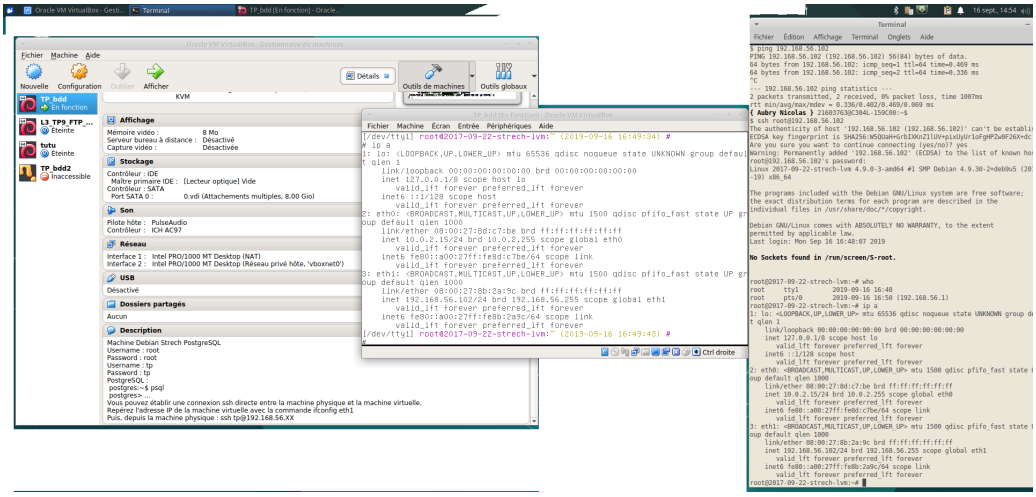
UNIVERSITÉ CAEN NORMANDIE

TP-Environnement

08.01.2023

Ils découvrirent un nouveau monde ☺

Auteur : Pascal Fougeray



Source : Moi ☺

1 Préambule

— Nous allons voir plein plein plein de choses qui pour certaines vont vous paraître brumeuses, mais ne vous inquiétez pas, la brume va se disperser au fil des autres TP. Vous verrez qu'à la fin de ce module ce TP vous paraîtra naturel.
— Vous pouvez travailler en binôme, cela ne me dérange pas au contraire. Par contre chacun prend ses notes !
— Vous pouvez prendre un pause quand vous voulez (On ne me demande pas d'aller au WC ☺)
— Si vous avez un message ultra urgent mais vraiment ultra urgent sur votre smartphone, vous sortez de la salle et vous le lisez. C'est vous qui gérez votre temps. Si je vous vois sur votre smartphone, je ne vous dirais rien, mais il ne faut pas m'appeler pour vous aider ! ! !
— Vous travaillez à votre rythme !
— N'hésitez pas à poser des questions, je suis là pour vous répondre et d'autres ont les mêmes...
— Vous pouvez travailler avec votre propre PC, mais qu'après ce premier TP.
— Certains TP pourront être fait chez vous si vous voulez. Par contre je fais l'appel à chaque TP. À vous de me prouver que vous avez fait le TP
— Vous travaillez pour vous, pas pour moi ☺
— **Prenez des notes sur ce que vous comprenez, ces notes vous y aurez le droit de les avoir avec vous au CT !**

2 Introduction

Dans ce premier TP, je vous propose de **découvrir l'environnement** dans lequel les 9 autres TP auront lieu.

Nous allons voir

— La salle S3-406 qui est un peu différente des autres
— Le HOST (Le PC sur lequel vous vous loguez avec votre compte étudiant)
— Penser au câble de la seconde interface réseau !
— Installer la VM, la lancer, la configurer et la gérer sur son compte de la Fac
— Voir rapidement le logiciel de capture Wireshark
— Voir rapidement le logiciel de simulation GNS3
— Faire un peu de réseau en découvrant de nouvelles commandes telles **ip a, ifconfig**
— etc...

3 La salle S3-406

Cette salle est une salle ou vous avez la possibilité de bénéficier d'une seconde interface réseau, je crois qu'elle s'appelle **bro** ☺

1. **Loguez** vous, **lancez** un terminal et **lancez** la commande **ip a**
2. Combien d'interfaces physiques possède le PC de la FAC ?
3. **Visualisez** la liste des interfaces : ***ip a*** et **expliquez** ce que vous trouvez !

```
                    fougeray@C304L-159C00:~$
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 8c:ec:4b:a8:54:57 brd ff:ff:ff:ff:ff:ff
    inet 10.38.19.111/22 brd 10.38.19.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8eec:4bff:fea8:5457/64 scope link
       valid_lft forever preferred_lft forever
3: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 96:12:5a:71:91:bd brd ff:ff:ff:ff:ff:ff
    inet6 fe80::906e:50ff:fef4:e61b/64 scope link
       valid_lft forever preferred_lft forever
4: tap0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master br0 state UNKNOWN group default qlen 100
    link/ether 96:12:5a:71:91:bd brd ff:ff:ff:ff:ff:ff
    inet6 fe80::9412:5aff:fe71:91bd/64 scope link
       valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:21:84:07:81 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
6: vboxnet0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 0a:00:27:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.1/24 brd 192.168.56.255 scope global vboxnet0
       valid_lft forever preferred_lft forever
    inet6 fe80::800:27ff:fe00:0/64 scope link
       valid_lft forever preferred_lft forever
                    fougeray@C304L-159C00:~$
$
```

   (a) Combien d'interfaces ?
   (b) Bizarre le PC en a que 2, c'est quoi ce trafic ? ...
   (c) Qu'est-ce que l'interface de **Loopback lo** ?
   (d) Rôle de chacune d'elles ? (On verra plus tard ?)
   (e) Pourquoi certaines ont des @IP et pas d'autres ?
   (f) Qu'est-ce que le réseau 172.17.0.0/24
   (g) **Qu'est-ce que le réseau 192.168.56.0/24**
   (h) Qu'est-ce que l'interface ***vboxnet0*** ?
   (i) Qu'est-ce que l'interface ***br0*** ?
   (j) Qu'est-ce que l'interface ***tap0*** ?
   (k) pourquoi l'interface ***tap0*** n'a pas d'@IP ?

   Quelle est l'adresse IP des différentes interfaces ?

4. **Visualisez** la table de routage : ***ip route ls*** et **expliquez** ce que vous comprenez !

```
$ ip route ls
default via 10.38.16.1 dev eth0
10.38.16.0/22 dev eth0 proto kernel scope link src 10.38.19.111
169.254.0.0/16 dev eth0 scope link metric 1000
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
192.168.56.0/24 dev vboxnet0 proto kernel scope link src 192.168.56.1 linkdown
                    fougeray@C304L-159C00:~$
$
```

(a) A quoi correspond la ligne commençant par ***default*** ?

(b) Pourquoi cette ligne existe t'elle ?

(c) L'interface ***eth0*** semble être sur 2 réseaux 10.38.16.0/22 et 169.254.0.0/16
Je comprends le 10.38.16.0/22 par contre je n'ai pas compris le second et vous ? C'est quoi la ***metric*** ?

(d) Pourquoi toutes ces routes ?

(e) Pourquoi les 2 interfaces ***docker0*** et ***vboxnet0*** sont-elles indiquées linkdown ?

Qu'est-ce que l'on comprend ?

Allez je vous explique au tableau, nous verrons cela plus en détails dans un prochain cours

5. Comment accède-ton à Internet ?
6. **Allez,** on câble cette interface pour avoir accès à Internet dans la VM.
   Remarque : Il faudra penser à le faire à chaque TP et surtout décâbler à la fin de chaque TP !
7. Quelle est l'adresse IP des différentes interfaces ?
8. **Visualisez** la table de routage : ***ip route ls*** et **expliquez** ce que vous comprenez !
   Qu'est-ce que l'on comprend ?
   Par rapport à la question précédente !

On verra ce qu'est le routage dans le TP suivant et dans d'autres TP ! Patience ☺

Le routage c'est savoir comment aller d'un point A à un point B et par où passer, aussi bien à l'aller qu'au retour ?

4 Dans la VM

IL Y A UN GROS BUG : XANDR ! ! ! <– Note pour le prof et qu'il faut supprimer au départ ! ! !

Pourquoi cette VM ?

Parce que pour faire de l'administration système et de l'administration réseau il faut pouvoir être administrateur d'une machine. On appelle cela **root** sous linux.

Attention pour cette partie vous n'êtes pas ***root*** donc on ne fait que d'analyser !

Cette VM tourne dans **l'hyperviseur** de type 2, Virtualbox.

Pour créer la VM, c'est simple. Pour la supprimer aussi. Du moins avec le script de la Fac. Chez vous ce sera un peu plus long, mais pas beaucoup plus

1. **Lancez** la commande ***virtualbox-createtp -l***
2. **Relevez** le nom de celle qui contient GNS3
3. **Lancez** la commande ***virtualbox-createtp -c UnNomQuiVousPlait LeNomRelevé***
   Normalement si tout se passe bien dans le meilleur des mondes vous avez une VM dans votre répertoire Document
4. **Vérifiez**
5. **Lancez** VirtualBox
6. **Lancez** la VM à l'aide de VirtualBox
7. **Loguez-vous**
   (a) Login : **etudiant**
   (b) MDP : **Etudiant1**

   Pour être root
   (a) Login : **root**
   (b) MDP : **Root1**

   Notez ces valeurs je ne les redonne pas !
8. **Lancez** firefox et allez sur **ecampus** chercher ce sujet de TP afin de ne plus devoir passer du HOST à la VM
9. **Lancez** un terminal et **lancez** la commande **ip a**

10. Combien d'interfaces physiques possède la VM ?
11. **Visualisez** la liste des interfaces : ***ip a*** et **expliquez** ce que vous trouvez !
    (a) Combien d'interfaces ?
    (b) Bizarre la VM en a que 4 , c'est quoi ce trafic ? ...
    (c) Qu'est-ce que l'interface de **Loopback lo** ?
    (d) Rôle de chacune d'elles ? (On verra plus tard ?)
    (e) Pourquoi certaines ont des @IP et pas d'autres ?
    (f) Qu'est-ce que le réseau 172.17.0.0/24
    (g) **Qu'est-ce que le réseau 192.168.56.0/24**
    (h) Qu'est-ce que l'interface ***vboxnet0*** ?
    (i) Qu'est-ce que l'interface ***tap0*** ?

    On passe root !
    ATTENTION : on est sous une **debian** et non une **ubuntu** donc il n'y a pas de **sudo** (Information pour ceux qui connaissent sudo)
12. **Lancez** la commande ***ifconfig***
    (a) Que se passe-t'il ?
    (b) Pourquoi (**Pensez** au **PATH**)
    (c) Lancez la commande ***echo $PATH***
13. **Lancez** la commande **su** et **loguez** vous en root
14. **Lancez** la commande ***ifconfig***
    (a) Que se passe-t'il ?
    (b) Pourquoi (**Pensez** au PATH)
15. **Lancez** la commande ***exit*** (Vous redevenez simple étudiant ☺
16. **Lancez** la commande **su -** et **loguez** vous en root
17. **Lancez** la commande ***ifconfig***
    (a) Que se passe-t'il ?
    (b) Pourquoi (**Pensez** au PATH)
18. **Concluez sur cette différence entre su et su - ! ! ! ! ! Pensez à variable d'Environnement**

Notez cette différence je ne les redonne pas !

5 Le logiciel Wireshark

Wireshark est un logiciel d'analyse réseau (sniffer) qui permettant de visualiser l'ensemble des trames, des paquets, des segments et des données qui transitent sur les réseaux et d'obtenir des informations sur les protocoles applicatifs utilisés.

Les octets sont capturés en utilisant la librairie réseau **PCAP**, puis regroupés en blocs d'informations et analysés par le logiciel.

Avant on utilisait le logiciel **tcpdump** qui est toujours d'actualité et développé
https://www.tcpdump.org/
Mais c'était avant ☺

Ce logiciel permet :

1. **d'écouter** une interface
2. de **capturer** les

Plus d'informations ici : https://www.wireshark.org/download.html

Un très bon tuto :

Vous ne pouvez pas l'utiliser sur les PC de la FAC ! ! !

Mais dans la VM oui et chez vous aussi.

Il fonctionne aussi bien sous Linux que sous Windows et MacOSx !

Il va nous servir pour comprendre plus facilement les mécanismes des réseaux ! ! !

Alors, on l'apprend, du moins les bases !

1. Sur le bureau, **cliquez** sur l'icône Wireshark
   Le logiciel est lancé...
   On va juste voir les bases là.
2. **Sélectionnez** l'interface ***vboxnet0***
3. Dans un terminal de la VM **lancez** la commande ***ping -c 2 192.168.56.1***
4. Que **voyez** vous dans Wireshark ?
5. On explique ?
6. **Concluez** sur l'utilité de Wireshark
7. Pourquoi un simple étudiant peut lancer wireshark dans la VM ?
   (a) **Lancez** la commande etudiant@debian-11-GNS3 :~$ ***cat /etc/group | grep wireshark***
   Vous devez avoir quelque chose comme : ***wireshark :x :124 :etudiant***
8. Dans le Host, **lancez** la commande wireshark (Pas certain que le logiciel soit installé...)
9. S'il est installé, que se passe t'il ?
10. **Concluez** sur la notion de root et simple utilisateur

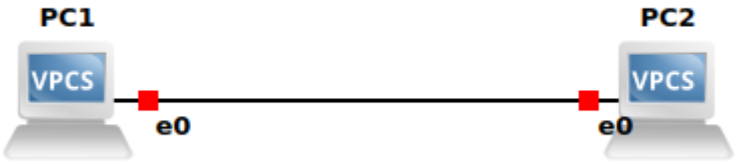
6 Le logiciel GNS3

Pour cette partie, pas grand chose de réseau, juste prendre en main le logiciel et **imaginez** que vous avez le tout nouveau smartphone ☺

Je vous donne des liens Web, n'hésitez pas à cliquer dessus pour lire la doc et comment faire au lieu de m'appeler ☺

Je peux rester à mon bureau avec le vidéo projecteur et faire le TP en même temps que vous...

1. Sur le bureau, **cliquez** sur l'icône GNS3
   Le logiciel est lancé...
   On va juste créer deux petits projets
   La documentation est ici : https://docs.gns3.com/docs/using-gns3/beginners/the-gns3-gui
2. **Créez** un nouveau projet que vous nommez **VPCS**
   (a) **Mettez** 2 VPCS et **Reliez** les par un câble.
   Voir https://docs.gns3.com/docs/emulators/vpcs/



   (b) **Cliquez** sur l'icône flèche verte, cela lance les 2 VM dans la VM... et oui des VM dans des VM !
   (c) **Cliquez** bouton droit sur chaque VPCS et sous menu **console**, cela devrait vous ouvrir un terminal avec un shell très très basique ☺
   (d) **Mettez** une adresse IP sur chaque VPCS par exemple 192.168.16.**1**/24 et 192.168.16.**2**/24

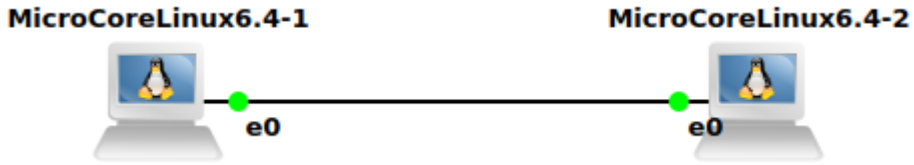
```
PC1> ip 192.168.16.1/24
Checking for duplicate address...
PC1 : 192.168.16.1 255.255.255.0

PC1> save
Saving startup configuration to startup.vpc
.  done
```

(e) Puis toujours **save** ! ! !

(f) **Mettez** une sonde Wireshark sur le câble entre PC1et PC2.
Pour cela clique droit sur le câble, **start capture,** wireshark doit se lancer automatiquement.
Rien ne doit se passer dans wireshark puisque les 2

3. **Créez** un nouveau projet que vous nommez **MicroCoreLinux**
Micro Core Linux est une variante plus petite de Tiny Core sans bureau graphique. Il s'agit d'un système Linux complet nécessitant peu de ressources pour fonctionner.
Quand je dis peu de ressources c'est : 128Mo de RAM et un SGF de

(a) **Mettez** 2 Micro Linux et **Reliez** les par un câble comme pour les VPCS



(b) **Cliquez** sur l'icône flèche verte, cela lance les 2 VM de type Linux dans la VM Linux ... et oui des Linux dans un Linux !

(c) **Cliquez** bouton droit sur chaque Linux et sous menu **console**, cela devrait vous ouvrir un terminal avec un Linux très très basique ☺

Sur **PC1**

(a) **Lancez** la commande **hostname PC1**

(b) **Lancez** la commande **ps** et à la fin vous devez voir la ligne
XXXX root /sbin/udhcpc -b -i eth0 -x hostname box -p /var/run/udhcpc.eth0.

(c) **Lancez** la commande ***kill -9 XXXX*** *afin de tuer ce processus (Les Linux ici sont des clients DHCP et on ne le veut pas)*

(d) **Vérifiez** qu'il est bien tué en relançant la commande **ps**.

(e) **Passez root** : **sudo su** <— sans le - ... Et oui tout n'est pas pareil ici

(f) **Lancez** la commande **ifconfig**

```
gns3@box:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0C:D3:DE:E5:00:00
          inet6 addr: fe80::ed3:deff:fee5:0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:170 errors:0 dropped:0 overruns:0 frame:0
          TX packets:178 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:58140 (56.7 KiB)  TX bytes:58788 (57.4 KiB)
```

L'interface eth0 n'a pas d'adresses IP, on va lui en mettre une :

(g) **Lancez** la commande ***ifconfig eth0 192.168.16.64 netmask 255.255.255.0***

```
gns3@box:~$ sudo su
root@box:/home/gns3# ifconfig eth0 192.168.16.64 netmask 255.255.255.0
root@box:/home/gns3# ifconfig
eth0      Link encap:Ethernet  HWaddr 0C:D3:DE:E5:00:00
          inet addr:192.168.16.64  Bcast:192.168.16.255  Mask:255.255.255.0
          inet6 addr: fe80::ed3:deff:fee5:0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
RX packets:186 errors:0 dropped:0 overruns:0 frame:0
TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:63612 (62.1 KiB)  TX bytes:64260 (62.7 KiB)
```

(h) **Faites** de même sur PC2

i. en changeant son nom

ii. en tuant le processus DHCP client.

iii. en mettant l'IP **192.168.16.33** ☺

(i) Sur les 2 Linux **lancez** la commande arp (Elle doit rien renvoyer). Normal le cache arp est vide pour l'instant

(j) **Mettez** une sonde Wireshark sur le câble entre les 2 Linux et **filtrez** avec le filtre **icmp || arp**

(k) **Pinguez** d'un Linux à l'autre à l'aide de la commande **ping -c 2 @IP de l'autre**

(l) Sur les 2 Linux **lancez** la commande arp

```
root@PC1:/home/gns3# arp
? (192.168.16.33) at 0c:84:30:ec:00:00 [ether]  on eth0
root@PC1:/home/gns3#

root@PC2:/home/gns3# arp
? (192.168.16.64) at 0c:d3:de:e5:00:00 [ether]  on eth0
root@PC2:/home/gns3#
```

4. **Synthèse** :

(a) C'est quoi une IP ?

(b) La commande pour mettre une IP sur une interface n'est pas toujours la même ! ! !

(c) C'est quoi ICMP ?

(d) C'est quoi ARP ?

7 SSH VM - Host

Nous allons voir qu'il est possible de faire communiquer la VM avec le HOST. De passer de l'un à l'autre.

Il y a un **pont** entre le HOST et la VM. On ne sait pas encore trop ce que c'est un pont mais l'image suivante est bonne. C'est une entité qui permet de relier deux rives. Ici les rives sont le HOST et la VM.

On va voir qu'il est possible de passer de l'un à l'autre.

1. **Laissez** la VM allumée
2. **Relevez** l'adresse IP de l'interface **enp0s8** à l'aide de la commande **ip a** vous devez voir quelque chose comme **192.16.56.xxx**
3. **Lancez** la commande **netstat -lntp**

   On remarque que le port 22 est ouvert (C'est le port de SSH)

```
etudiant@debian-11-GNS3:~$ netstat -ltnp
(Tous les processus ne peuvent être identifiés, les infos sur les processus
non possédés ne seront pas affichées, vous devez être root pour les voir toutes.)
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale           Adresse distante         Etat        PID/Program nam
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
```

4. **Lancez** la commande **ps aux | grep ssh**

   Vous devez voir une ligne comme celle-ci

```
etudiant@debian-11-GNS3:~$ ps aux | grep ssh
root XXX 0.0 0.0 13356 6896 ? Ss 12:06 0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 star
```

5. **Allez** sur le HOST
6. **Lancez** la commande **netstat -lntp**
   On remarque que le port 22 est ouvert aussi ?
7. **Lancez** la commande **ps aux | grep ssh**
   Vous devez voir une ligne du même genre

   ```
   Je n'ai pas fait sur le PC de la FAC ;)
   ```

8. Dans un terminal **lancez** la **ip a** et **relevez** l'IP de l'interface **vboxnet0**

   ```
   X: vboxnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
       link/ether 0a:00:27:00:00:00 brd ff:ff:ff:ff:ff:ff
       inet 192.168.56.1/24 brd 192.168.56.255 scope global vboxnet0
          valid_lft forever preferred_lft forever
       inet6 fe80::800:27ff:fe00:0/64 scope link
          valid_lft forever preferred_lft forever
   ```

   Cette interface **vboxnet0** sert de **pont** entre la VM et le HOST
9. **Lancez** la commande **ssh etudiant@192.168.56.XXX**
   ssh veut dire **shell sécurisé** nous étudierons ce protocole et cette commande plus en détails plus tard !

   ```
   2216643351@PC-FAC:~$ ssh etudiant@192.168.56.108
   etudiant@192.168.56.108's password:
   ```

   Mettez le MDP de etudiant : **Etudiant1**
   Et voilà vous êtes logué-e à distance du HOST à la VM (J'adore le mot distance ici alors que physiquement on est au même endroit)
10. Vous pouvez faire de même de la VM au HOST
11. Après l'avoir fait, sur le HOST comme sur la VM **lancez** la commande **who** et **interprétez** le résultat !
12. **Concluez** sur **pont**, **port** et **ssh** !

8 Conclusion

Pour un premier TP on a appris plein de choses que nous allons détaillées davantage dans les prochains TP.

N'oubliez pas de faire une synthèse ! ! ! !