

# Revenng

## [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.

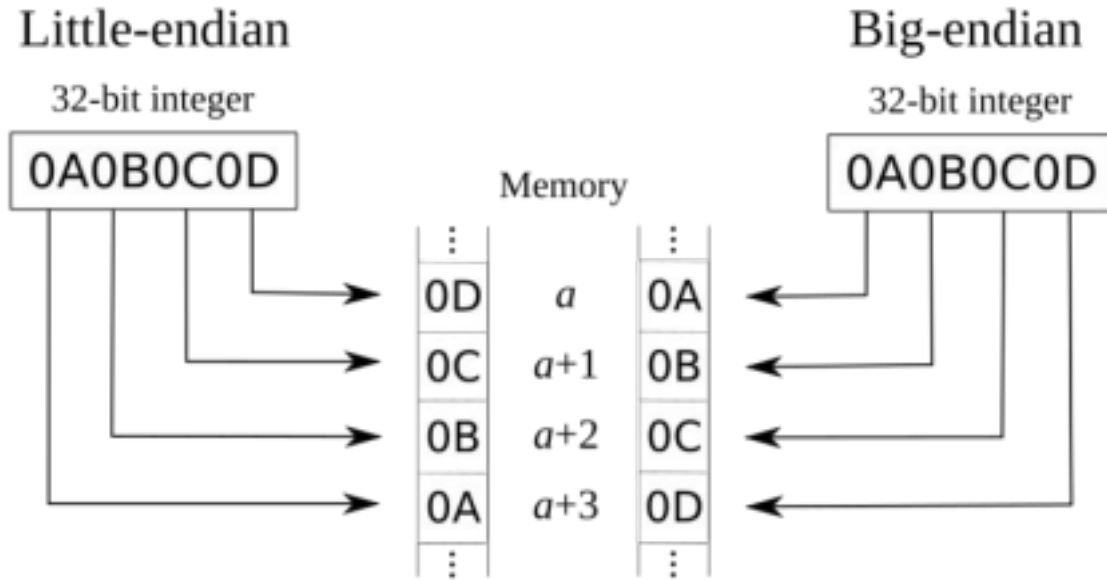
## 4- find, grep, strings

- 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)

|                       |                     |           |   |   |   |   |   |           |   |   |   |   |   |            |   |   |   |   |   |            |   |   |   |   |   |
|-----------------------|---------------------|-----------|---|---|---|---|---|-----------|---|---|---|---|---|------------|---|---|---|---|---|------------|---|---|---|---|---|
| <b>Source</b>         | <b>Text (ASCII)</b> | <b>M</b>  |   |   |   |   |   | <b>a</b>  |   |   |   |   |   | <b>n</b>   |   |   |   |   |   |            |   |   |   |   |   |
|                       | <b>Octets</b>       | 77 (0x4d) |   |   |   |   |   | 97 (0x61) |   |   |   |   |   | 110 (0x6e) |   |   |   |   |   |            |   |   |   |   |   |
| <b>Bits</b>           |                     | 0         | 1 | 0 | 0 | 1 | 1 | 0         | 1 | 0 | 1 | 1 | 0 | 0          | 0 | 0 | 1 | 0 | 1 | 1          | 0 | 1 | 1 | 1 | 0 |
| <b>Base64 encoded</b> | <b>Sextets</b>      | 19        |   |   |   |   |   | 22        |   |   |   |   |   | 5          |   |   |   |   |   | 46         |   |   |   |   |   |
|                       | <b>Character</b>    | <b>T</b>  |   |   |   |   |   | <b>W</b>  |   |   |   |   |   | <b>F</b>   |   |   |   |   |   | <b>u</b>   |   |   |   |   |   |
|                       | <b>Octets</b>       | 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.

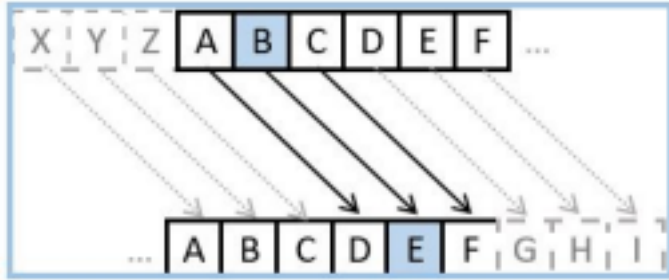
Tools : xxd, hexdump, hexedit, ghex, bless hex editor

# 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'.

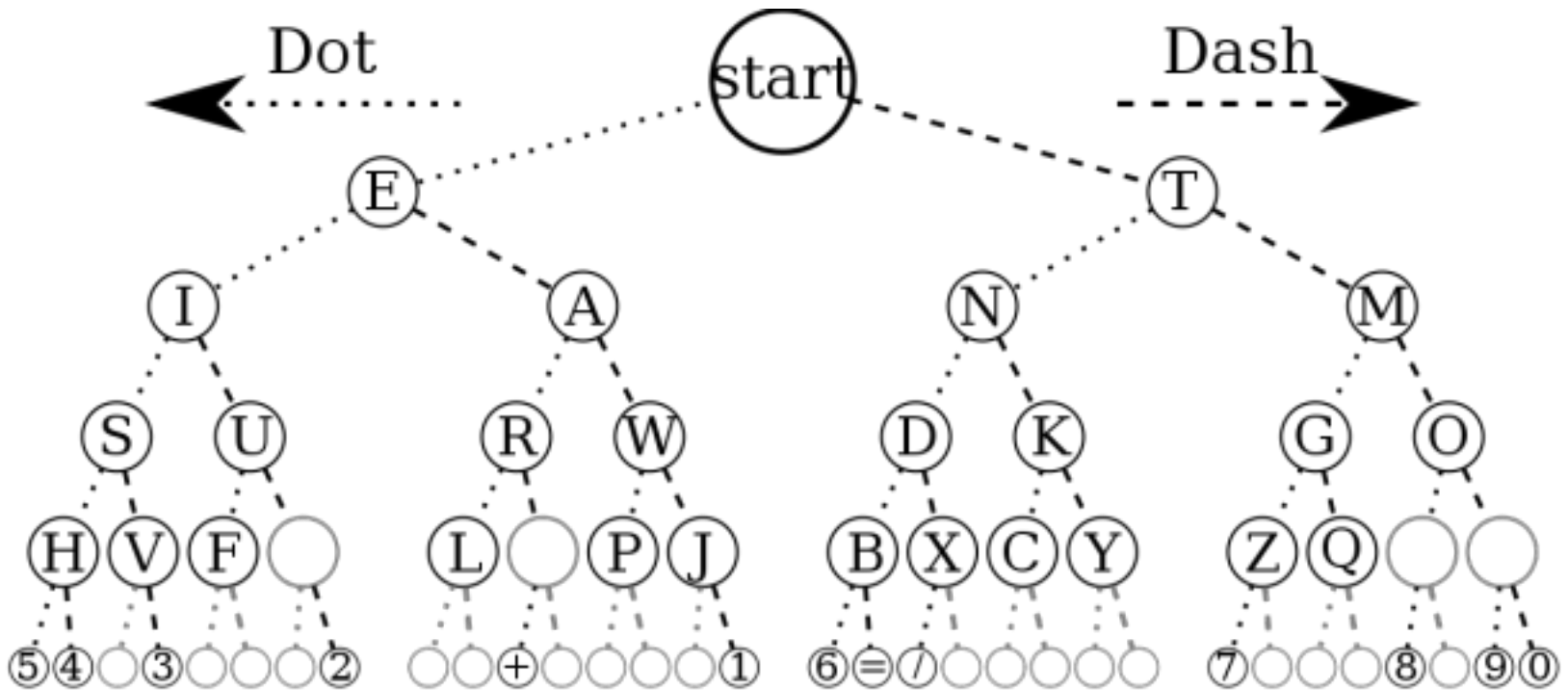
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | 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 → (points to the top row)

Ciphertext → (points to the bottom row)

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

3- Morse Code



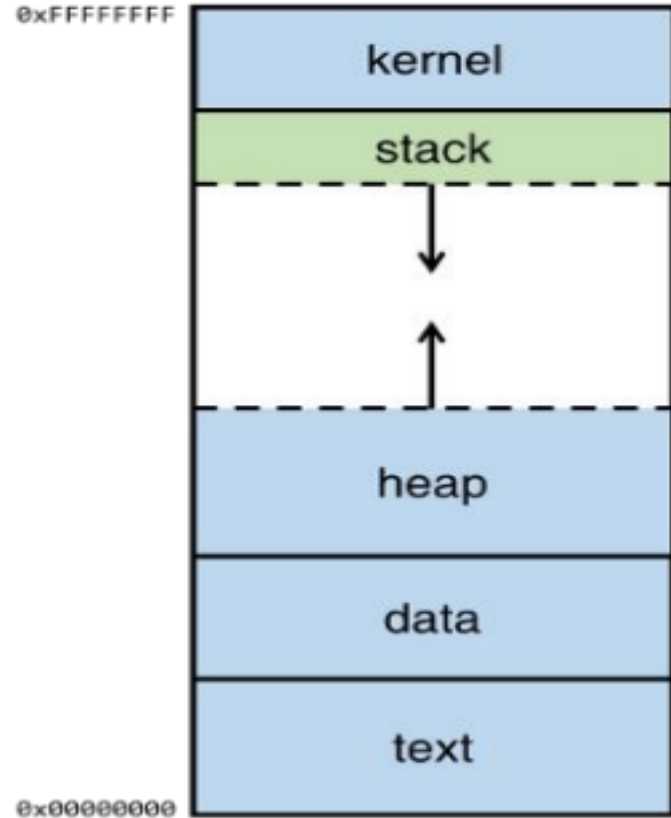
Resources : CyberChef, cryptii.com, dcode.fr, tio.run

# 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

```

Address  Instruction
004937F4  MOV EDX,ECX
004937F6  MOV EAX,EDX
004937F8  CALL 00494000
004937FD  INC EAX
004937FE  CMP EAX,500
00493803  JE 00450129

;pretend there is a lot of code inbetween here.

00494000  ADD EAX,100
00494005  ADD EDX,100
0049400B  SUB ECX,60
0049400E  RETN
  
```

|          |          |        |
|----------|----------|--------|
| 0022FEE0 | 00493000 | CALL   |
| 0022FEE4 | 00000000 | ..     |
| 0022FEE8 | 00401285 | μj0.   |
| 0022FEF0 | 0022FED0 | 0p''.  |
| 0022FEF4 | 00000002 | 3...'  |
| 0022FEF8 | 0022FFC4 | 0ij''. |
| 0022FEFC | 76478CD5 | 0MGu   |
| 0022FF00 | CF1227D3 | 0'1Y   |
| 0022FF04 | FFFFFFFF | 0jii0  |
| 0022FF08 | 764598DA | 0Euv   |
| 0022FF0C | 00000010 | 7...'  |
| 0022FF10 | 002E0F55 | Xg..   |
| 0022FF14 | 002E0FA8 | "s..   |
| 0022FF18 | 00222F38 | 8U''.  |
| 0022FF1C | 00000030 | 0...'  |
| 0022FF20 | 4F4C4548 | HELO   |
| 0022FF24 | 4F4C4548 | HELO   |
| 0022FF28 | 4F4C4548 | HELO   |
| 0022FF2C | 4F4C4548 | HELO   |
| 0022FF30 | 4F4C4548 | HELO   |
| 0022FF34 | 4F4C4548 | HELO   |
| 0022FF38 | 4F4C4548 | HELO   |
| 0022FF3C | 4F4C4548 | HELO   |
| 0022FF40 | 4F4C4548 | HELO   |
| 0022FF44 | 4F4C4548 | HELO   |
| 0022FF48 | 4F4C4548 | HELO   |
| 0022FF4C | 4F4C4548 | HELO   |
| 0022FF50 | 00000001 | ..     |

Jump to address 494000

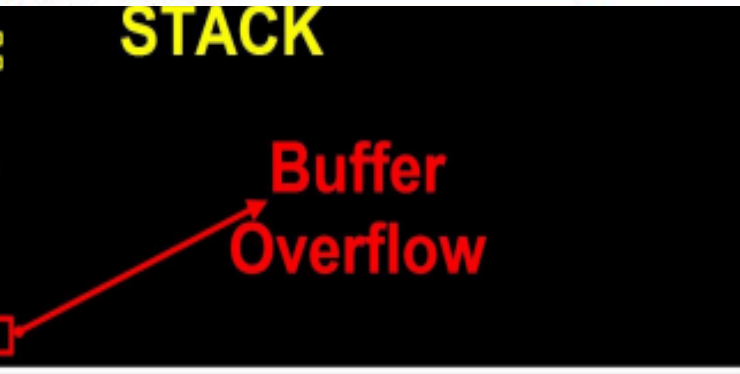
Automatically jump back to the address directly after the last CALL used.

**STACK**

**Buffer Overflow**



EBP



# 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

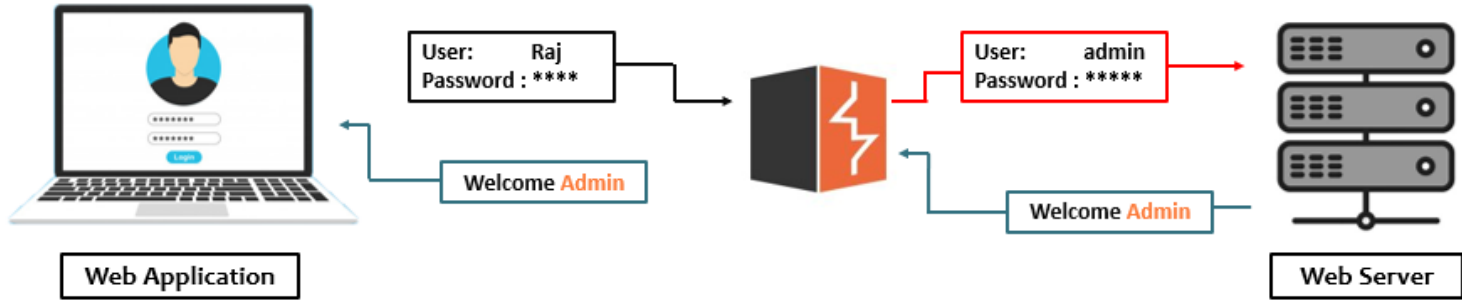
Ghidra

GUI -----> Cutter

# Proxy Interceptors

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





## Directory Bruteforcers

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