SecurityTube Linux Assembly Expert (SLAE^{64})

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?

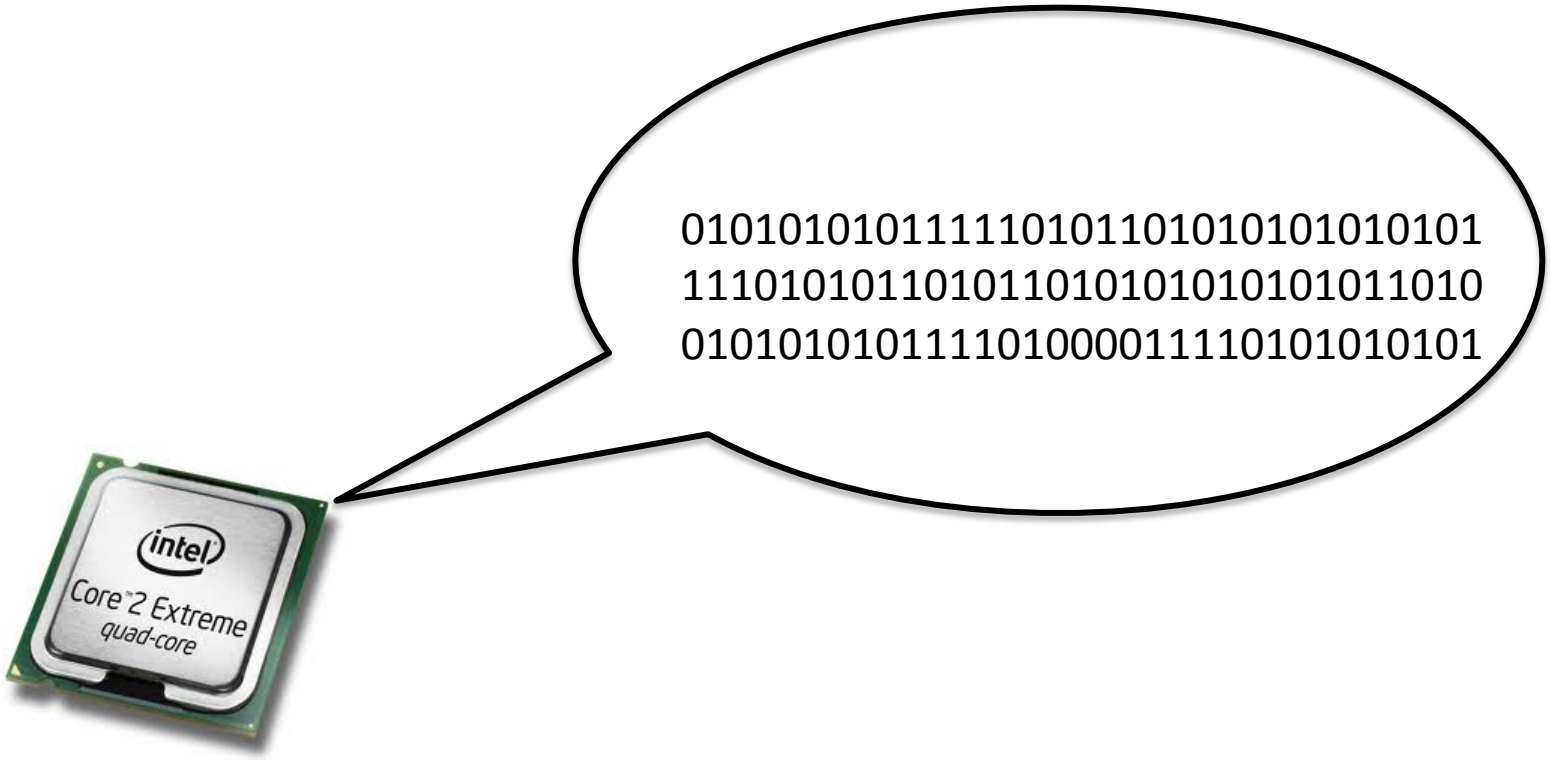
Vivek Ramachandran
SWSE, SMFE, SPSE, SGDE, SISE, SLAE^{64}, SLAE^{32} Course Instructor

http://SecurityTube-Training.com

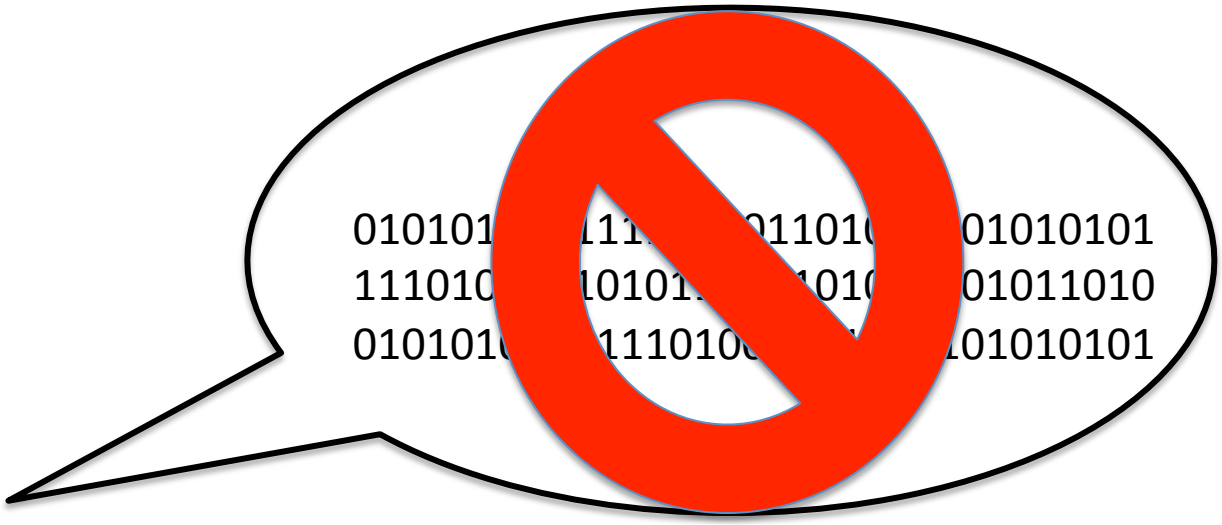
What is Assembly Language?

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

I only speak binary!



Humans cannot speak binary



Assembly Language

Assembly Language

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

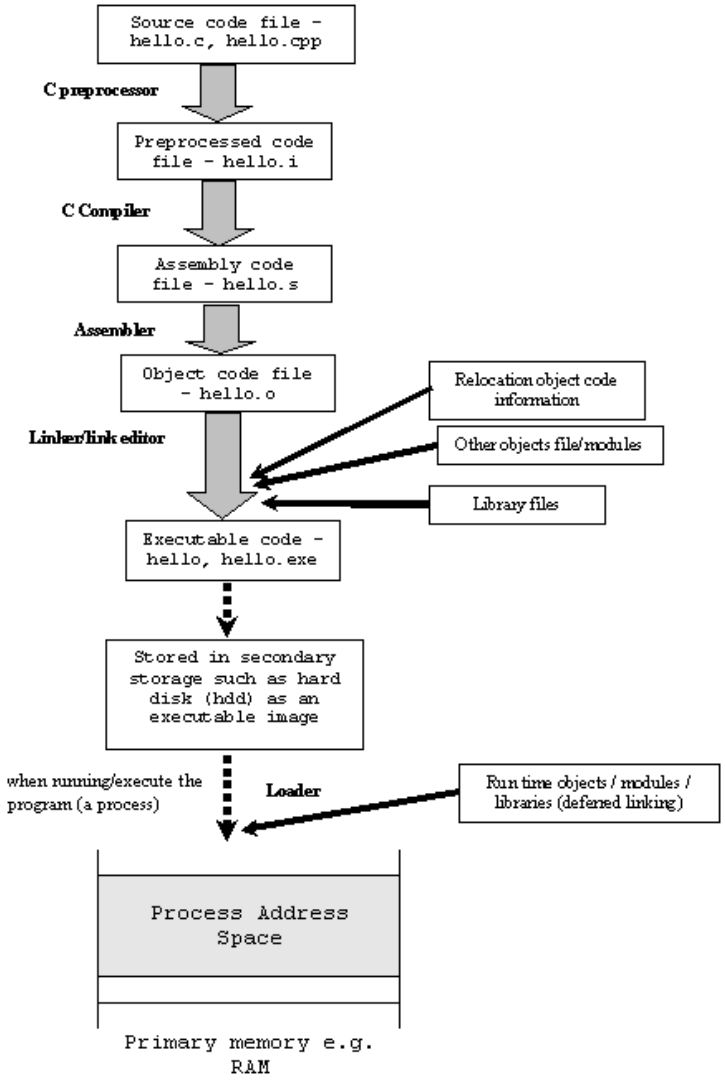
Assembler + Linker

Translator

Machine Language

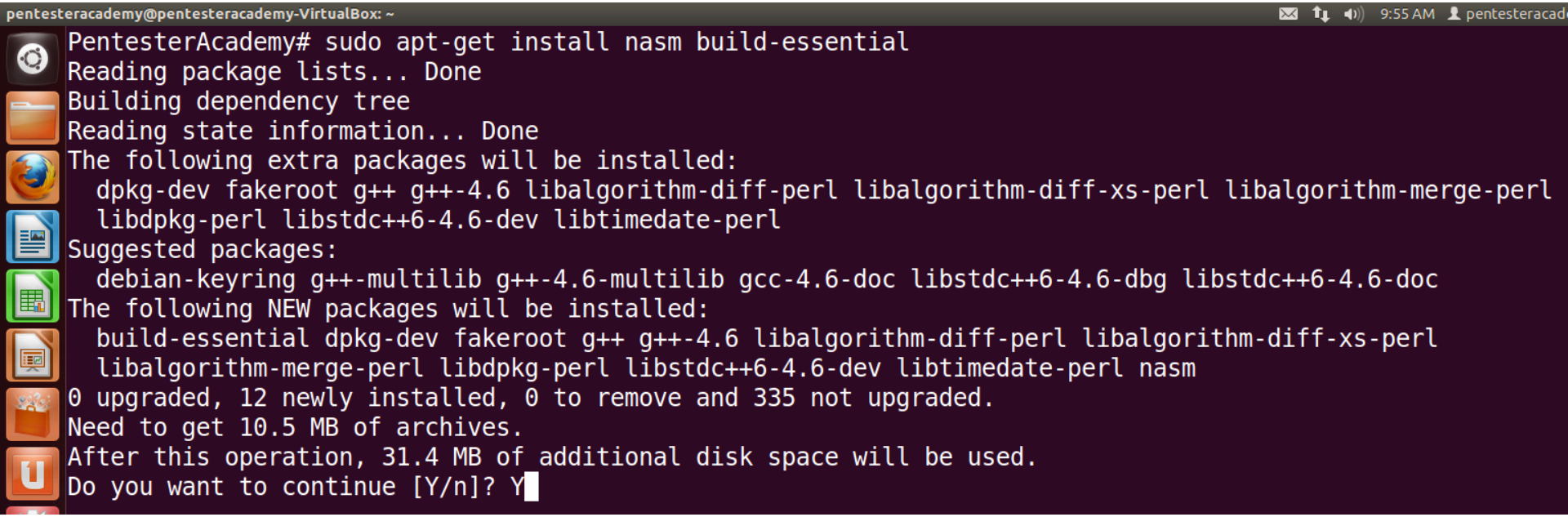
```
010110100101
111010101010
101010101010
```

Correlation with HLLs



http://www.tenouk.com/ModuleW_files/ccompilerlinker001.png

Installing Nasm, Build-Essential



How does 64-bit ASM look like?

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
```