nathan

M E E T I N G F L A G

sigpwny{plz_no_nsa_backdoor}

G H I D R A

Get started:

- View all functions in list on left side of screen. Double click main to decompile main

Decompiler:

- Middle click a variable to highlight all instances in decompilation
- Type “L” to rename variable
- “Ctrl+L” to retype a variable
- Type “;” to add an inline comment on the decompilation and assembly
- Alt+Left Arrow to navigate back to previous function

General:

- Double click an XREF to navigate there
- Search -> For Strings -> Search to find all strings (and XREFs)
- Choose Window -> Function Graph for a graph view of disassembly

G D B

- “b main” - Set a breakpoint on the main function
  - “b *main+10” - Set a breakpoint a couple instructions into main
- “r” - run
  - “r arg1 arg2” - Run program with arg1 and arg2 as command line arguments. Same as ./prog arg1 arg2
  - “r < myfile.txt” - Run program and supply contents of myfile.txt to stdin
- “c” - continue
- “si” - step instruction (steps into function calls)
- “ni” - next instruction (steps over function calls)
- “x /32xb 0x5555555551b8” - Display 32 hex bytes at address 0x5555555551b8
  - “x /4xg addr” - Display 4 hex “giants” (8 byte numbers) at addr
  - “x /16i $pc” - Display next 16 instructions at $rip
  - “x /s addr” - Display a string at address
- “info registers” - Display registers
- “info file” or “info proc map” - Display memory mappings

PWNTOOLS

```
from pwn import *

#Testing locally
p = process("./a.out")

#Ready to try on remote server
p = remote("chal.sigpwny.com", 5001)
```

```
#Send input followed by a newline
p.sendline(...)
p.send(...)

#Read some data
result = p.recv()
#Better yet
result = p.recvuntil(...)

#Let human interact
p.interactive()
```

P R A C T I C E

- Ghidra:
  - rot13 (easy)
  - irreversible (intermediate, new)
  - Ouroboros (hard)
  - signals (hard)
  - angry (well, technically. You'll want to use angr for this.)

- GDB + Ghidra:
  - debugging (easy, new)
  - Heap chals
  - GOT chals
  - Basically all pwn chals

- Pwntools:
  - Math god (easy)
  - Hash God (intermediate)
  - Prime God (intermediate)
  - All pwn chals (heap, got, stack)