Hi

whoami

- Srimanta Barua
- Computer Science student from India
- Interested in systems programming, reverse engineering... figuring out how things work

GSoC ‘17

- Original proposal: gdbserver
- Ended up focusing on gdb client
  - Symbol loading, monitor commands, thread-switching, and other features added
  - A lot of time spent fixing bugs
- Mentors - pancake and xvilka
  - Would also thank Maijin, Nighterman, oddcoder, vifino, among others

r2’s internal gdbserver

```
$ r2 -
[0x00000000]> # Check remote commands
[0x00000000]> =?
...
|
gdbserver:
| =g port file [args]   listen on 'port' debugging 'file' using gdbserver
| =g! port file [args]  same as above, but debug protocol messages (like gdbserver --remote-debug)
...
[0x00000000]> # Start gdbserver listening on port 8000, debugging r2 itself
[0x00000000]> =g 8000 /bin/radare2 -
```

- Obviously it's untested and probably quite buggy

r2 remote gdb 101

- Connect on starting r2

```
$ r2 -d gdb://localhost:8000
```

- Most options work normally, like -a for arch, -e for config etc.
- Debug normally

```
[0x7f286c8d6cc0]> ds
[0x7f286c8d6cc0]> pd 2
            0x7f286c8d6cc0      4889e7          mov rdi, rsp
            ;-- rip:
            0x7f286c8d6cc3      e8380c0000      call 0x7f286c8d7900
[0x7f286c8d6cc0]>
```

What’s new?

- Monitor commands

```
[0x7f286c8d6cc0]> =!?
...
=!monitor cmd     - hex-encode monitor command and pass to target interpreter
...
[0x7f286c8d6cc0]> =!monitor help
The following monitor commands are supported:
  set debug <0|1>
    Enable general debugging messages
  set debug-hw-points <0|1>
    Enable h/w breakpoint/watchpoint debugging messages
  set remote-debug <0|1>
    Enable remote protocol debugging messages
  set debug-format option1[,option2,...]
    Add additional information to debugging messages
    Options: all, none, timestamp
  exit
    Quit GDBserver
```

What’s new?

- Limited packet size, subject to user override

```
[0x7f286c8d6cc0]> =!?
...
 =!pktsz            - get max packet size used
 =!pktsz bytes      - set max. packet size as 'bytes' bytes
[0x7f286c8d6cc0]> =!pktsz
packet size: 2048 bytes
[0x7f286c8d6cc0]> =!pktsz 512
[0x7f286c8d6cc0]> =!pktsz
packet size: 512 bytes
```

```
$ R2_GDB_PKTSZ=512 r2 -d gdb://localhost:8000
...
[0x7ff518804cc0]> =!pktsz
packet size: 512 bytes
```

What’s new?

- Get threads with dpt and set active thread with dpt=<thread>
- Parse XML target description
- Get process memory maps

```
[0x7f286c8d6cc0]> dm=
map 140K * x00007ffff7dd9000 |-----------------| 0x00007ffff7dfc000 -r-x /usr/lib/ld-2.25.so
map 12K - 0x00007ffff7ff7000 |-----------------| 0x00007ffff7ffa000 -r-- [vvar]
map 8K - 0x00007ffff7ffa000 |-----------------| 0x00007ffff7ffc000 -r-x [vdso]
map 8K - 0x00007ffff7ffc000 |-----------------| 0x00007ffff7ffe000 -rw- /usr/lib/ld-2.25.so
map 4K - 0x00007ffff7ffe000 |-----------------| 0x00007ffff7fff000 -rw- unk0
map 4K - 0xffffffffff600000 |-----------------| 0xffffffffff601000 -r-x [vsyscall]
map 132K - 0x00007ffffffde000 |-----------------| 0x00007fffffffff000 -rw- [stack]
map 36K - 0x0000555555554000 |#----------------| 0x000055555555d000 -r-x /home/barua/Documents/rad
map 8K - 0x000055555575c000 |-------------#--| 0x000055555575e000 -rw- /home/barua/Documents/rada
map 388K - 0x000055555575e000 |-------------###| 0x00005555557bf000 -rw- [heap]
```

What’s new?

- Speed improvement with no-ack mode and register caching
- Kill/detach from target
- Automatic symbol loading

```
$ r2 -d gdb://localhost:8000
...
[0x7ffff7dd8f30]> is | head
[Symbols]
vaddr=0x555555556f20 paddr=0x00002f20 ord=035 fwd=NONE sz=0 bind=LOCAL type=FUNC name=deregister_t
vaddr=0x555555556f60 paddr=0x00002f60 ord=036 fwd=NONE sz=0 bind=LOCAL type=FUNC name=register_tm_
vaddr=0x555555556fb0 paddr=0x00002fb0 ord=037 fwd=NONE sz=0 bind=LOCAL type=FUNC name=__do_global_
vaddr=0x55555575d4e0 paddr=0x000094e0 ord=038 fwd=NONE sz=1 bind=LOCAL type=OBJECT name=completed.
vaddr=0x55555575cc80 paddr=0x00008c80 ord=039 fwd=NONE sz=0 bind=LOCAL type=OBJECT name=__do_globa
vaddr=0x555555556ff0 paddr=0x00002ff0 ord=040 fwd=NONE sz=0 bind=LOCAL type=FUNC name=frame_dummy
vaddr=0x55555575cc78 paddr=0x00008c78 ord=041 fwd=NONE sz=0 bind=LOCAL type=OBJECT name=__frame_du
vaddr=0x555555556ffa paddr=0x00002ffa ord=043 fwd=NONE sz=99 bind=LOCAL type=FUNC name=blob_versio
vaddr=0x55555575d500 paddr=0x00009500 ord=044 fwd=NONE sz=8 bind=LOCAL type=OBJECT name=rabin_cmd
```

Thank you