



# CYBERSECURITY 101

PAR TAD



# SOMMAIRE

1. Linux c'est kwa ?
2. Intro à WSL
3. On tape des commandes Linux
4. Tour du monde des catégories en CTF
5. A vos claviers les artistes
6. Ricard





# CHAPTER 1 :

## LINUX C'EST KWA ?



# 1. Linux c'est kwa ?



MAC OS

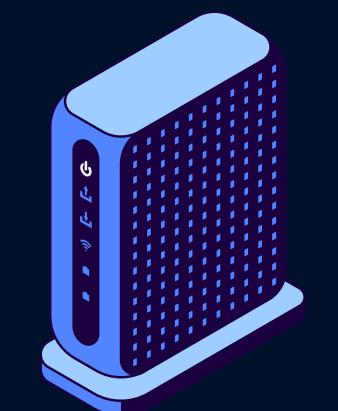
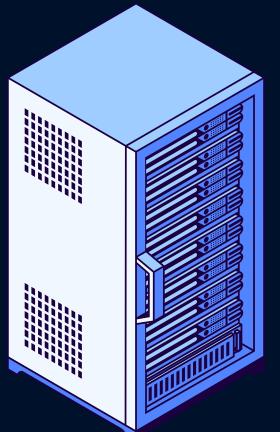


LINUX



WINDAUBÈ

un système d'exploitation comme Windows ou macOS, mais construit différemment : on peut tout modifier, tout comprendre.



# 1. Linux c'est kwa ?



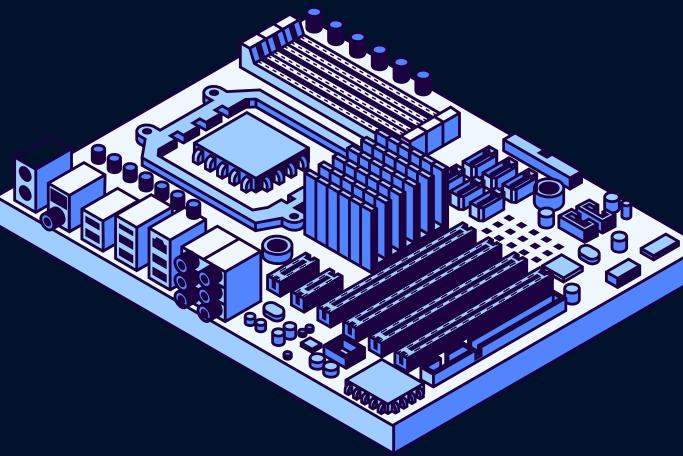
POURQUOI ON AIME LINUX ?

CONTRÔLE TOTAL SUR LA MACHINE

ACCÈS BAS-NIVEAU  
OUTILS OPEN-SOURCE  
C'EST AUSSI NOTRE CIBLE



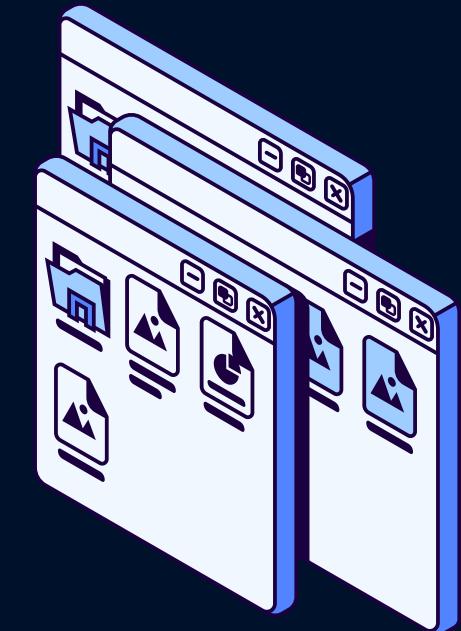
# 1. Linux c'est kwa ?



**OS = NOYAU + UTILITAIRES**

GÈRE LE MATERIEL  
(CPU, MÉMOIRE,  
DISQUE, RÉSEAU)

EMPAQUETTE LE  
NOYAU AVEC DES  
LOGICIELS POUR LE  
RENDRE UTILISABLE

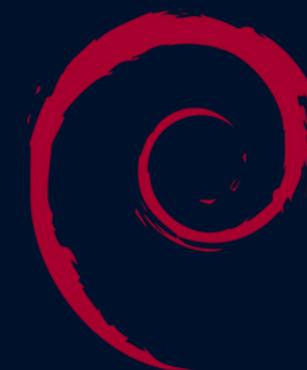


# 1. Linux c'est kwa ?

## LES DISTRIBUTIONS



UBUNTU  
(BUREAUTIQUE)



DEBIAN  
(SERVEUR)



KALI  
(SÉCURITÉ)



## CHAPTER 2 :

# INTRO À WSL

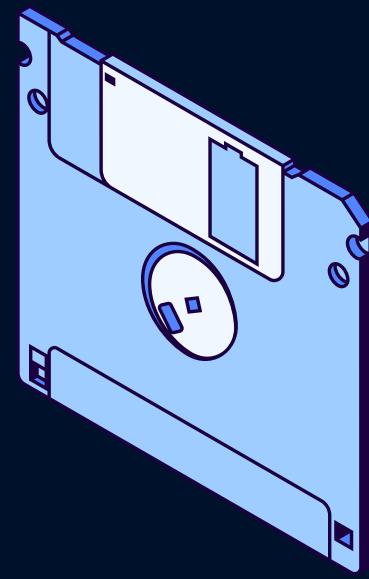


## 2. Intro à WSL

### INSTALLER LINUX



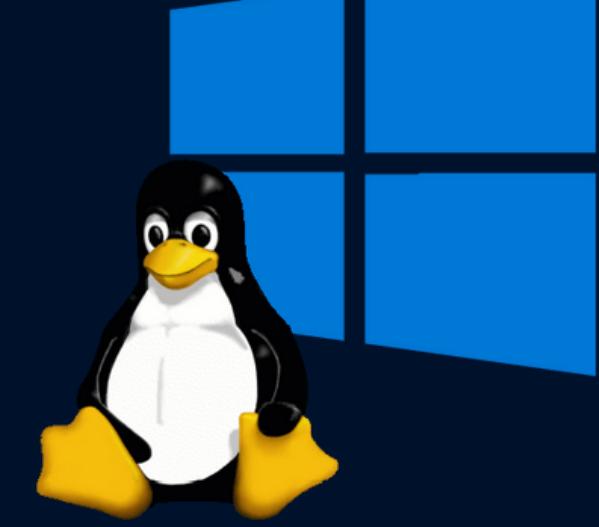
BARE METAL



DUAL BOOT



MACHINE VIRTUELLE



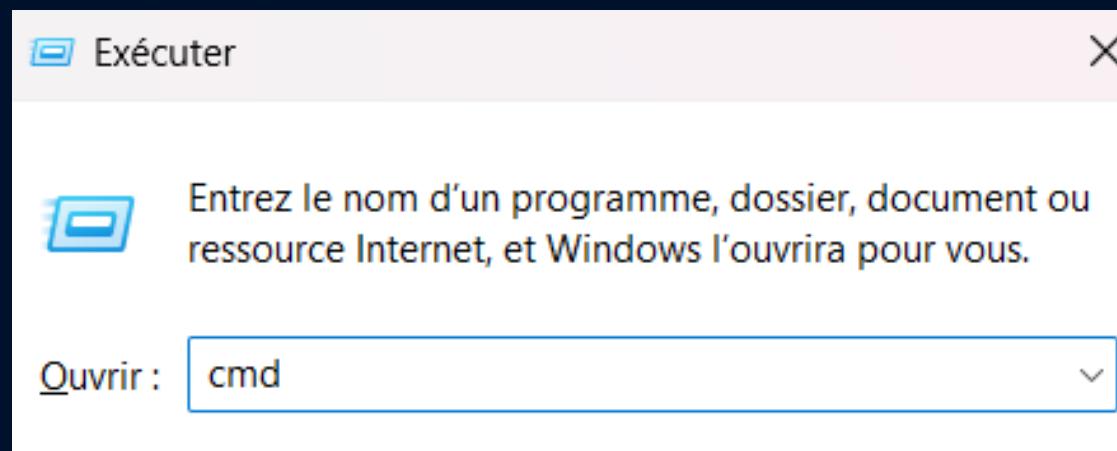
WSL



## 2. Intro à WSL

### INSTALLER WSL

1 - TOUCHE WINDOWS + R



2 - TAPER WSL + ENTRÉE

```
Version de l'image : 10.0.26100.6899  
Activation de la ou des fonctionnalités  
[=====100.0%=====  
L'opération a réussi.
```

3 - WSL --INSTALL KALI-LINUX

4 - REDÉMARRER LE PC

5 - BRAVO !! GG WP ! EAZYWIN !



# CHAPTER 3 :

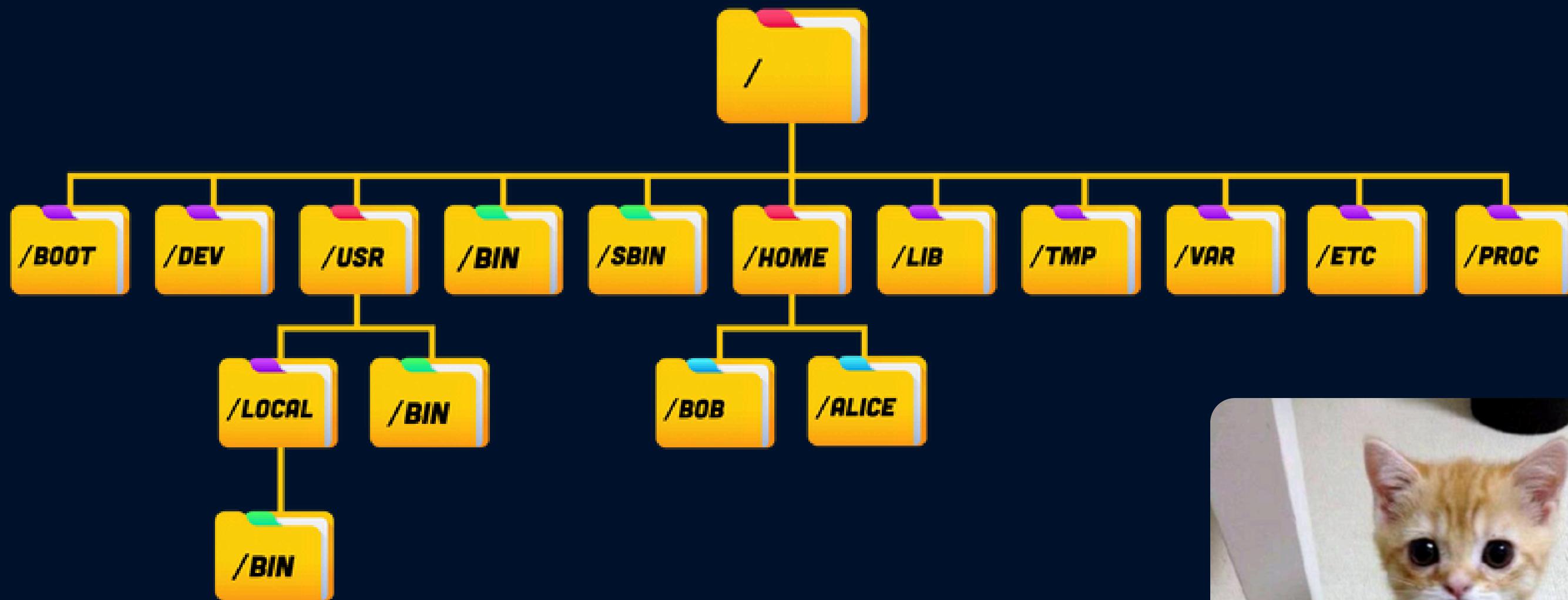
# ON TAPE DES COMMANDES

# LINUX

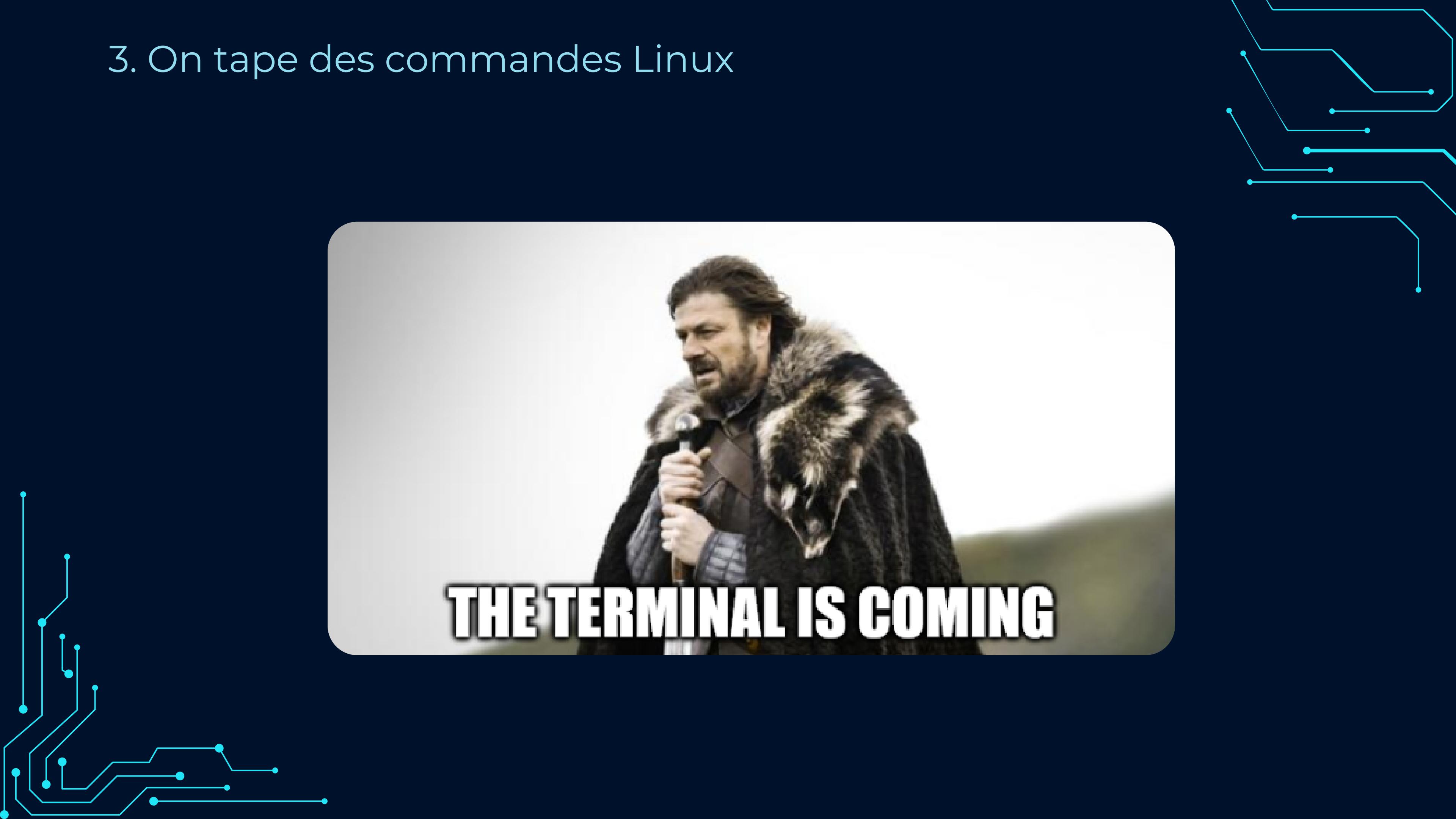


### 3. On tape des commandes Linux

## LE SYSTÈME DE FICHIER



### 3. On tape des commandes Linux



### 3. On tape des commandes Linux

#### RÉSUMÉ DES COMMANDES UTILES :

ls  
cd  
pwd  
mkdir  
rm  
mv  
echo  
>  
head  
tail

whois  
whoami  
id  
sudo  
su  
grep  
pipe |  
ps  
chmod  
ctrl +c

clear  
man  
xxd  
ifconfig  
cat  
curl  
ping  
touch

ctrl



# CHAPTER 4 :

## TOUR DU MONDE DES CATÉGORIES EN CTF



# 4.Tour du monde des catégories en CTF

WEB

Please enter your details

**Welcome back**

Email address

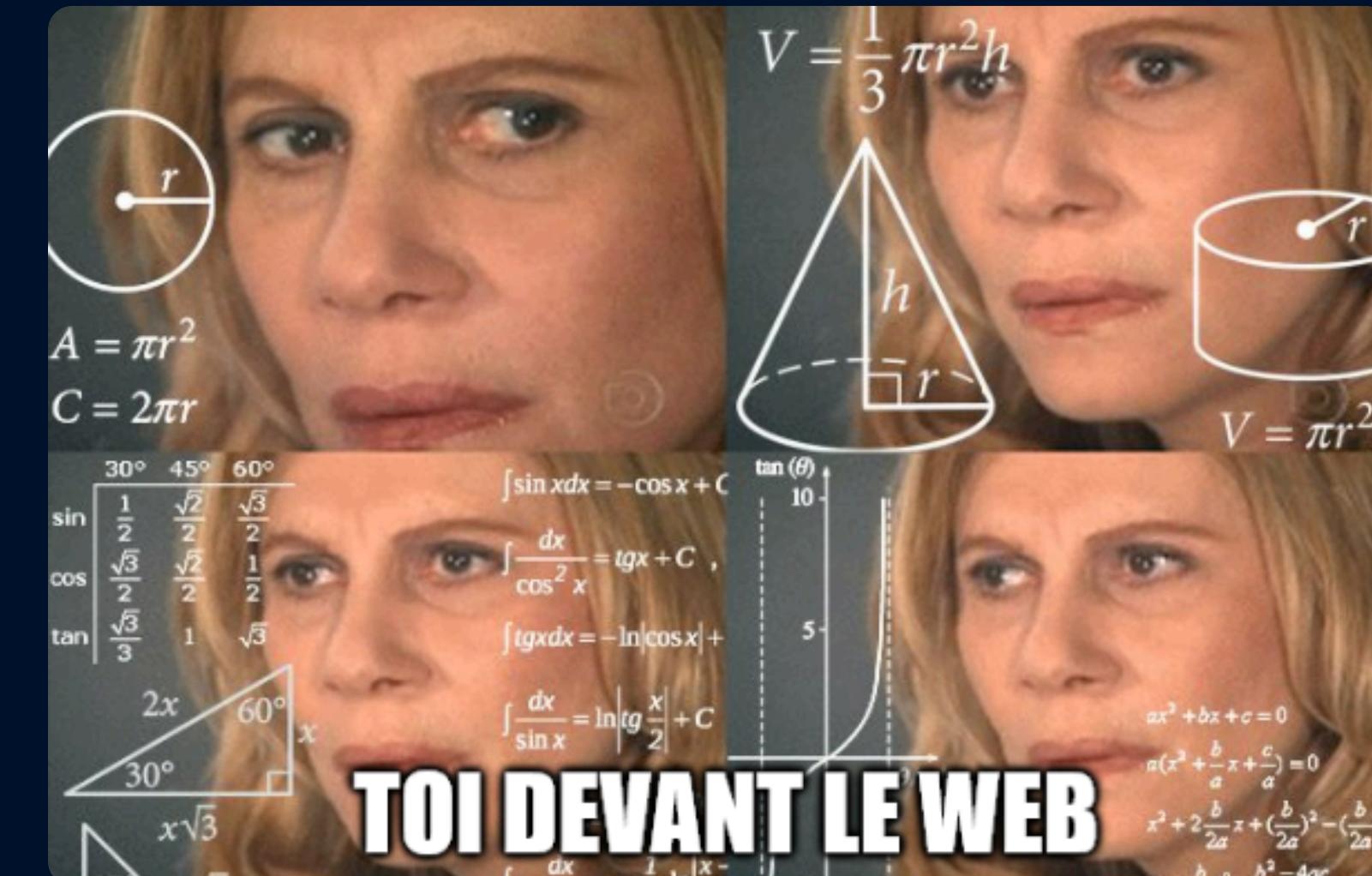
Password

Remember for 30 days      [Forgot password](#)

**Sign up**

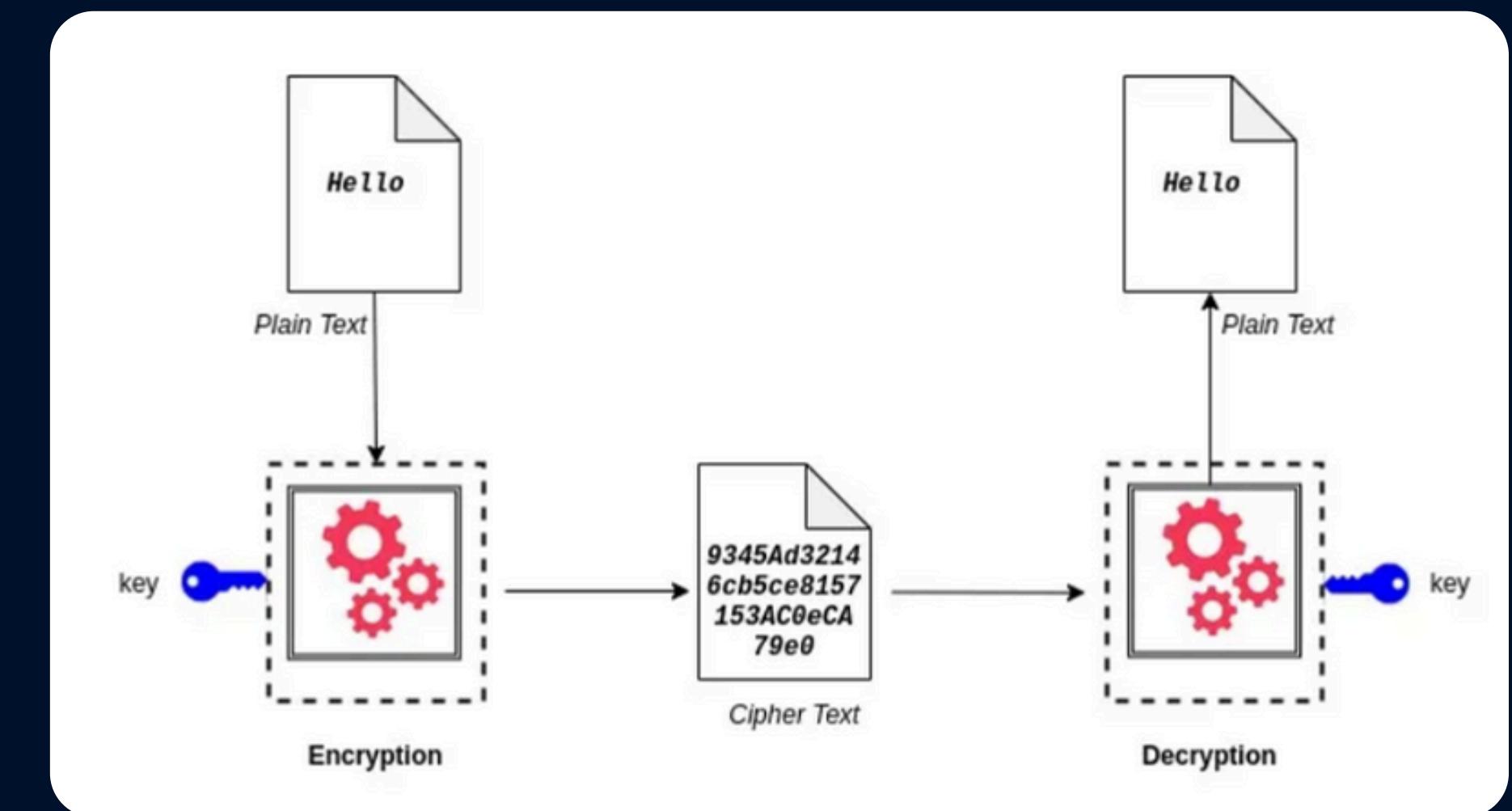
 [Sign in with Google](#)

Don't have an account? [Sign up](#)



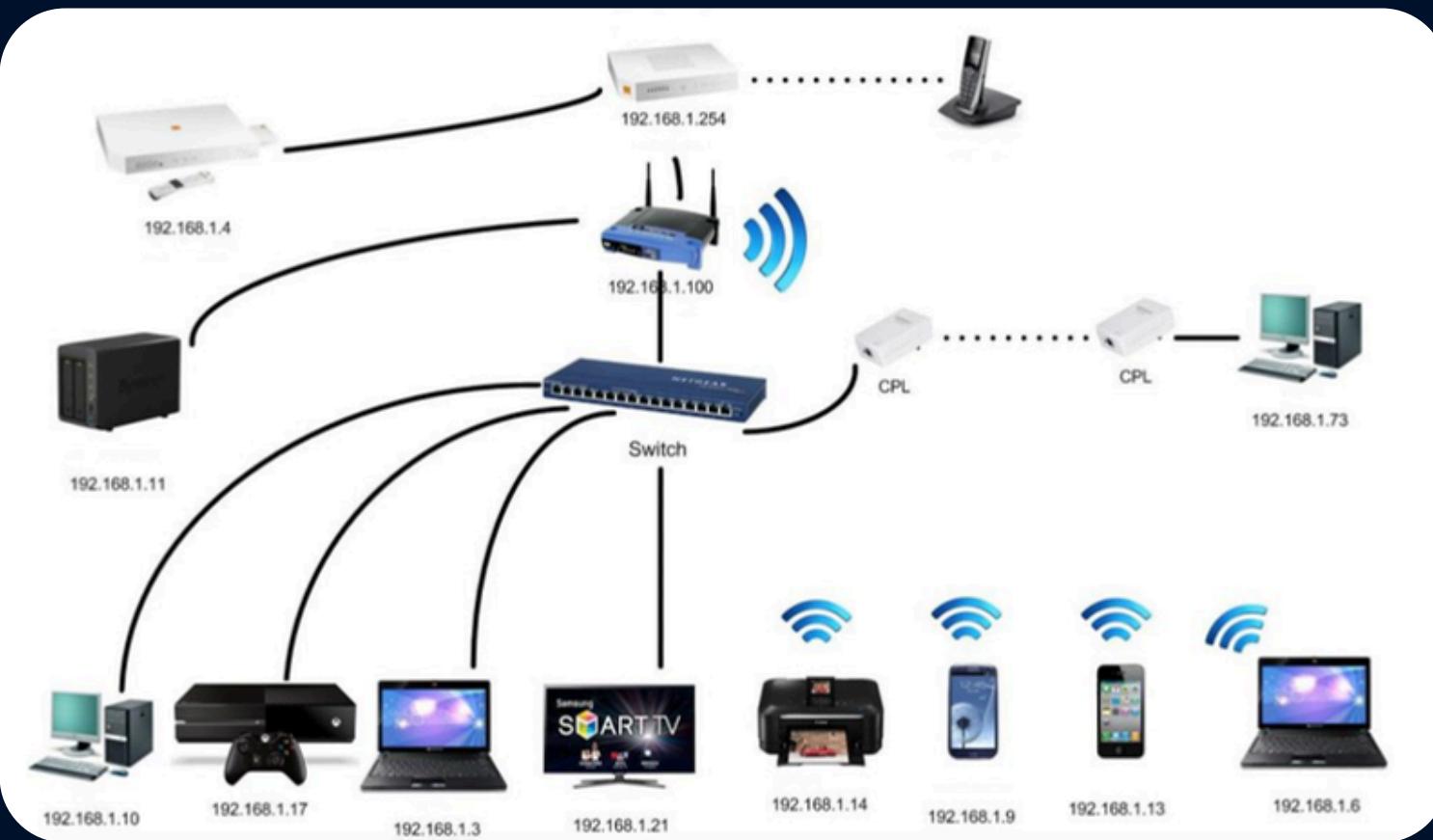
## 4.Tour du monde des catégories en CTF

### CRYPTOGRAPHIE



## 4.Tour du monde des catégories en CTF

### RÉSEAU



# 4.Tour du monde des catégories en CTF

## FORENSICS



# 4.Tour du monde des catégories en CTF

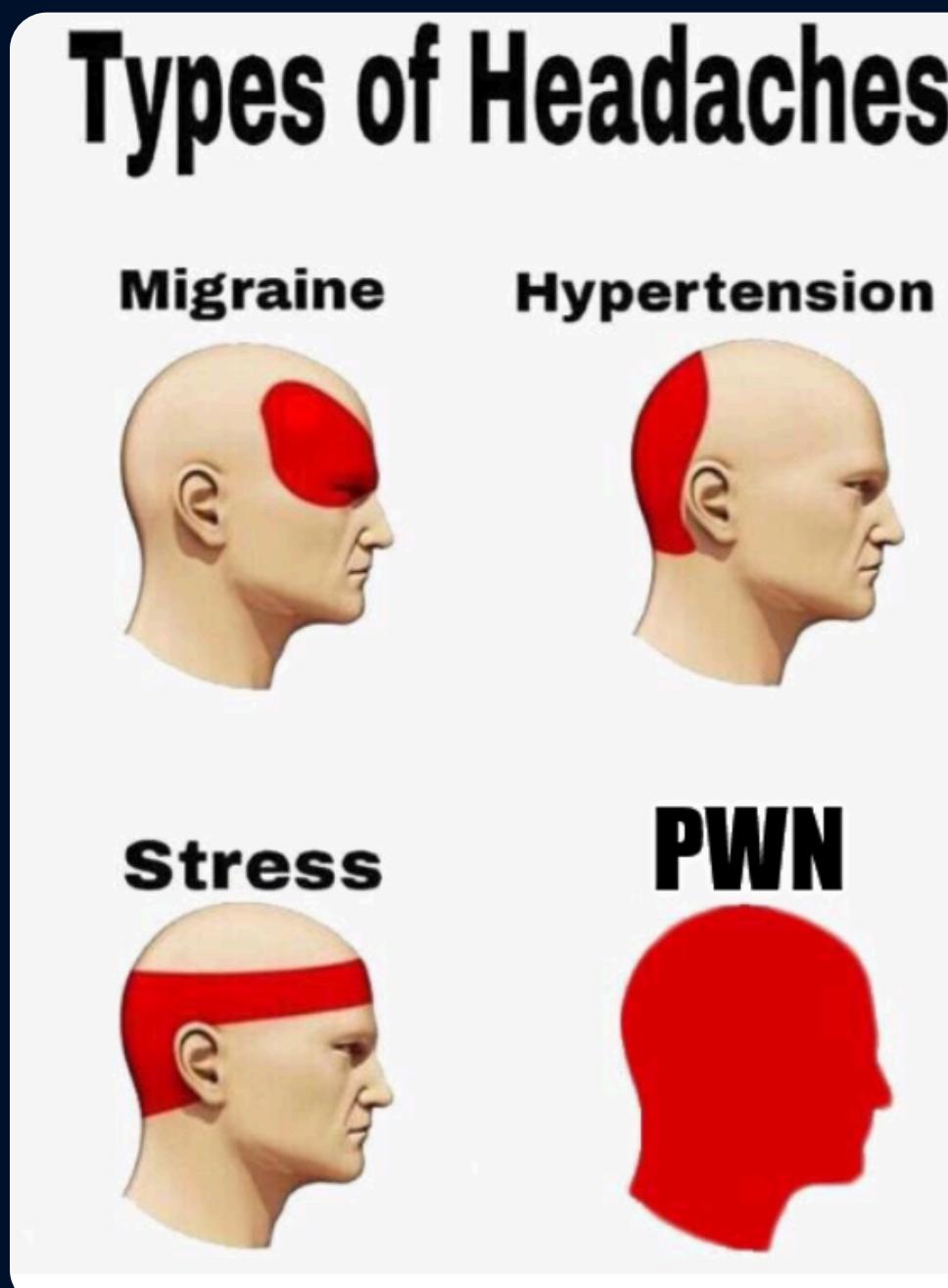
REVERSE

```
00000020 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00000030 00 00 00 00 40 00 38 00 09 00 40 00 1f 00 1c 00  
00000040 06 00 00 00 05 00 00 00 40 00 00 00 00 00 00 00  
00000050 40 00 40 00 00 00 00 00 40 00 40 00 00 00 00 00  
00000060 f8 01 00 00 00 00 00 00 f8 01 00 00 00 00 00 00  
00000070 08 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00  
00000080 38 02 00 00 00 00 00 00 38 02 40 00 00 00 00 00  
00000090 38 02 40 00 00 00 00 00 1c 00 00 00 00 00 00 00  
kh3m@kh3m-machine:~/Research/ELF/tests/baseline/compile_options$  
  
readelf -l ./compile_me.elf | head -n 20  
  
Elf file type is EXEC (Executable file)  
Entry point 0x400430  
There are 9 program headers, starting at offset 64  
  
Program Headers:  
Type Offset FileSiz VirtAddr MemSiz PhysAddr Flags Align  
PHDR 0x0000000000000040 0x0000000000400040 0x0000000000400040 R E 8  
INTERP 0x0000000000000001f8 0x0000000000000001f8 0x0000000000000001f8 0x0000000000000001f8 0x0000000000000001f8 0x0000000000000001f8 0x0000000000000001f8 0x0000000000000001f8  
0x0000000000000000238 0x0000000000400238 0x0000000000400238 0x0000000000400238 0x0000000000400238 0x0000000000400238 0x0000000000400238 0x0000000000400238
```



## 4.Tour du monde des catégories en CTF

PWN



REGISTERS

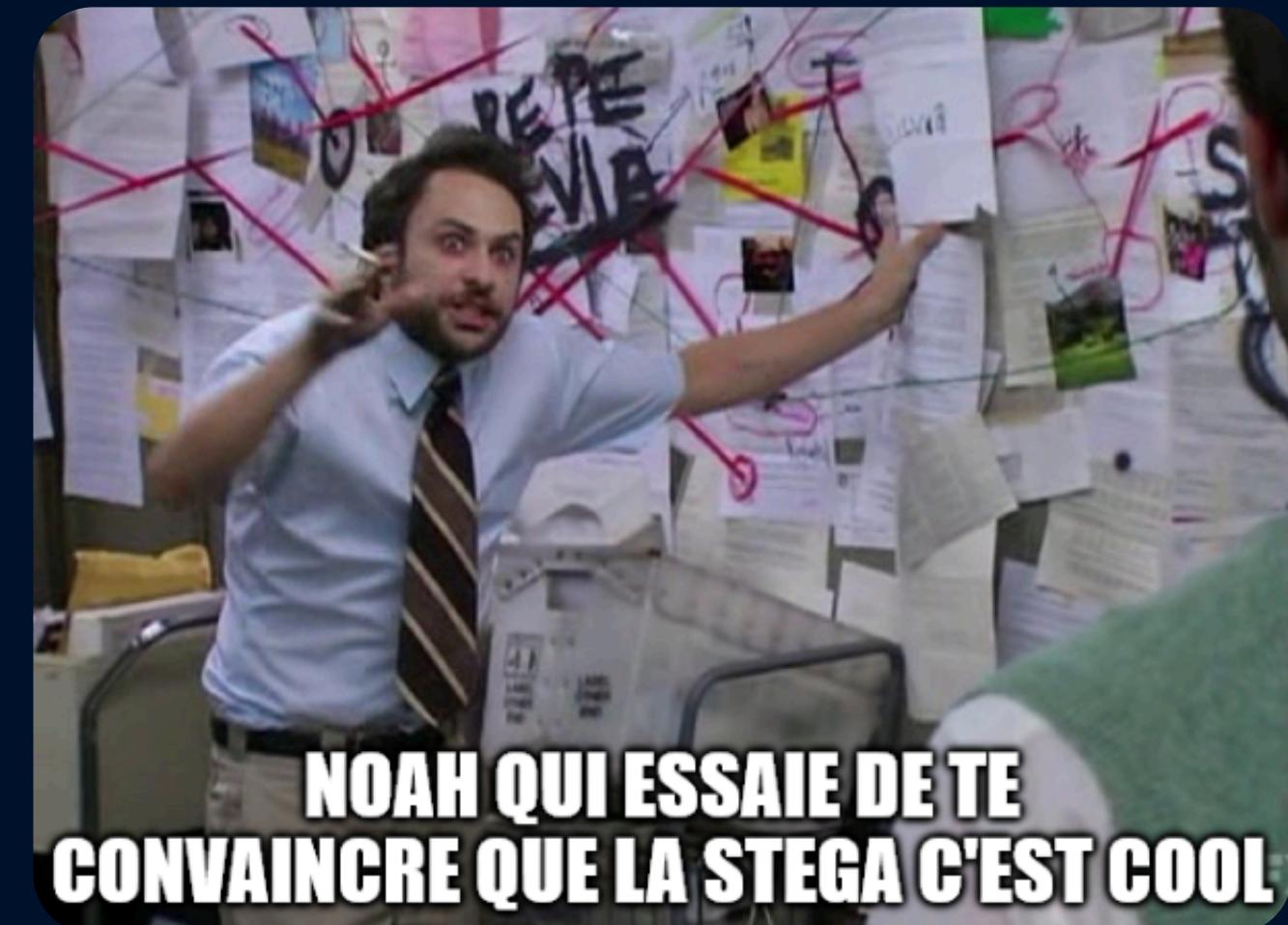
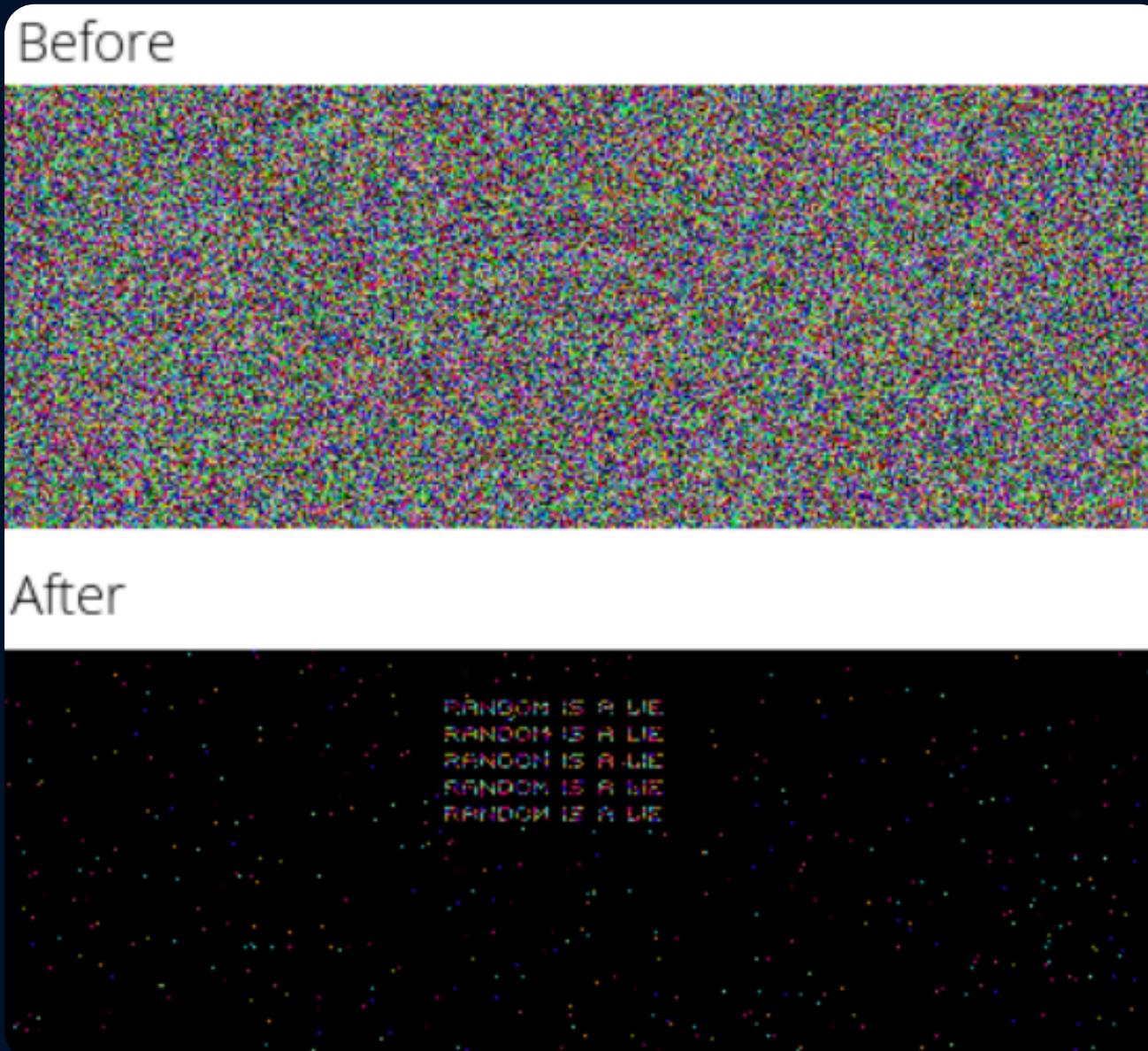
RAX	0x0
RBX	0xfffff7ff5000 ← mov ecx, 0x1000
RCX	0xfffff7b0e737 (mprotect+7) ← cmp rax, -0xffff
*RDX	0x109b00000000
RDI	0xfffff7ff5000 ← mov ecx, 0x1000
RSI	0x1000
R8	0xfffffffffffffff
R9	0x0
R10	0x487
R11	0x202
*R12	0x109bc31d6ab4
R13	0xfffffffffdc50 ← 0x1
R14	0x0
R15	0x0
RBП	0xfffffffffdb60 → 0xfffffffffdb70 → 0x555555554b60 (__libc_csu_init) ← push r15
RSP	0xfffffffffdb40 ← 0x0
RIP	0x555555554b16 (do_test+86) ← call rbx

[ DISASM ]

► 0x555555554b16 <do_test+86>	call rbx
0x555555554b18 <do_test+88>	rdtsc
0x555555554b1a <do_test+90>	mov edi, 1
0x555555554b1f <do_test+95>	shl rdx, 0x20
0x555555554b23 <do_test+99>	lea rsi, [rbp - 0x18]
0x555555554b27 <do_test+103>	or rdx, rax
0x555555554b2a <do_test+106>	sub rdx, r12
0x555555554b2d <do_test+109>	mov qword ptr [rbp - 0x18], rdx
0x555555554b31 <do_test+113>	mov edx, 8
0x555555554b36 <do_test+118>	call write@plt
0x555555554b3b <do_test+123>	cmp rax, 8
	<0x5555555547b0>

## 4.Tour du monde des catégories en CTF

### STÉGANOGRAPHIE



# 4.Tour du monde des catégories en CTF

# PROGRAMMATION



# CHAT MARCHE PAS

```
// the text runs across the top <p> the  
// persisted properties <html><p style="font-weight:bold;">  
<html><body style="background-color:#0000ff; color:white; font-size:12px;">  
<html>text - :200px;> <todoistic> data </todoistic> <br>  
// Non - text - :200px;>persisted properties<br>  
<html><errorMessage = ko , observable><br>  
<p style="color:orange;">HTML font code is <br>  
function todoitem(data) : <br><html><br>  
var self = this <html><br>  
data = data || <html><br>
```

## 4.Tour du monde des catégories en CTF

MISC



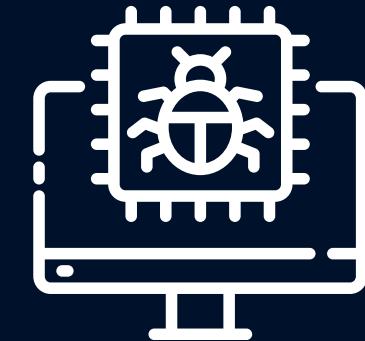
## 4.Tour du monde des catégories en CTF

RÉALISTE

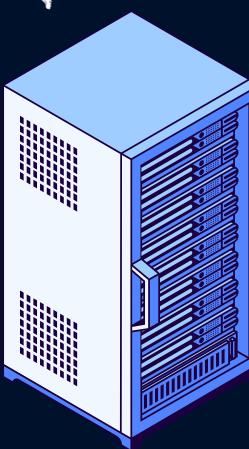


FAILLE

EXPLOITATION



ESCALADE DE PRIVILÈGE



SERVEUR



# CHAPTER 5 :

# RICARD



# ON VA AU BAR !

