Revengg

Use of Linux in CTF events

- It has an awesome command line.
- Bash Scripting
- Has all the tools required for CTFing.

WSL

- WSL stands for Windows Subsystem for Linux
- WSL can run Linux programs on Windows

Linux

1- Shell redirection / shell piping

Pipes connect the standard output of one command to the standard input of another. Eg. cat pipe.txt | grep “second” pipe.txt | grep second

Shell redirection can redirect that output to a file using the > operator. Eg. echo “hello” > file.txt

Linux

2- **file command**

file command is used to determine the type of a file.

3- nano command

Command Line Text Editor similar to vim.

4- find, grep, strings

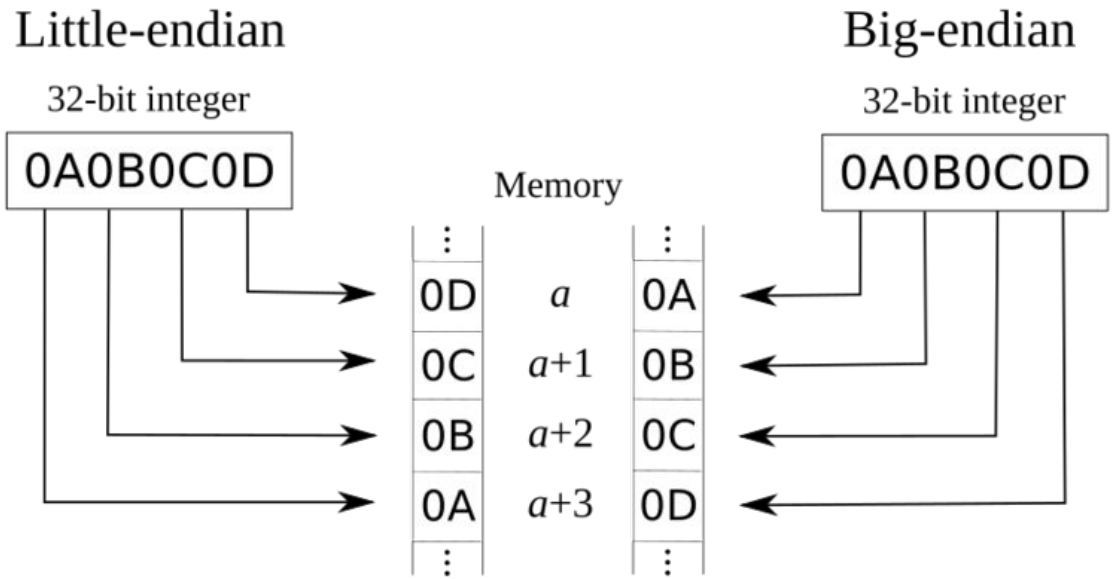
- find command is used to search a file or directory in a file hierarchy.eg find dir/ -name hi.txt
- Grep command is used to search in a file

- The strings command returns each string of printable characters in files.

Different number systems (Binary, Octal, Base-64, Hexadecimal)

Source	Text (ASCII)	M							a								n							
	Octets	77 (0x4d)							97 (0x61)								110 (0x6e)							
Bits		0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Base64 encoded	Sextets	19							22					5				46							
	Character	T							W					F				u							
	Octets	84 (0x54)							87 (0x57)					70 (0x46)				117 (0x75)							

Little/Big Endian



WEB

1- Developer Tools

2- Methods of HTTP

- GET (Read)
- POST (Create)
- PUT (replace
- DELETE (delete)

WEB

3- **Cookies**

An HTTP cookie (web cookie, browser cookie) is a small piece of data that a server sends to the user's web browser.

4- **User Agent**

The User-Agent request header is a characteristic string that lets servers and network peers identify the application, operating system, vendor, and/or version of the requesting user agent.

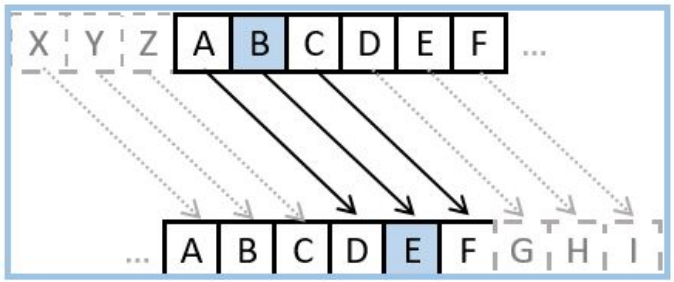
Forensics

- Hex Editor
- Headers and Footers in files
- Magic Numbers
  - Magic numbers are the first few bytes of a file that are unique to a particular file type.

Cryptography

1- Plaintext and CipherText

2- Caesar Cipher



SHIFT +3

This Caesar cipher has a shift of 3 characters.

The letter ‘A’ becomes a ‘D’. The letter ‘B’ becomes ‘E’.

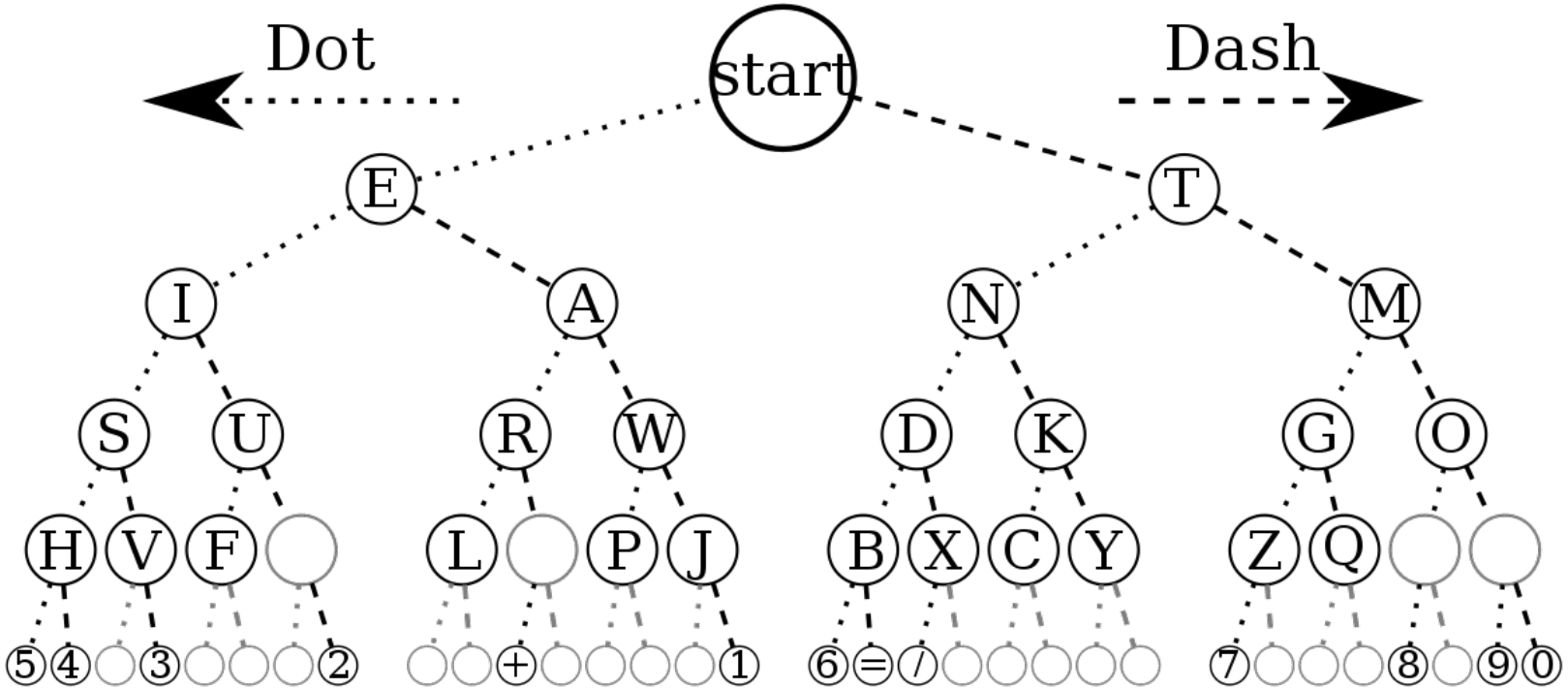
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Plaintext

Ciphertext

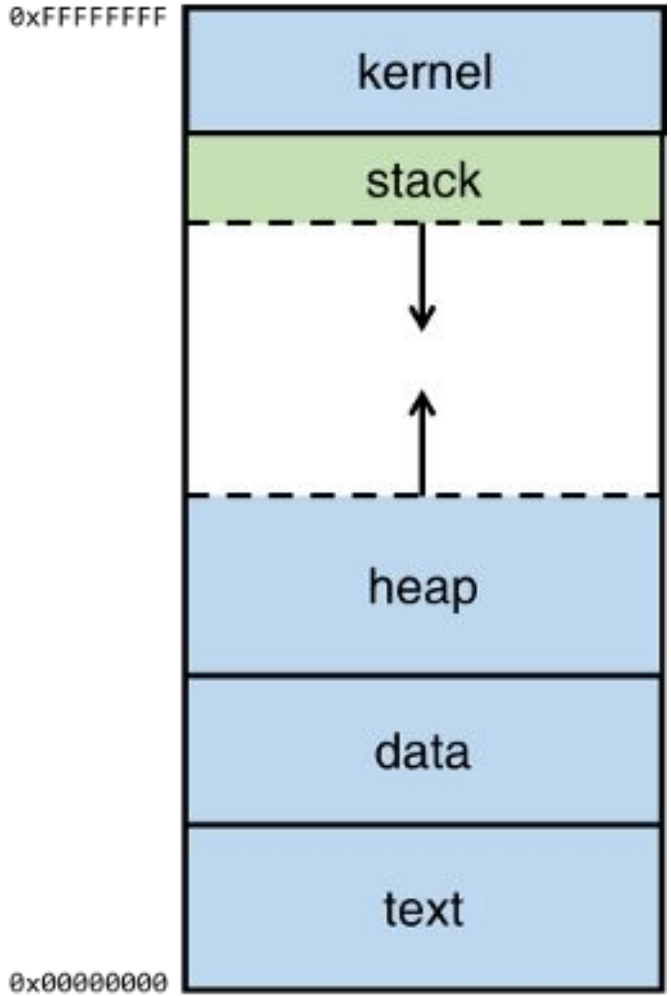
Cryptography

3- Morse Code



Binary / Binary Exploitation

- How a program compiles
  - Assembly language
  - gcc -S filename.c -o outputfilename.asm
- Binary exploitation: https://uperesia.com/buffer-overflow-explained

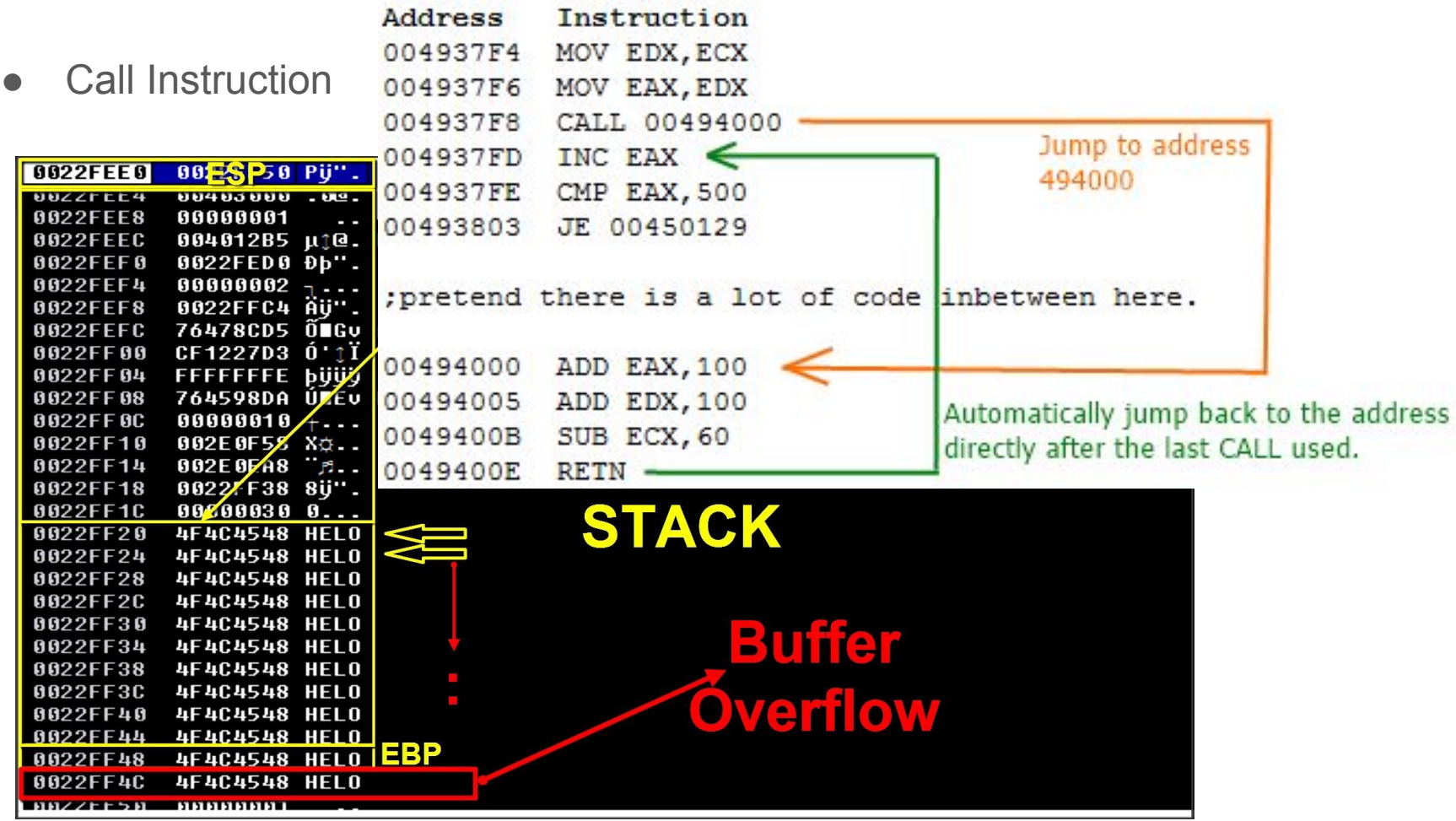


```
section     .text
global      _start                  ;must be declared for linker (ld)

_start:                             ;tell linker entry point

    mov     edx,len                 ;message length
    mov     ecx,msg                 ;message to write
    mov     ebx,1                   ;file descriptor (stdout)
    mov     eax,4                   ;system call number (sys_write)
    int     0x80                    ;call kernel

    mov     eax,1                   ;system call number (sys_exit)
    int     0x80                    ;call kernel

section     .data

msg     db  'Hello, world!',0xa     ;our dear string
len     equ $ - msg                 ;length of our dear string
```

```
#include <stdlib.h>
int sub(int x, int y){
        return 2*x+y;
}

int main(int argc, char ** argv){
        int a;
        a = atoi(argv[1]);
        return sub(argc,a);
}
```

```
.text:00000000 _sub:      push   ebp
.text:00000001            mov    ebp, esp
.text:00000003            mov    eax, [ebp+8]
.text:00000006            mov    ecx, [ebp+0Ch]
.text:00000009            lea    eax, [ecx+eax*2]
.text:0000000C            pop    ebp
.text:0000000D            retn
.text:00000010 _main:     push   ebp
.text:00000011            mov    ebp, esp
.text:00000013            push   ecx
.text:00000014            mov    eax, [ebp+0Ch]
.text:00000017            mov    ecx, [eax+4]
.text:0000001A            push   ecx
.text:0000001B            call   dword ptr ds:__imp__atoi
.text:00000021            add    esp, 4
.text:00000024            mov    [ebp-4], eax
.text:00000027            mov    edx, [ebp-4]
.text:0000002A            push   edx
.text:0000002B            mov    eax, [ebp+8]
.text:0000002E            push   eax
.text:0000002F            call   _sub
.text:00000034            add    esp, 8
.text:00000037            mov    esp, ebp
.text:00000039            pop    ebp
.text:0000003A            retn
```

- Call Instruction



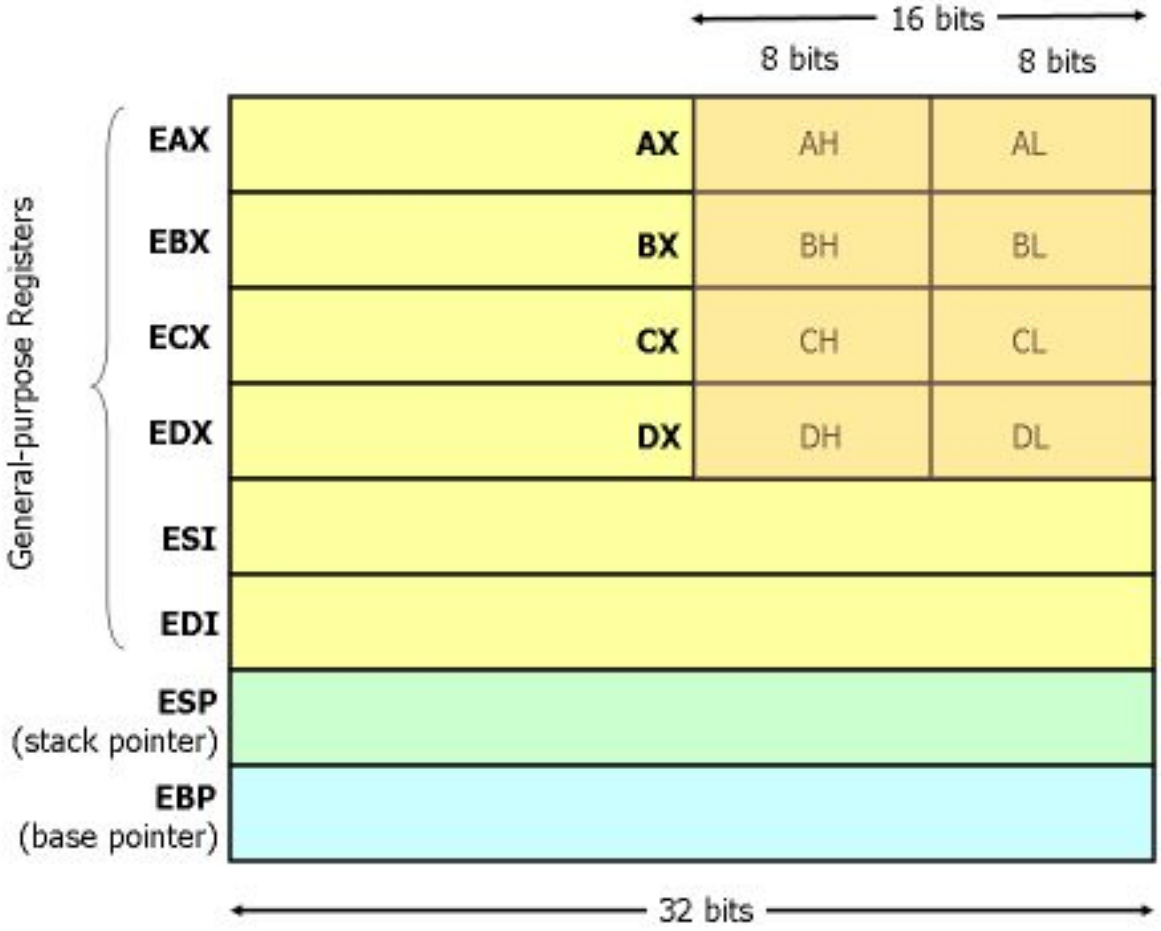


Figure 1. x86 Registers

Disassembler / Decompiler

- Disassembler
  - A disassembler is a software tool which transforms machine code into a human readable mnemonic representation called assembly language.
  - c, c++
  - GDB, Hopper, Radare2
- Decompiler
  - Software used to revert the process of compilation. Decompiler takes a binary program file as input and output the same program expressed in a structured higher-level language.
  - java, c#, android apps
  - Google them :P