درس ۱۱

ASM

GDB با debug

hello.asm

```
(gdb) break _start
(gdb) stepi
(gdb) info registers
```

یک کورس رایگان از MyWebUniversity

زبان Assembly

درس ۱۱

debug با GDB و objdump



breakpoint ها، قدم زدن، بررسی register ها و حافظه، disassembly و خواندن فایل‌های باینری

شروع GDB

با -g، assemble کنید تا اطلاعات debug شامل شود. GDB را با پروگرام خود شروع کنید، با break ...

layout asm و layout regs دستورها و register ها را در پنجره‌های جدا نشان می‌دهند.



01

قدم زدن در کود

stepi یک دستور را اجرا می‌کند. nexti هم یکی را اجرا می‌کند، اما از روی call ها رد می‌شود. ...

تغییر register ها را بعد از هر قدم ببینید. این بهترین راه یادگیری کار واقعی دستورها است.

ASSEMBLY LANGUAGE · 11

فرمان GDB	کار
`break label`	توقف در یک label
`stepi · si`	یک دستور
`nexti · ni`	رد شدن از call
`continue · c`	اجرا تا break بعدی
`info registers`	نشان دادن همهٔ register ها

02

بررسی register ها و حافظه

print/x $rax یک register را به hex نشان می‌دهد. فرمان x حافظه را بررسی می‌کند: x/4dw چهار ...

x/s یک رشته را نشان می‌دهد، و x/8xg $rsp بالای stack را نشان می‌دهد.



03

objdump: disassembly

objdump -d یک فایل باینری را disassemble می‌کند: آدرس هر دستور، بایت‌های کود ماشین آن و ...

-M intel را برای نحو Intel که در این کورس استفاده می‌کنیم اضافه کنید، به جای نحو پیش‌فرض AT&T.

ASSEMBLY LANGUAGE · 11

terminal

```
$ objdump -d -M intel hello
0000000000401000 <_start>:
  401000:  b8 01 00 00 00     mov    eax,0x1
  401005:  bf 01 00 00 00     mov    edi,0x1
  40100a:  48 be 00 20 40 00  movabs rsi,0x402000
  401014:  0f 05              syscall
```

04

ابزارهای بیشتر

strace هر system call که یک پروگرام انجام می‌دهد را نشان می‌دهد. readelf، section ها و ...

Ghidra، یک ابزار رایگان مهندسی معکوس، فایل‌های باینری را دوباره به کودی خوانا شبیه C تبدیل ...

ASSEMBLY LANGUAGE · 11

terminal

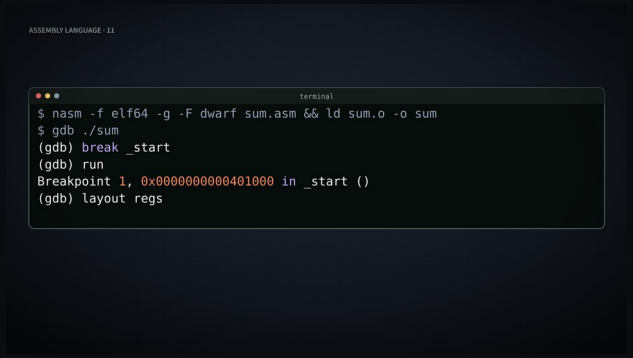
```
$ strace ./hello
write(1, "Salaam, World!\n", 15) = 15
exit(0)                          = ?
$ readelf -S hello | grep -E 'text|data'
  [ 1] .text   PROGBITS  0000000000401000
  [ 2] .data   PROGBITS  0000000000402000
```

05

نقشهٔ درس


1
شروع GDB
2
قدم زدن در کود
3
بررسی register ها و حافظه
4
objdump: disassembly
5
ابزارهای بیشتر

منابع و مطالعهٔ بیشتر





تشکر از تماشای شما

MyWebUniversity.com

آموزش رایگان تکنالوژی از سال ۲۰۰۰ — انگلیسی و دری

@MyWebUniversity-Dari · @MyWebUniversity