Revengg
[Capture The Flag]

Challenge Categories:

- Misc
- Web
- Crypto
- Forensics
- Binary Exploitation
- Reversing
- OSINT
- .....

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.

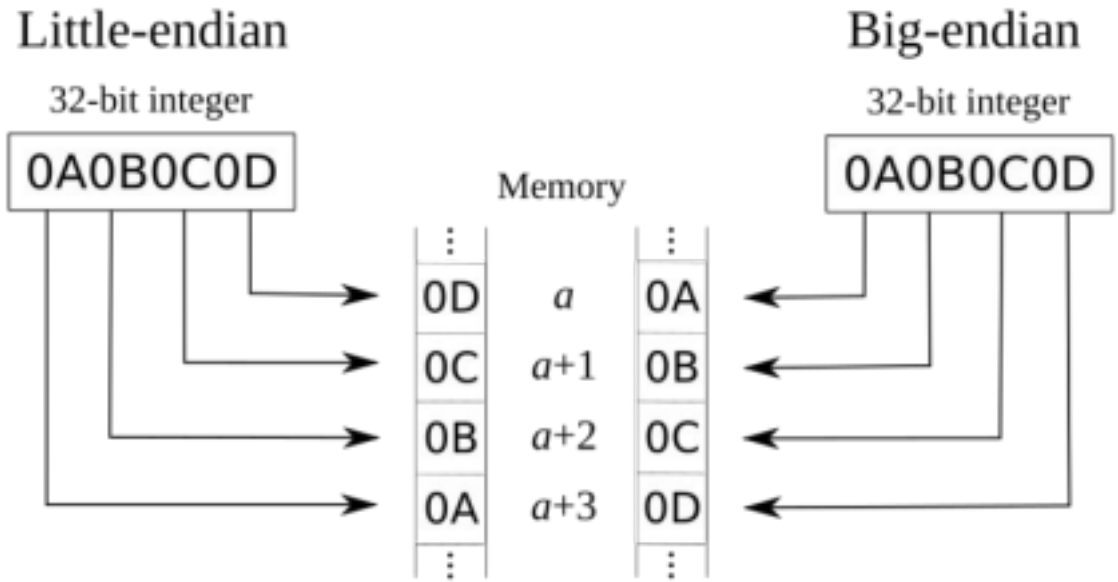
4- find, grep, strings

- 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)

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- **HTTP Headers (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.

Resources : MDN web docs

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.

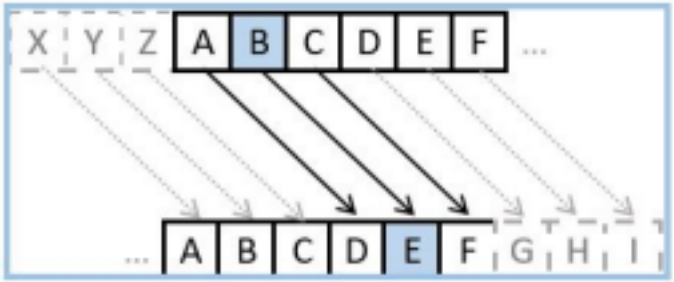
Tools : xxd, hexdump, hexedit, ghex, bless hex editor

Cryptography

1- Plaintext and CipherText

Plaintext ---------> [Encryption Algorithm] ---------> 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'.

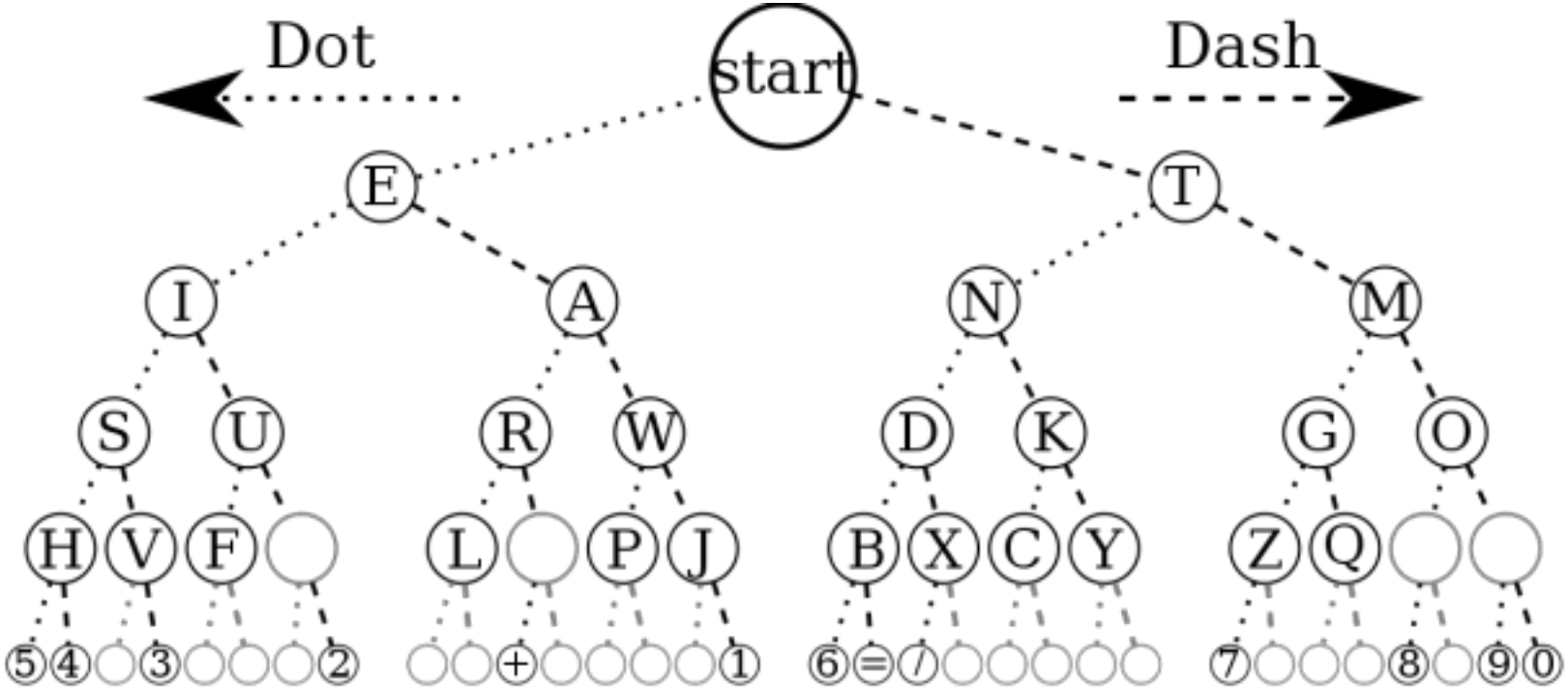
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Plaintext

Ciphertext

some more ciphers : Vigenere Cipher,Atbash Cipher, Affine Cipher, ROT13, ROT47

3- Morse Code



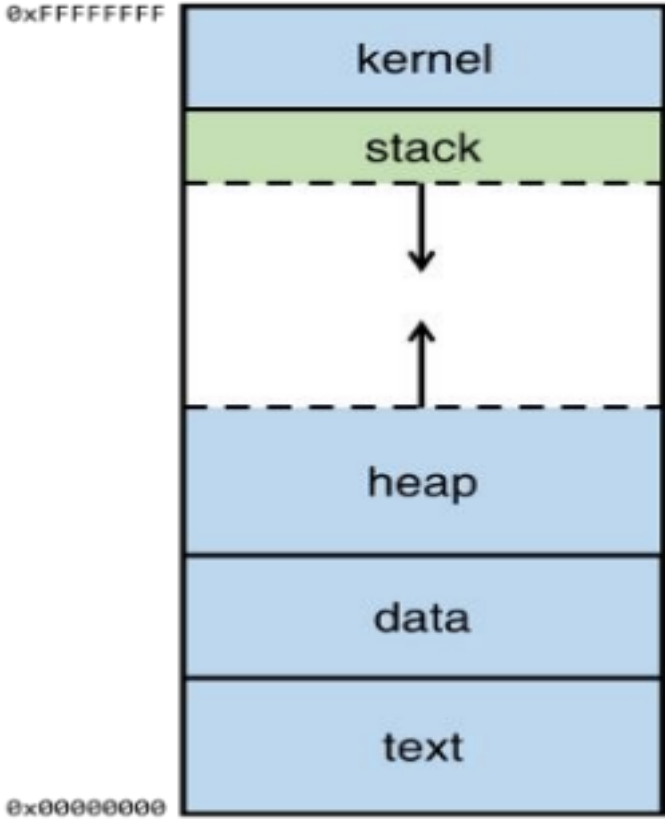
Resources : CyberChef, cryptii.com, dcode.fr, tio.run

Binary / Binary Exploitation

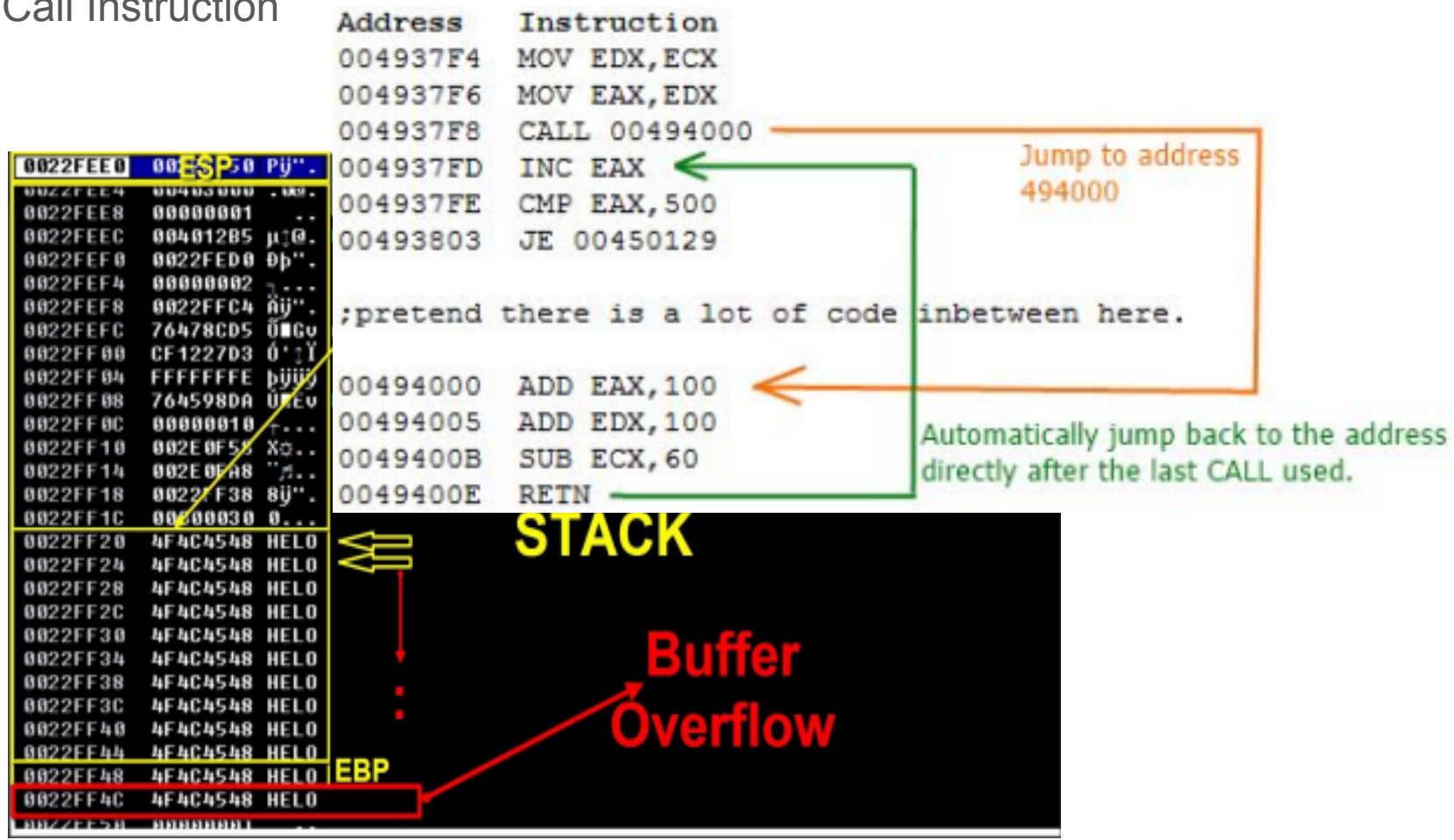
- How a program compiles
  - Assembly language
  - gcc -S filename.c -o outputfilename.asm
  - Binary exploitation:

    buffer overflow explained

    Binary Exploitation / Memory Corruption by LiveOverflow



- Call Instruction



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 (Mac), Radare2 <----- [CLI]

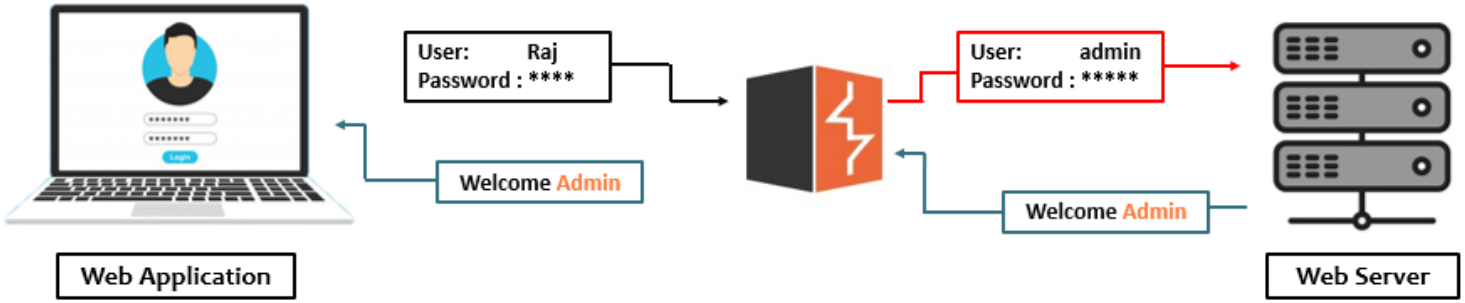
  Dynamic Analysis ----> IDA
- Decompiler
  - Software used to revert the process of compilation. Decompiler takes a binary program file as input and output the same program expressed in a structured higher-level language.
  - java, c#, android apps
  - Google them :P

  Ghidra

  GUI -----> Cutter

Proxy Interceptors

- PortSwigger’s Burp Suite
- OWASP ZAP
- Mitmproxy
- Postman



Directory Bruteforcers

- Gobuster
- DIRB
- DirBuster (Graphical User Interface) [GUI]