

# Introduction à la cybersécurité

```
kali-user@kali:~$ msfconsole

.

      dBBBBbb  dBBP dBBBBBBP dBBBBbb  .
      'dB'
dB'dB'dB' dBBP  dBP  dBP  BB
dB'dB'dB' dBP  dBP  dBP  BB
dB'dB'dB' dBBBBP  dBP  dBBBBBBB

      dBBBBP  dBBBBbb  dBP  dBBBBP  dBP  dBBBBBBP
      dB' dBP  dB' .BP
      dBP  dBBBB' dBP  dB' .BP  dBP  dBP
      dBP  dBP  dBP  dB' .BP  dBP  dBP
      dBBBBP  dBP  dBBBBP  dBBBBP  dBP  dBP
```



Ce trimestre nous allons voir les différents aspects de l'informatique qui sont utiles dans la cybersécurité, et nous exercer avec des activités pratiques fun et du rp

# Sommaire

- **I) Compétences fondamentales**
  - a) GNU-linux (VM, fonctionnement, perms, commandes de base)
  - b) programmation (python on va pas trop loin non plus)
  - c) réseaux (protocole TCP-IP, routage, quelques protocoles)
  - d) le web (php+sql oui c de la programmation oh c bien tu est plus intelligent que tt le monde rassis toi)
  - e) Cryptographie (pas grand chose juste les hash et le chiffrement asymétrique de loin)

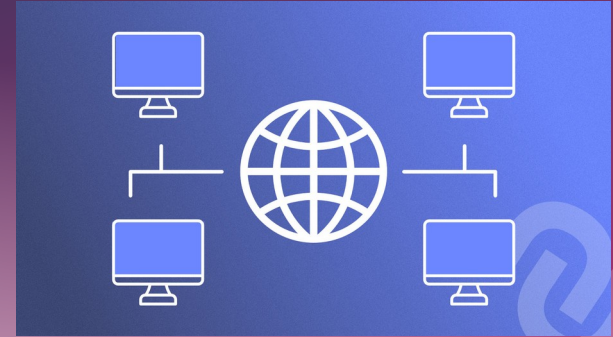
# Sommaire

- **II) Bases de la cybersécurité**
  - a) Définitions
  - b) Cadre legal
  - c) Installation de linux en VM+création de compte replit

# Sommaire

- III) Travaux pratiques
  - a)exo-bash
  - b)exo-injection
  - c)exo-hash
  - d)Presentation de root-me, hackthebox et vulnhub
  - e)alors on fait quoi ?

# Compétences fondamentales



# GNU-Linux

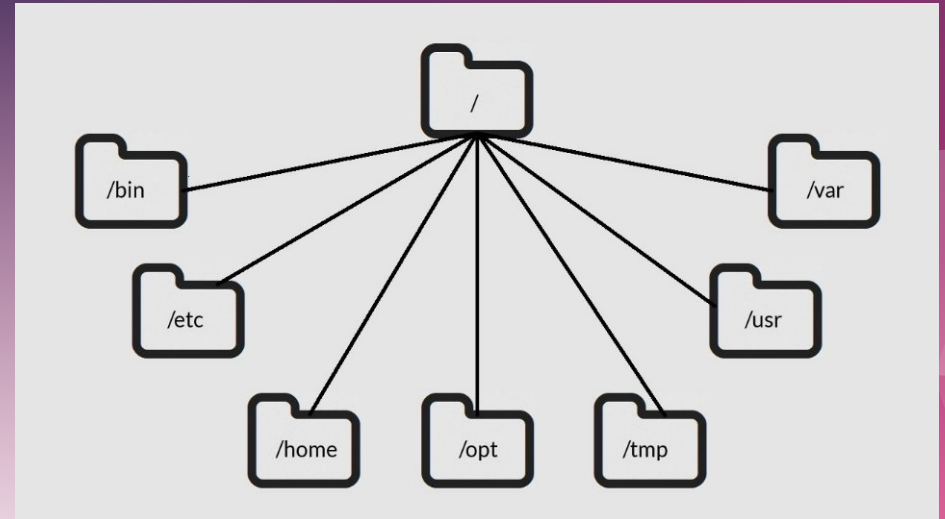
- Créé en 1991 par ce mec:
  - Plusieurs distros
  - Basé \*("oui mais..." on a pas le tps !) sur unix, open source \*
  - Ubuntu, Arch, Redhat (+Fedora)
- 
- C'est quoi un OS ?
  - Pourquoi on va utiliser linux ?
  - Vous aurez tous mangé du linux d'ici à 2 semaines
  - Linux ne se mange pas





# L'organisation des fichiers sur Linux

- Sur windows : C/
- Sur linux :
- Bin;etc;home;opt;tmp;usr;var
- Comment on fait pour accéder à tout ça ?



# Les commande de base

- ls
- Cd
- Mkdir
- Cat
- Nano
- Apt
- Touch
- Pwd
- Man
- cp

- Chmod ?
- Sudo ? Su?
- Ifconfig ?
- Traceroute ?





# ls

- `ls` liste les fichiers et les dossiers du repertoire dans lequel vous vous trouvez
- Elle s'utilise de cette manière :
- `$ls` pour lister les fichier
- `$ls -l` pour lister les fichiers, fichiers cachés et permissions

# CD

- La commande `$cd` sert à changer de repertoire
- Elle s'utilise de cette manière :
  - “`$cd nom_du_repertoire`” pour se rendre dans un repertoire
  - “`$cd ..`” pour revenir en arrière

# mkdir

- Crée un dossier
- “\$mkdir nom\_du\_dossier”

# cat

- Affiche le contenu d'un fichier



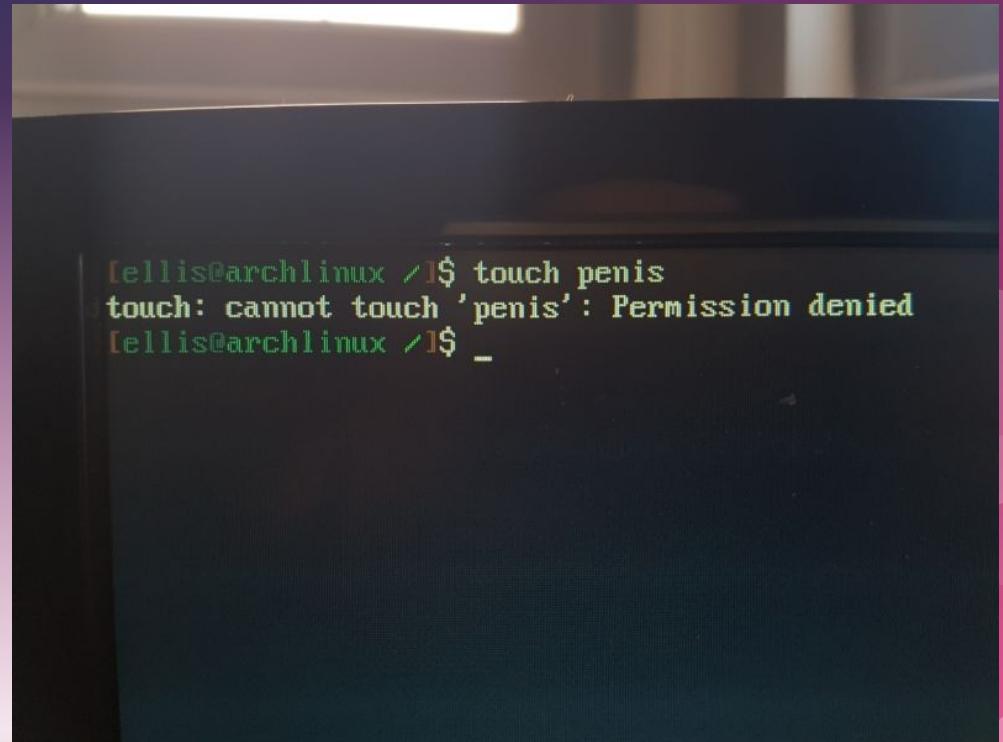
- “\$cat nom\_du\_fichier”

# Nano

- Editeur de texte de base
  - Il faut peut-être l'installer `$sudo apt install nano`
  - Il y a aussi vim (:q 'enter' pour quitter)
- 
- `$nano nom_du_fichier`

# Touch

- Pour créer un fichier
- “\$touch nom\_du\_fichier”

A photograph of a computer terminal window. The terminal has a dark background with green and white text. The prompt is '[ellis@archlinux ~]\$'. The user has entered the command 'touch penis'. The terminal output is 'touch: cannot touch \'penis\': Permission denied'. The prompt is now '[ellis@archlinux ~]\$ \_' with a cursor.

```
[ellis@archlinux ~]$ touch penis  
touch: cannot touch 'penis': Permission denied  
[ellis@archlinux ~]$ _
```



# pwd

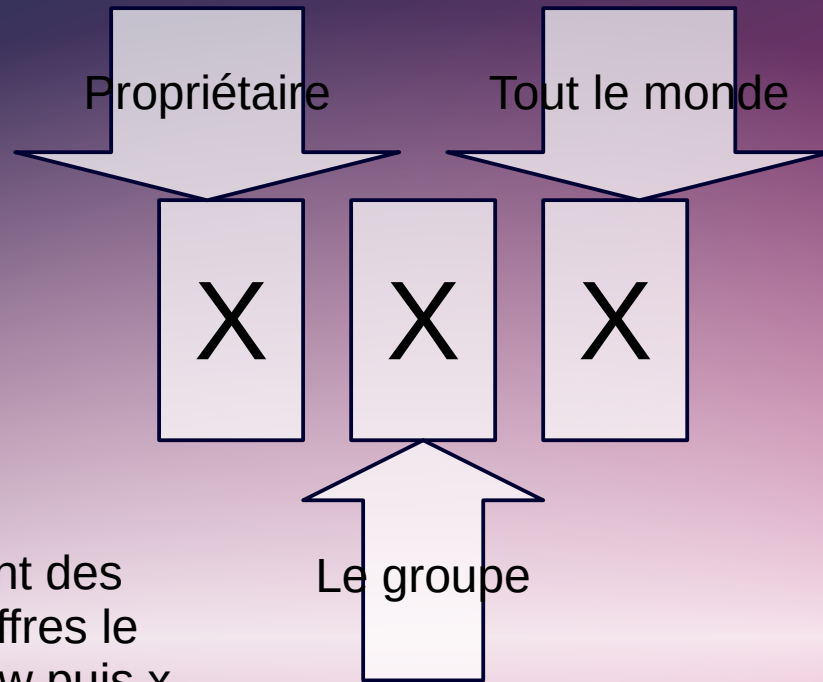
- Affiche le repertoire actuel
- “\$pwd” (je sais c dur)

# cp

- Copie des trucs
- “\$cp nom\_du\_fichier /chemin/de-la/destination/”
- “\$cp -r nom\_du\_repertoire /chemin/de-la/destination/” pour un repertoire

# Les Permissions

Les permissions existent en : lecture (r), écriture (w), execution (x)



Les permissions peuvent se représenter sous la forme de 3 entiers de 0 à 7

Les chiffres représentent des valeurs binaires à 3 chiffres le premier pour r, ensuite w puis x.  
Exemple :  $6=4+2+0=110=rw-$  lire et écrire

# Les permissions (suite)

- Avec `ls -l`, on affiche les permissions comme ceci :

```
drwxr-xr-x  6 roza lycee  4096 2019-10-29 23:09 Bureau
drwxr-x---  2 roza lycee  4096 2019-10-22 22:46 Documents
lrwxrwxrwx  1 roza lycee    26 2019-09-22 22:30 Examples -> /usr/share/ex
-rw-r--r--  1 roza lycee 1544881 2019-10-18 15:37 forum.xcf
drwxr-xr-x  7 roza lycee  4096 2019-09-23 18:16 Images
```

Ici les permissions  
pour Images/  
peuvent s'écrire 755

- La commande `chmod` permet d'assigner des permission à un fichier :
- `$chmod XXX nom_du_fichier`
- `Chown` pour changer de proprio:
- `$chown utilisateur fichier`

# Les utilisateurs sur linux

- Le root
  - Les sudoers
  - Les **autres**
- 
- Comment on change ?
  - Ils peuvent faire quooiii ?
  - Pourquoi on peut pas manger du linux ?



# Root

- C'est le dieu, l'admin de l'admin, littéralement le
- super-utilisateur
- Son dossier est /root et il peut écrire partout depuis la racine /



```
vladi@vladi-laptop:/$ ls
bin boot cdrom control- dev etc home initrd initrd.img lib lost-found media mnt opt prefs.js proc root
sbin srv sys tmp tools usr var vmlinuz
vladi@vladi-laptop:/$ uname -a
Linux vladi-laptop 2.6.24-24-generic #1 SMP Sat Aug 22 01:06:14 UTC 2009 i686 GNU/Linux
vladi@vladi-laptop:/$ apt-get moo

  ____
 /  ____ \
/_____/

... "Have you mooed today?"
vladi@vladi-laptop:/$ python
Python 2.5.2 (r232:60911) on linux2
[GCC 4.2.4 (Ubuntu 4.2.4-14ubuntu2)]
Type "help", "copyright", "credits()" or "quit()"
>>> exit()
vladi@vladi-laptop:/$ perl

vladi@vladi-laptop:/$ sysinfo &
[1] 12438
vladi@vladi-laptop:/$ sudo su
[sudo] password for vladi:
root@vladi-laptop:/$ ls
bin boot cdrom control- dev etc home initrd initrd.img lib lost-found media mnt opt prefs.js proc root
sbin srv sys tmp tools usr var vmlinuz
root@vladi-laptop:/$ pwd
/
root@vladi-laptop:/$ whoami
root
root@vladi-laptop:/$
```

#root


Vladimir Kolev



# Les autres

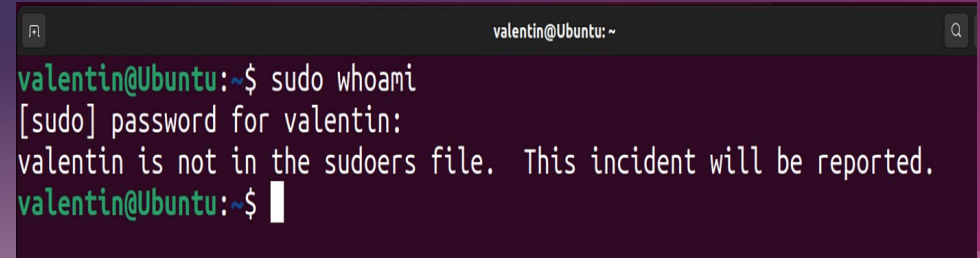
- Ils ont rien de special
- Leur dossier est dans /home

```
vivek@wks01:/tmp$ find . -iname "data*.txt"
./rtzip/data005.txt
./rtzip/data001.txt
./rtzip/data004.txt
./rtzip/data003.txt
./rtzip/data002.txt
./rtzip/data008.txt
./rtzip/data006.txt
./rtzip/data007.txt
./rtzip/data009.txt
find: `./vmware-root': Permission denied
find: `./orbit-Debian-gdm': Permission denied
```



# Les sudoers

- Ils peuvent utiliser la commande sudo pour se faire passer pour le root quand il faut
- Leurs dossier est aussi dans /home

A terminal window titled 'valentin@Ubuntu: ~' with a search icon in the top right. The prompt is 'valentin@Ubuntu:~\$'. The user enters 'sudo whoami'. The prompt changes to '[sudo] password for valentin:'. The user presses enter, and the terminal displays the message 'valentin is not in the sudoers file. This incident will be reported.' followed by the prompt 'valentin@Ubuntu:~\$' and a cursor.

```
valentin@Ubuntu:~$ sudo whoami
[sudo] password for valentin:
valentin is not in the sudoers file. This incident will be reported.
valentin@Ubuntu:~$
```

Rip valentin

# La commande sudo et su

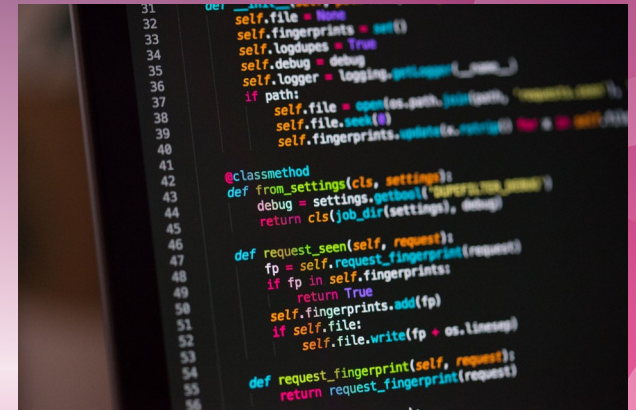
- “\$sudo commande” pour effectuer une action en tant que root

```
debian@linux:~$ su - malekalmorte  
Password:  
malekalmorte@r[REDACTED]:~$
```



# Programmation

- Python: interprété
  - 1991
- 
- C vachement pratique



# Alors comment on fait ?

- Et bah on cherche sur google mon reuf, ググれカス

- <https://www.youtube.com/watch?v=kqtD5dpn9C8>
- [http://jerome.courtois2.free.fr/NSI\\_premiere/NSI\\_premierePDF/NSI\\_Python\\_partie\\_1\\_Variables\\_et\\_affectations.pdf](http://jerome.courtois2.free.fr/NSI_premiere/NSI_premierePDF/NSI_Python_partie_1_Variables_et_affectations.pdf)

# Les réseaux

Oh tien courtois a un cours  
la dessus

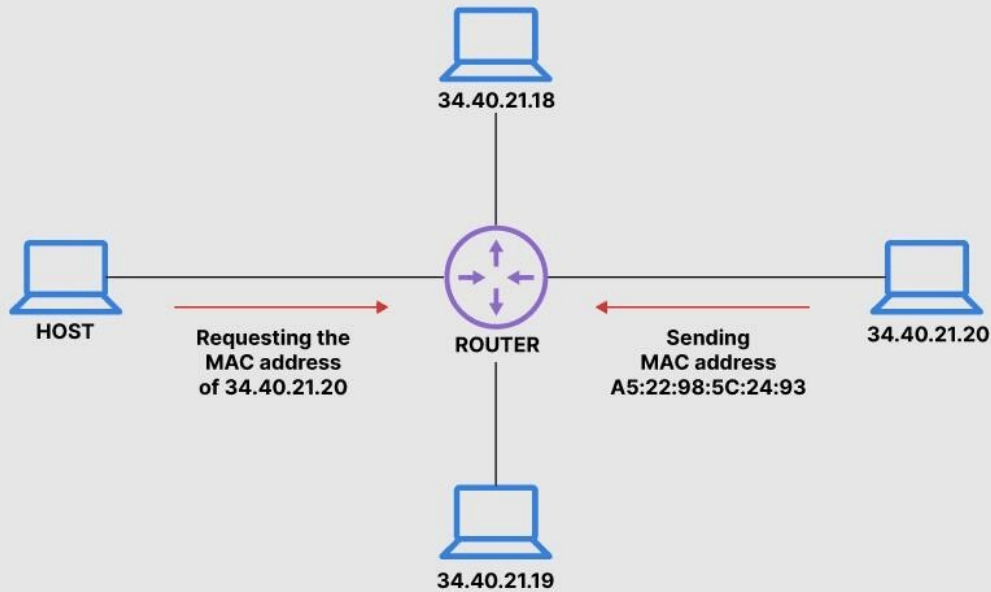
- trkl on va faire vite

- [http://jerome.courtois2.free.fr/NSI\\_teminale/NSI-ProtocoleTCPIP.pdf](http://jerome.courtois2.free.fr/NSI_teminale/NSI-ProtocoleTCPIP.pdf)



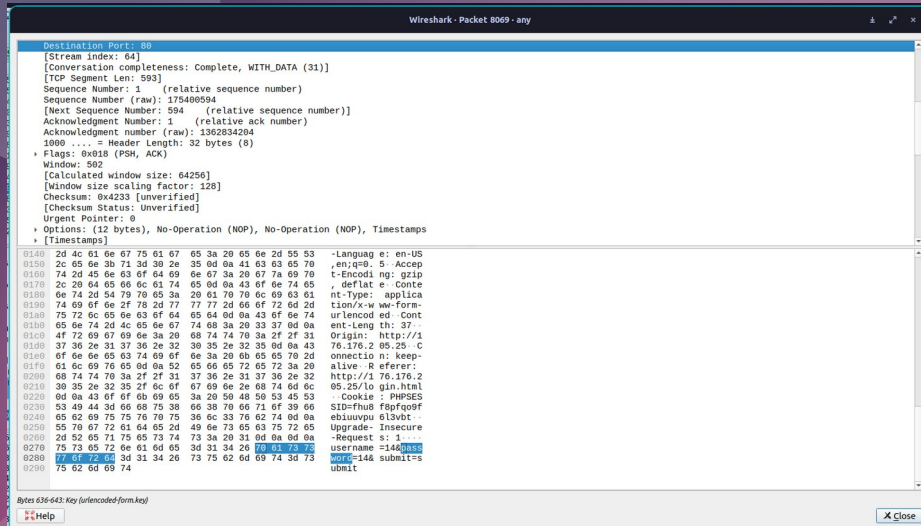
# Le protocole arp

## How Address Resolution Protocol (ARP) Works



# Ethernet Frame

ip.dst==176.176.205.25						
No.	Time	Source	Destination	Protocol	Length	Info
7640	186.817380539	192.168.1.73	176.176.205.25	TCP	68	56304 → 80 [ACK] Seq=755 Ack=171291 Win=247680 Len=0 TSval=3172904382 TSecr=1874189615
7642	186.817665526	192.168.1.73	176.176.205.25	TCP	68	56304 → 80 [ACK] Seq=755 Ack=194459 Win=294016 Len=0 TSval=3172904382 TSecr=1874189616
7644	186.817821470	192.168.1.73	176.176.205.25	TCP	68	56304 → 80 [ACK] Seq=755 Ack=211835 Win=328704 Len=0 TSval=3172904382 TSecr=1874189616
7646	186.817851016	192.168.1.73	176.176.205.25	TCP	68	56304 → 80 [ACK] Seq=755 Ack=214675 Win=334464 Len=0 TSval=3172904382 TSecr=1874189616
7647	186.858941348	192.168.1.73	176.176.205.25	TCP	68	56300 → 80 [ACK] Seq=741 Ack=2750 Win=64128 Len=0 TSval=3172904424 TSecr=1874189609
7686	191.816465973	192.168.1.73	176.176.205.25	TCP	68	56300 → 80 [FIN, ACK] Seq=741 Ack=2751 Win=64128 Len=0 TSval=3172909381 TSecr=1874194615
7689	191.818726867	192.168.1.73	176.176.205.25	TCP	68	56306 → 80 [FIN, ACK] Seq=358 Ack=30078 Win=81664 Len=0 TSval=3172909383 TSecr=1874194617
7692	191.821228165	192.168.1.73	176.176.205.25	TCP	68	56304 → 80 [FIN, ACK] Seq=755 Ack=214676 Win=334464 Len=0 TSval=3172909386 TSecr=1874194620
8066	224.383863960	192.168.1.73	176.176.205.25	TCP	76	55230 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3172941948 TSecr=0 WS=128
8068	224.385101423	192.168.1.73	176.176.205.25	TCP	68	55230 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3172941950 TSecr=1874227184
8069	224.385190982	192.168.1.73	176.176.205.25	HTTP	661	POST /register-sign-in.php HTTP/1.1 (application/x-www-form-urlencoded)
8081	226.309821896	192.168.1.73	176.176.205.25	TCP	68	55230 → 80 [ACK] Seq=594 Ack=408 Win=64128 Len=0 TSval=3172943874 TSecr=1874229108
8082	226.311506373	192.168.1.73	176.176.205.25	HTTP	512	GET /index.php HTTP/1.1
8085	226.315732543	192.168.1.73	176.176.205.25	TCP	68	55230 → 80 [ACK] Seq=1038 Ack=2306 Win=64128 Len=0 TSval=3172943880 TSecr=1874229114
8130	231.322434243	192.168.1.73	176.176.205.25	TCP	68	55230 → 80 [FIN, ACK] Seq=1038 Ack=2307 Win=64128 Len=0 TSval=3172948887 TSecr=1874234120



Cookie : PHPSES  
SID=fhu8 f8pfqo9f  
ebuiuuvpu 6l3vbt  
Upgrade-Insecure  
-Request s: 1...  
username =14&pass  
word=14& submit=s  
ubmit

# Le web

- Le php c un language qui s'execute côté serveur quand on charge la page web, facebook était fait en php

- [http://jerome.courtois2.free.fr/NSI\\_teminale/NSI\\_SQL.pdf](http://jerome.courtois2.free.fr/NSI_teminale/NSI_SQL.pdf)
- Le SQL c'est un language pour les bases de données

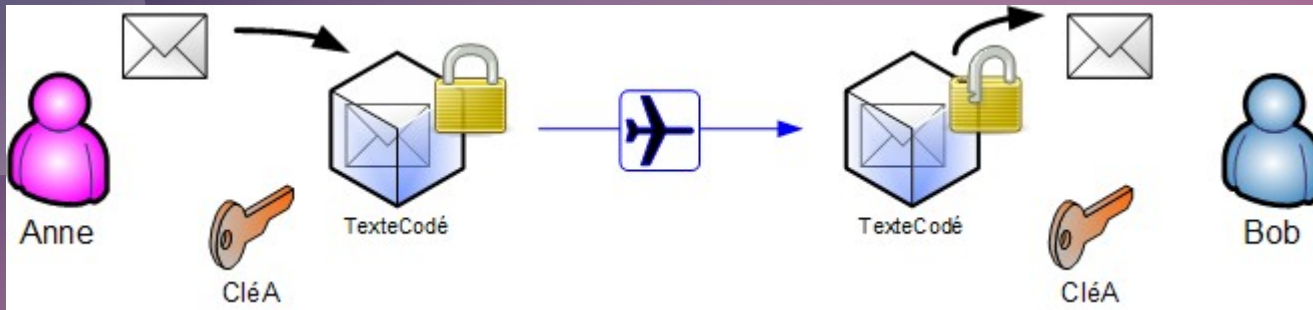
# Cryptographie

- Chiffrement
- Chiffrement asymetrique
- Hash



# Chiffrement symétrique

- Bon le chiffrement César tout le monde connaît mais il y en a d'autres, le AES notamment



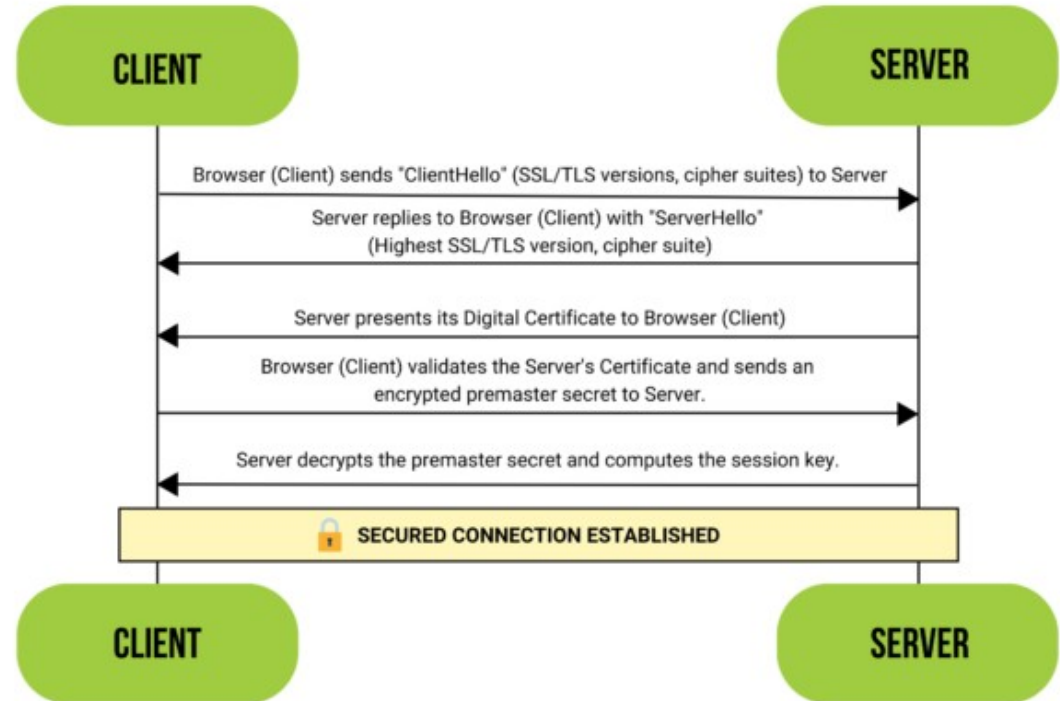
# Chiffrement asymétrique





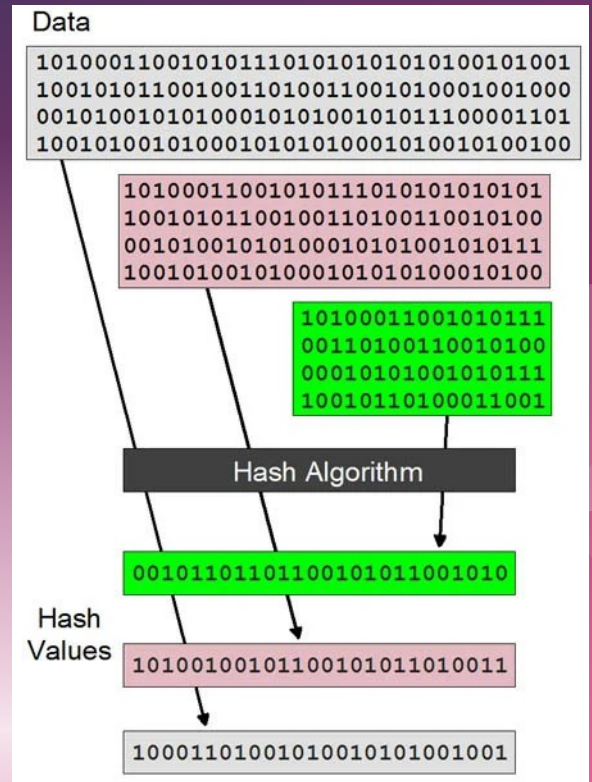
Aussi

# SSL/TLS HANDSHAKE



# Hash

- A hashing algorithm is a mathematical function that garbles data and makes it unreadable. Hashing algorithms are one-way programs, so the text can't be unscrambled and decoded by anyone else.
- Sha256
- MD5



## II) Bases de la cybersécurité



- Couleurs de chapeau
- Legal ou pas
- C quoi une VM
- Installation de linux en VM
- replit

# Couleurs de chapeau





# Cadre Legal

- En France, le cadre juridique relatif au piratage informatique est principalement défini par la loi de 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que par le Code pénal.



- Le Code pénal français réprime différentes infractions liées au piratage informatique. Parmi les principales infractions figurent l'accès frauduleux à un système informatique, l'atteinte aux données, le vol ou la destruction de données, la diffusion de programmes malveillants, le phishing...
- Maître Samuel ZUBAROGLU

# Machine virtuelle



- une machine virtuelle ou VM est un environnement entièrement virtualisé qui fonctionne sur une machine physique. Elle exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipement qu'une machine physique : CPU, mémoire RAM, disque dur et carte réseau.





# Installation de linux sur une VM

- <https://www.youtube.com/watch?v=l0JgWilK6ok>



- [Www.kali.org](http://www.kali.org)
- Download installer iso
- Install virtualbox
- Create new VM
- Configure stuff
- Launch the vm

# Creer un compte replit

- <https://replit.com>

Voilà voilà

# III)Travaux pratique



- lulucienfirst sur replit
- 1)exo-bash
- 2)exo-injection
- 3)exo-hash
- 4)sumo 1
- 5)Windows rat avec msf
- 6)projet: MITM credential harvesting

# Sumo 1 ?

- Identify the problem
- Gather information
- Analyze clues
- Test and iterate
- Importance of communication and teamwork

- <https://sevenlayers.com/index.php/340-vulnhub-sumo-1-walkthrough>

- On y va avec un tuto flm d'y passer des heures

# Windows rat (Remote Access Trojan)

- Using msfconsole/msfvenom
- Sending through discord



# MITM credential harvesting

- 1)web-server
- 2)redirect traffic
- 3)faux login google ou fausse page de MAJ
- 4)Faire un virus qui recupère les logins et les envois à un server
- Python, socket et pycompile



# Sources

- <https://snyk.io/series/ctf/strategies-techniques/>
- <http://jerome.courtois2.free.fr/>
- Google image (film de détailler)
- Alexia.fr
- Eau de source