

CSE 127 Week 2

Discussion

PA1: GDB + x86

- Friday, October 7th at 11:59 pm
- Group submissions - Groups of 2
- Goal is to prepare you for the next assignment

Virtual Machine

- Weird stack trace on startup and system doesn't start
 - In advanced boot options, try booting using sysvinit or switch to an older kernel
- VirtualBox throws an error on startup
 - This varies, but on windows it is most likely because you haven't enabled Hyper-V, which there are resources to do [here](#).
- To make SSH work within WSL or other OS you can enable [port-forwarding](#).
- Use QEMU for M1 macs.
- SSH is not required, but you need a way to transfer your solution out of the VM.

GDB



- GNU Debugger
- Allows you to "see" inside your program
 - See registers, memory access, instructions
 - Breakpoints allow you to pause execution at any point

GDB Demo

GDB

- Layout next → shows the code
- b main → add breakpoint
- info frame → print info about the current stack frame
- info registers → registers in both hex and natural format
- x/[count][format][unit] → defaults: count = 1, format = x, unit = w
- x/10x \$ebp+4 → show as hex
- x/10i \$eip → show as instructions
- x/5c name → show as char
- More uses of x [here](#)

GDB

- disass main → disassemble a function
- tui enable → enable text user interface (gdb -tui)
- layout src/asm → show source code/assembly
- tui reg general → show registers
- print i → prints variable value
- print i=10 → sets variable value
- set \$ebp = 123 → set value for a register
- set {int}0xffff12345 = 123 → set value for a memory region

More resources [here](#)

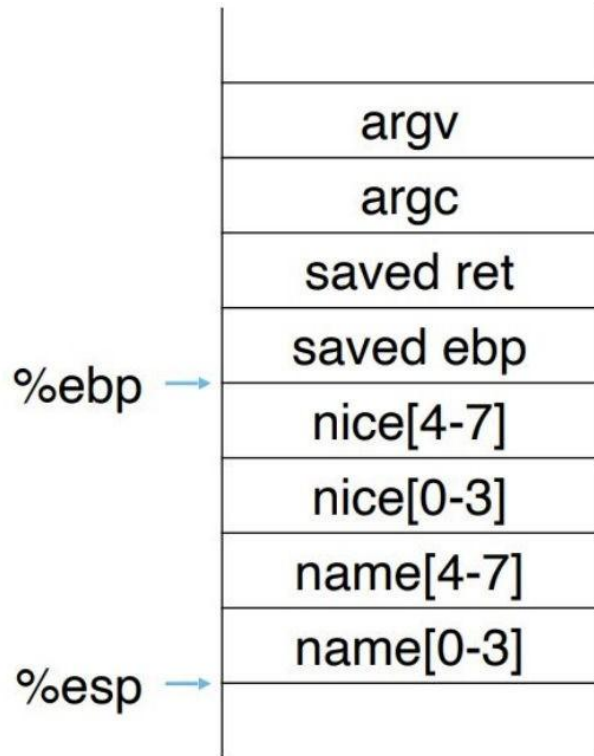
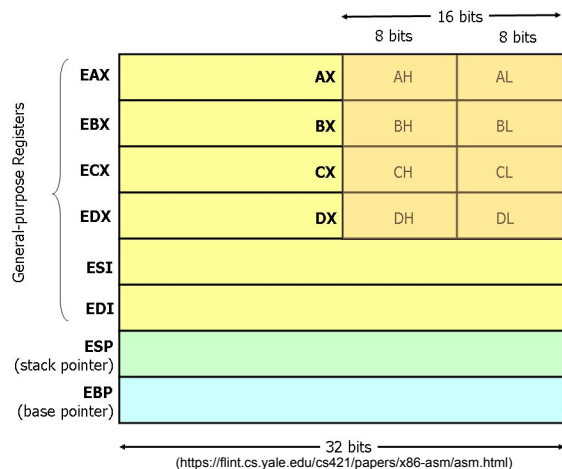
echo

- Write a simplified version of the echo utility using the example code provided
- Use only raw x86 assembly code
- Hints:
 - Strings are terminated by a null byte (a null byte has value 0x0)
 - You might need to write a loop
 - You can make more than one system call
 - You can append a `-g` flag to the `ASFLAGS` in `Makefile` to get debugging information generated, but you need to make sure your program also work without the flag

x86 Registers

x86 Registers

- `%esp`, or the Stack Pointer
 - Designates the top of the stack
 - Grows from high to low memory addresses
- `%ebp`, or the Frame Pointer/Base Pointer
 - Points to middle of stack frame(to the saved base pointer)
 - Doesn't move as function calls are made



x86 Registers

- %eip, or the Instruction Pointer
 - Holds the address of the next instruction to be executed

%eip →

```
pushl    %ebp
movl     %esp, %ebp
subl     $40, %esp
movl     16(%ebp), %eax
movl     %eax, -28(%ebp)
movl     %gs:20, %eax
movl     %eax, -12(%ebp)
xorl     %eax, %eax
```

x86 Registers

- `inc %eax` → `eax`
- `inc (%eax)` → `*eax`
- `inc 4(%eax)` → `*(eax + 4)`
- `inc 4(%eax, %ebx, 2)` → `*(eax + 4 + %ebx * 2)`

<https://patshaughnessy.net/2017/1/20/pointers-in-c-and-x86-assembly-language>

x86 Instructions

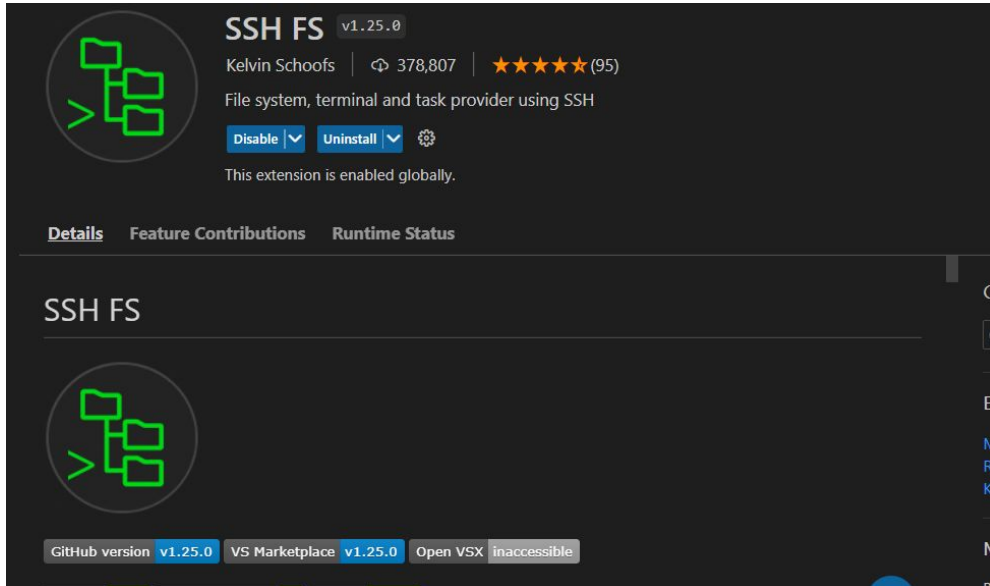
- movl
- cmpb
- je, jne, jmp
- add, sub, inc, dec
- int 0x80 - ?

x86 Instructions

- Byte (B)
 - 8-bits
- Word (W)
 - 16-bits = 2 bytes
- Double word (L)
 - 32-bits = 4 bytes
- Quad word (Q)
 - 64-bits = 8 bytes

SSH FS with VS Code

get syntax highlighting, File system GUI and terminal with VSCode



The screenshot shows the VS Code Marketplace page for the SSH FS extension. At the top left is the extension's icon, a green terminal prompt with three overlapping file icons. To its right, the extension name "SSH FS" is displayed in white, followed by the version "v1.25.0". Below the name, the author "Kelvin Schoofs" is listed, along with a download count of "378,807" and a star rating of "★★★★★ (95)". A description reads "File system, terminal and task provider using SSH". Below the description are two buttons: "Disable" and "Uninstall", both with dropdown arrows, and a gear icon for settings. A status message says "This extension is enabled globally." Below this is a navigation bar with three tabs: "Details" (selected), "Feature Contributions", and "Runtime Status". The main content area has a heading "SSH FS" and a smaller version of the extension icon. At the bottom, there are three buttons: "GitHub version v1.25.0", "VS Marketplace v1.25.0", and "Open VSX inaccessible".

SSH FS v1.25.0
Kelvin Schoofs | 378,807 | ★★★★★ (95)
File system, terminal and task provider using SSH
Disable Uninstall ⚙️
This extension is enabled globally.

Details Feature Contributions Runtime Status

SSH FS

GitHub version v1.25.0 VS Marketplace v1.25.0 Open VSX inaccessible