Laboratoire Vbox-Linux (90 min)

0	Introduction	sudo ./c 2

Objectifs Ce travail fait suite aux labo DHCP, DNS, router, iptables et IPv6 du cours RPI effectués avec la distribution CentOS https://www.centos.org/ version 6.4
Il est aussi complémentaire au cours Système d'exploitation

Prérequis **Les pages 1 à 8 sont des prérequis à ce travail**
Valider vos connaissances avant la séance de labo

Session Ouvrir une **session administrateur sur le PC Win7** : compte=**albert** username=**admin**

Action Copier le dossier partagé **\\10.2.1.1\doclabo\Secu\Linux** sur le bureau
Clic sur **CentOS_NoFW**

Parcourir la fenêtre pour identifier les info utiles comme username, password, config. réseau, …

Démarrer cette VM
Ouvrir une session Linux
Entrer ifconfig pour contrôler que l'interface eth0 est bien configuré via DHCP
Noter la valeur de l'adr IP = ……
Démarrer votre labo à la page 9

Convention **La commande à entrer est en rouge et en gras.** **Exemple =** **who**
La réponse est en bleu **root**
Le commentaire éventuel est en italique ***username***

Remarque Faire attention à la casse car Linux distingue entre majuscule et minuscule

Astuce Utiliser la touche TAB pour simplifier l'écriture d'une commande ou d'un chemin d'accès

Livres Ces livres, disponibles au labo, fournissent un excellent complément à cette étude

Lien **Bash command line for Linux** → http://ss64.com/bash/

pdf **Red Hat – Deployment Guide** → dans **dossier copié :**

- **§3 Users & Groups**
- **§4 Gaining Privilieges (su & sudo)**
- **§6 Yum**
- **§9 Network Interfaces**
- **§11 Services & Daemons**

1	Quelques commandes de base	Prérequis

Remarque Le compte **root** créé lors de l'installation est un compte privilégié possédant les droits d'administration

a) **Qui suis-je ? Quel compte a été utilisé lors de l'ouverture de session ?**

```
who
root        tty1        2014-09-23 09:33
username    terminal    login time
```

b) **Quel est le nom du système ?**

```
uname –n
centos
node name
```

`hostname` donne le même résultat

c) **Comment interprétez-vous le prompt (invite de commande) `[root@centos ~]#`**

```
root → username
centos → node name
~ → dossier personnel
# → droit d'administration
```

d) **Quelle est la date et l'heure du système ?**

```
date
```

e) **Quelle est la version du noyau utilisé ?**

```
uname –a
Linux centos 2.6.32-358.e16.x86_64 #1 SMP Fri Feb 22 00 :31 :26 UTC
2013 x86_64 GNU/Linux
kernel-name node-name kernel-release kernel-version machine-
hardware-name operating-system
```

f) **Quelle est la version de CentOS ?**

```
cat /etc/redhat-release
CentOS release 6.4 (Final)
```

g) **Qui est connecté ? Combien d'utilisateurs sont connectés ?**

```
who –q
root
# users=1
```

h) **Où suis-je ? Dans quel dossier ?**

```
pwd
/root
```

i) **Quel est le contenu du dossier ?**

```
ls
anaconda-ks.cfg  install.log  install.log.syslog
```

`ll` Plus de détail → suite des explications dans §2
`ls –al` Affichage de tous les fichiers et y compris les fichiers cachés

j) **Créer le compte alice** `adduser alice`
Entrer un mot de passe facile à retenir `passwd alice`

k) **Quel est le groupe du nouvel utilisateur ?**

```
groups alice
alice : alice
user : group
```

Le nom du groupe principal est identique au nom d'utilisateur

Fermer la session root avec **exit**
Etablir une session avec le compte **alice**
Observer le symbole $ signifiant droit utilisateur à la fin du prompt

l) **Quel est le dossier par défaut ?**
/home/alice
Le symbole **~** signifie dossier personnel

m) **Que se passe-t-il si alice exécute la commande adduser bob ?**
Permission denied
Seul le compte root possède le droit d'ajouter un utilisateur ou un groupe au système

Remarque Idem pour supprimer un compte avec **userdel**

n) **Aller dans le dossier root (racine)**
cd /
Test avec **pwd**

o) **Aller dans le dossier /etc/**
cd etc
Test avec **pwd**

p) **Retourner dans le dossier personnel**
cd ~
Test avec **pwd**

q) **Retourner dans le dossier précédent**
cd -

r) **Effacer l'affichage**
clear

Astuce **Il est possible d'accéder aux commandes typées précédemment en utilisant les flèches HAUT et BAS du clavier**

s) **Créer le fichier texte.txt avec nano**
nano texte.txt
Ajouter le texte **1234**
Sauvegarder avec **CTRL+O** (min) » puis **ENTER**
Quitter nano avec **CTRL+X** (min)

t) **Répéter l'opération précédente en vous plaçant dans le bon dossier**
Test avec **ls** puis **cat texte.txt** pour afficher (lire) ce fichier sur le terminal

u) **Elever les privilèges d'alice pour lui permettre de créer le compte bob**
sudo adduser bob
alice is not in the sudoers file. This incident will be reported

v) **Comprendre les pipes et les redirections des flux d'entrée-sortie**
Rediriger la sortie d'une commande vers un fichier **ls –l > flux.txt**
Contrôler le contenu du fichier avec **nano flux.txt**

Remarque **>** Pour remplacer le contenu du fichier.
>> Pour ajouter à la fin du fichier.

Exécuter la commande **grep --help** pour connaître son utilisation
Le contenu est trop long et on ne voit pas le début du texte d'aide de la fonction grep.
Utiliser la commande **grep --help | more** qui va passer à l'aide d'un pipe le contenu de la commande **grep --help** à la commande **more** pour afficher le texte page par page

Caractères spéciaux peuvent être utilisée dans les chemins d'accès et dans certaines commandes :

```
?     match any single char
*     match any string
```

2	Sécurité	Prérequis

Objectif

Un serveur (de fichiers, de messageries, web, …) doit être configuré correctement.
Ce paragraphe traite :

- du contrôle d'accès discrétionnaire pour les utilisateurs avec ou sans droit d'administration
- des autorisations (read-write-execute)

Un auditeur informatique peut contrôler les principaux points de sécurité en comparant la configuration d'un serveur avec les bonnes pratiques (best practices)
RedHat fournit un excellent Security Guide :

- https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/
- Security_Guide_Linux6.pdf dans le **dossier partagé**

Avec le compte root

a) **Où sont stockés les logs ?**
Sec_Guide §4 → By default, security-relevant system logs are written to **`/var/log/secure`**

Sec_Guide §4 Never log in as the root user unless absolutely necessary
It is recommended that administrators use **sudo** to execute commands as root when required
Users capable of running **sudo** are specified in **/etc/sudoers**
Use the **visudo** utility to edit **/etc/sudoers**

b) **Ajouter alice dans /etc/sudoers**

```
visudo
```

Rechercher la ligne `root  ALL=(ALL)  ALL`
Ajouter la ligne `alice ALL=(ALL)  ALL`
Sauver et quitter `:wq`

Tester

```
exit
```

Etablir une session **alice**
Créer le compte bob

Remarque Voir Annexe 2 slides 7 – 8

c) **Changer de compte avec su (switch user)**
su sans argument donne accès au compte root

```
su -
```

Remarque Le mot de passe entré est mémorisé pendant 5 minutes

d) **Ouvrir le fichier /etc/shadow contenant username – password**

```
cat /etc/shadow
more /etc/shadow
```

Remarque Voir chap. Authentification

Le fichier **`/etc/group`** contient les groupes

e) **Changer de compte avec su (switch user)**

```
su - alice
```

Remarque **Les mêmes mécanismes existent sur Windows depuis 2007 (Vista)**

f) **Comprendre les droits d'accès aux fichiers**

Action Avec le compte **alice**

```
[alice@centos ~]$ ls -al
total 28
drwx------. 2 alice alice 4096 Apr 26 08:54 .
drwxr-xr-x. 5 root  root  4096 Apr 27 11:34 ..
-rw-------. 1 alice alice  257 Apr 27 11:24 .bash_history
-rw-r--r--. 1 alice alice   18 Feb 21  2013 .bash_logout
-rw-r--r--. 1 alice alice  176 Feb 21  2013 .bash_profile
-rw-r--r--. 1 alice alice  124 Feb 21  2013 .bashrc
-rw-rw-r--. 1 alice alice    5 Apr 26 08:50 texte.txt
[alice@centos ~]$
```

Information

d	→ dossier
rwx	→ autorisations Read – Write – eXecute pour le **propriétaire** (owner) du fichier
rw-	→ autorisations ……pour le **groupe**
r--	→ autorisations ……pour tous les autres utilisateurs (**other**)

Important **Le compte root n'est pas concerné par ces autorisations et peut donc tout faire sur tous les fichiers et dossiers**

g) **Qui est le propriétaire des fichiers & dossiers ?**

```
drwx------. 2 alice alice 4096 Apr 26 08:54 .
drwxr-xr-x. 5 root  root  4096 Apr 27 11:34 ..
-rw-------. 1 alice alice  257 Apr 27 11:24 .bash_history
-rw-r--r--. 1 alice alice   18 Feb 21  2013 .bash_logout
-rw-r--r--. 1 alice alice  176 Feb 21  2013 .bash_profile
-rw-r--r--. 1 alice alice  124 Feb 21  2013 .bashrc
-rw-rw-r--. 1 alice alice    5 Apr 26 08:50 texte.txt
              USER  GROUP
```

h) **Quelles sont les autorisations sur le fichier texte.txt créé au §1s) ?**

```
-rw-rw-r--. 1 alice alice    5 Apr 26 08:50 texte.txt
```

Read + Write pour Owner & Group
Read pour tous
Conclusion

- alice et root peuvent lire & écrire
- bob peut lire

i) **Ouvrir un 2ème terminal avec le compte root**

<CTRL+Alt+F2> pour ouvrir un 2ème terminal
<CTRL+Alt+F1> pour accéder au 1er terminal

j) **Ouvrir un 3ème terminal avec le compte bob**

k) **bob peut-il accéder au fichier créé par alice ?**

```
[bob@centos ~] cat /home/alice/texte.txt
... Permission denied
```

l) **root peut-il accéder au fichier créé par alice ?**

```
[root@centos ~] cat /home/alice/texte.txt
```

root peut lire et modifier ce fichier

m) **Pourquoi bob n'a pas accès fichier créé par alice ?**

```
[root@centos ~]# ls -al /home/alice
...
drwx------. 2 alice alice 4096 Apr 29 18:59 .
```

Seule alice peut accéder à ce dossier pour lire son inode (les fichiers présents)
Voir slide 4 de l'Annexe 2

n) **Donner à bob l'accès en lecture à ce fichier créé par alice ?**

```
[root@centos ~]# chmod o+r /home/alice
```

o) **Tester**

```
[root@centos ~]# ls -al /home/alice
...
drwx-----x. 2 alice alice 4096 Apr 29 18:59 .
```

bob peut lire ce fichier

```
[bob@centos ~]$ cat /home/alice/texte
1234
```

p) **Créer le groupe g2 comprenant alice et bob**

```
[root@centos ~]# groupadd g2
                 usermod –aG g2 alice      append Group
                 usermod –aG g2 bob
```

q) **Créer le dossier d2 réservé au groupe g2**

```
[root@centos ~]# mkdir /tmp/d2
                 ls –al /tmp/d2
drwxr-xr-x. 2 root root 4096 Apr 29 20:27 .
drwxrwxrwt. 4 root root 4096 Apr 29 20:27 ..
                 chmod 750 /tmp/d2
                 ls –al /tmp/d2
                 chown root:g2 /tmp/d2
                 ls –al /tmp/d2
```

r) **alice créé le fichier f2**

```
[alice@centos ~]$ groups
alice
[alice@centos ~]$ exit
```

Etablir une nouvelle session alice

```
[alice@centos ~]$ groups
alice g2
[alice@centos ~]$ touch /tmp/d2/f2      Créer le fichier f2
                  ls –al /tmp/d2
```

s) **tester les autorisations (r et w) pour alice & bob**

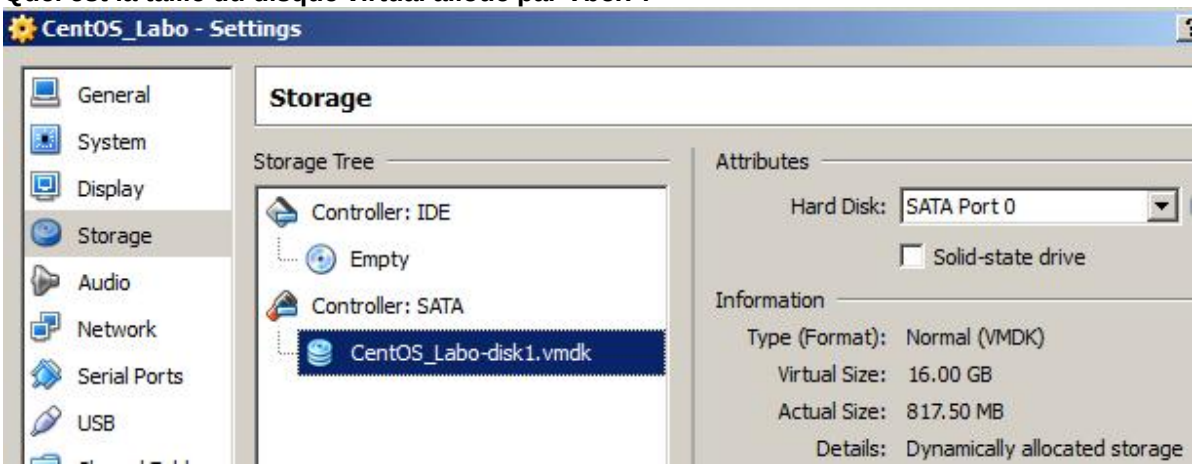
alice peut lire et écrire
bob ne peut que lire

3	Stockages local & distant	Prérequis

Objectifs Avec le compte **root**, retrouver l'information utile du système de stockage : disques physiques, partitions, taux d'occupation, systèmes de fichiers, fichiers ouverts, …

a) **Quelle est la taille du fichier CentOS_NoFW.ova ?**
267 MB (MegaByte) selon Explorer Windows

b) **Quel est la taille du disque virtual alloué par Vbox ?**



16 GB

c) **Quelles sont les disques présents ? Quelle est leur taille ?**

```
[root@centos ~]# fdisk -l

Disk /dev/sda: 17.2 GB, 17179869184 bytes
...
Disk /dev/mapper/vg_centos-lv_root: 14.5 GB, 14537457664 bytes
...
Disk /dev/mapper/vg_centos-lv_swap: 2113 MB, 2113929216 bytes
...
```

3 disques

- Il n'y a en fait qu'un seul disque utile /dev/sda construit avec la couche LVM (Logical Volume Manager)
- LVM assure l'indépendance entre disque(s) physique(s) et disque accessible au système de fichiers → Cours chap. Virtualisation
- **Ignorer donc la partie LVM** → /dev/mapper

d) **Quelle est leur taille en Mebibyte (1 Mebibyte = 1024 x 1024 = 1'048'576) ?**

```
[root@centos ~]# sfdisk -l -uM

Disk /dev/sda: 2088 cylinders, 255 heads, 63 sectors/track
Units = mebibytes of 1048576 bytes, blocks of 1024 bytes, counting from 0

   Device Boot  Start    End     MiB    #blocks   Id  System
/dev/sda1   *      1    500     500     512000   83  Linux
/dev/sda2        501  16383   15883   16264192   8e  Linux LVM
/dev/sda3          0      -       0          0    0  Empty
/dev/sda4          0      -       0          0    0  Empty
```

Le disque **/dev/sda** comprend 4 partitions :

- **/dev/sda1** Capacité = 500 MiB avec démarrage (boot)
- **/dev/sda2** Capacité = 15883 MiB
- **/dev/sda3** Capacité = 0
- **/dev/sda4** Capacité = 0

Remarque Les disques SCSI, SATA et USB sont nommés **/dev/sda, /dev/sdb, …**
Les disques IDE sont nommés **/dev/hda**

e) **Quel est le taux d'occupation des partitions ?**

```
[root@centos ~]# df -H      disk free in Mebibyte
Filesystem              Size   Used  Avail Use% Mounted on ...
                         15G   792M    13G   6% /
tmpfs                   523M     0   523M   0% /dev/shm
/dev/sda1               508M    33M   449M   7% /boot
```

La partition de démarrage est occupée à 7%
Le disque est occupé à 6%

f) **Quel est le système de fichiers ?**

```
 [root@centos ~]# df -T
Filesystem     Type   1K-blocks      Used Available Use% Mounted ...
               ext4    13973860    773032  12490992   6% /
tmpfs         tmpfs      510268         0    510268   0% /dev/shm
/dev/sda1      ext4       495844     31954    438290   7% /boot
```

Disque et partition sont formatés en ext4

Remarques Système de fichiers ext4 → http://fr.wikipedia.org/wiki/Ext4
Prochain système de fichiers → http://fr.wikipedia.org/wiki/Btrfs
Principaux dossiers et fichiers d'un système Linux
→ http://www.tecmint.com/linux-directory-structure-and-important-files-paths-explained/

g) **Quels sont les packages installés ?**

```
rpm –qa
```

La liste étant longue, afficher écran après écran avec `rpm –qa ¦ less`
`space puis CTRL z`

h) **Le package nano est-il installé ?**

```
rpm –q nano
```

oui

i) **Le package telnet est-il installé ? non**

j) **Ajouter - retirer une clé USB**

Activer USB dans Vbox → VM Power Off – USB - 

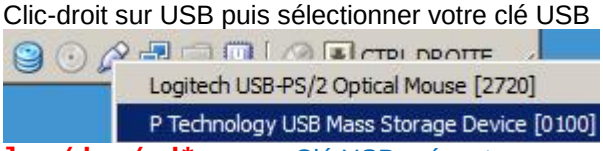

```
yum –y install usbutils
lsusb          Quels sont les périphériques USB présents ?
Bus 001 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

Connecter une clé USB

Cliquer sur la notification Windows → 


```
ls /dev/sd*          Pas de périphérique sdb
```

Clic-droit sur USB puis sélectionner votre clé USB




```
ls /dev/sd*          Clé USB présente
mkdir /mnt/key
mount /dev/sd* /mnt/key
sfdisk -l            Le système de fichiers (FAT16, …) est détecté
```

Opération inverse avant de retirer la clé

```
umount /mnt/key
```

Remarque Lorsque l'on démonte un périphérique, le dossier n'est pas supprimé. Vous pouvez soit le supprimer, soit le laisser pour la prochaine fois que vous monterez ce périphérique.

4	Réseau	30 min

Objectifs Savoir gérer et configurer la partie réseau (interface, services) avec le compte **root**
Administrer le système CLI Linux à distance avec des outils conviviaux comme **PuTTY** et **WinSCP**

Liens https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html-single/Deployment_Guide/
Voir aussi Deploy.pdf dans le **dossier partagé**

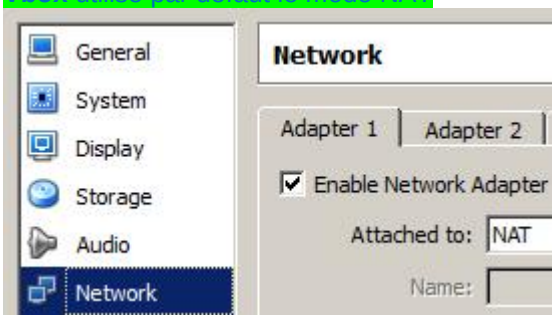
But 4.1 **Déterminer les paramètres réseau**

```
[root@centos ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:80:3F:4A
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr:
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:143 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25930 (25.3 KiB)  TX bytes:7439 (7.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
```

a) **Quelles interfaces sont disponibles et à quoi correspondent-elles?**

eth0 Correspond à la carte réseau virtuelle qui communique sur l'interface Ethernet physique de la carte mère du PC
Aller dans la configuration Réseau de Virtual Box pour connaître le détail
Vbox utilise par défaut le mode NAT



Voir slides 59-60 du chap. Défense_Périmétrique

lo Correspond à la boucle locale

b) **Quelle est l'adresse Ethernet ?**
HWaddr 08:00:27:80:3F:4A

c) **Quelle est l'adresse IP ?**
inet addr:10.0.2.15

Info Cette adresse a été fournie par le serveur DHCP que Vbox active en mode NAT
Vbox : File – Preferences – Network – Edit – DHCP Server

d) **Quel est le masque de sous-réseau ?**
Mask:255.255.255.0

e) **Quel est l'état de l'interface**
UP

Info **Pour le désactiver `ifdown eth0`**
Tester
Pour l'activer `ifup eth0`
Tester

f) **Quel est le débit binaire du port Ethernet ?**

```
[root@centos ~]# ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 0
        Transceiver: external
        Auto-negotiation: on
        MDI-X: Unknown
        Supports Wake-on: d
        Wake-on: d
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
```

Variante

```
[root@centos ~]# dmesg | grep -i duplex
e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
```

g) **Quelle est la route par défaut (adresse IP du routeur) ?**

```
[root@centos ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
0.0.0.0         10.0.2.2        0.0.0.0         UG    0      0        0 eth0
```

IP = 10.0.2.2 est l'adresse du routeur ; correspond au module NAT implémenté par Vbox

Test avec `ping 10.0.2.2`

h) **Quel est le serveur DNS utilisé par défaut ?**

```
cat /etc/resolv.conf
; generated by /sbin/dhclient-script
nameserver 10.2.0.1
```

= interface LAN du firewall pfSense
pfSense configuré en DNS forwarder
Voir slide 107 du chap. Défense_Périmétrique

Remarque A chaque résolution DNS, le client lit le fichier **`/etc/resolv.conf`**

But 4.2 **Déterminer les ports et les services utilisant le réseau**

a) **Quels sont les ports à l'écoute ?**

```
netstat –ltupn        listen – tcp – udp – program – numeric
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address    State   PID/Program name
tcp        0      0 0.0.0.0:22     0.0.0.0:*          LISTEN  1092/sshd
tcp        0      0 127.0.0.1:25   0.0.0.0:*          LISTEN  1168/master
tcp        0      0 ::22           :::*               LISTEN  1092/sshd
tcp        0      0 ::1:25         :::*               LISTEN  1168/master
udp        0      0 0.0.0.0:68     0.0.0.0:*                  983/dhclient
```

Remarque Voir aussi http://www.thegeekstuff.com/2010/03/netstat-command-examples/

b) `yum –y install lsof` Installer cet excellent outil

`lsof –i`

	COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
1	dhclient	983	root	5u	IPv4	10270	0t0	UDP	*:bootpc
2	sshd	1092	root	3u	IPv4	10598	0t0	TCP	*:ssh (LISTEN)
3	sshd	1092	root	4u	IPv6	10607	0t0	TCP	*:ssh (LISTEN)
4	master	1168	root	12u	IPv4	10797	0t0	TCP	localhost:smtp (LISTEN)
5	master	1168	root	13u	IPv6	10799	0t0	TCP	localhost:smtp (LISTEN)

Remarque L'affichage est plus riche et mieux structuré

1 Processus dhclient (PID=983) en attente sur UDP:68 (bootp)

2 Processus sshd (PID=1092) en attente sur TCP:22 (ssh)

3 IPv6

4 Processus master → serveur de messagerie smtp à désactiver

5 IPv6

c) `yum –y remove postfix` Supprimer le package Serveur de messagerie

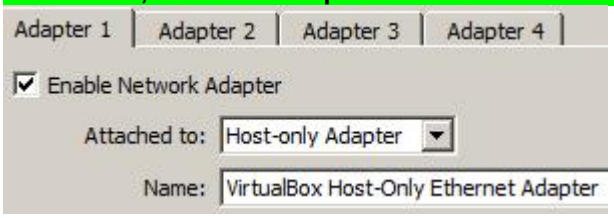
d) `lsof -i` Contrôler

e) **Quels sont les services actifs ?**

```
[root@centos ~]# service –-status-all
iscsi is stopped
iscsid is stopped
lvmetad is stopped
mdmonitor is stopped
multipathd is stopped
netconsole module not loaded
Configured devices:
lo eth0
Currently active devices:
lo eth0
rdisc is stopped
restorecond is stopped
rsyslogd (pid  999) is running...
sandbox is stopped
saslauthd is stopped
openssh-daemon (pid  1048) is running...
```

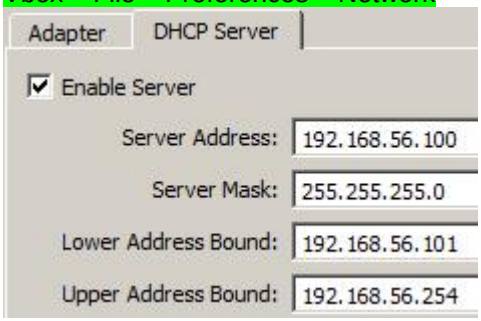
But 4.3 **Administrer le système à distance avec le protocole SSH**
Il donne un accès distant sécurisé (chiffré et signé) en mode terminal comme telnet

a) **Dans Vbox, arrêter la VM pour utiliser le mode réseau Host-Only**



Remarque Lors de son installation, Vbox ajoute cette interface virtuelle dans Win7

Activer le serveur DHCP dans le réseau Host-Only
Vbox – File – Preferences – Network



Démarrer la VM
`ifconfig eth0` déterminer l'adresse IP

Info Le fiewall pfSense, qui protège le labo, attribue une adresse IP=10.2.3.X aux clients DHCP

b) **Désactiver les firewalls**

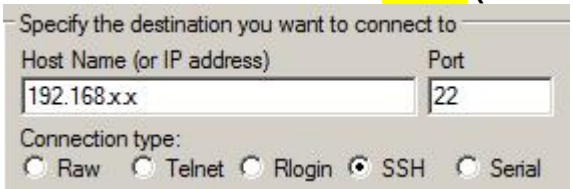
```
service iptables stop          Arrêter le service
service ip6tables stop
chkconfig iptables off         Ne plus démarrer ce service lors du prochain démarrage
chkconfig ip6tables off
```

Info Ces 4 commandes sont optionnelles car le firewall contient les règles pour SSH → Voir labo iptables

c) **Tester la connectivité avec ping depuis Win7**

d) **Tester la connectivité avec ping depuis la VM**

e) **Etablir une session SSH avec PuTTY (raccourci bureau)**



Yes pour accepter

f) **Observer cette nouvelle connexion avec `lsof -i`**

```
sshd ...  TCP 192.168.1.45:ssh>192.168.1.50:8335 (ESTABLISHED)
```

g) **Utiliser WinSCP (Secure Copy) pour administrer**
Utiliser raccourci bureau

But 4.4 **Configurer l'interface réseau avec une adresse IP statique**

```
ifconfig eth0 down
ifconfig eth0 192.168.56.2 netmask 255.255.255.0
ifconfig eth0 up
```

Test

```
ping 192.168.56.1
```

Remarques La configuration ci-dessus n'est pas permanente car les paramètres par défaut sont appliqués au redémarrage du système

Lors d'analyse de type forensique, il est important de récupérer ces données volatiles (qui disparaissent lors d'un redémarrage)

Voir §6 h) pour une configuration permanente nécessaire pour équipements serveurs, routeurs, …

But 4.5 **Configurer l'interface réseau avec `/etc/sysconfig/network-scripts/ifcfg-ethX`**

La configuration réseau précédente disparait lors d'un redémarrage car le système initialise chaque interface à partir de **`/etc/sysconfig/network-scripts/ifcfg-ethX`**

Config DHCP par défaut

```
DEVICE=ethX
TYPE=Ethernet
#UUID       used by Network Manager
ONBOOT=yes  Device activated at boot
NM_CONTROLLED=yes    Network Manager
BOOTPROTO=dhcp        boot protocol
HWADDR=08:00:27:xx:xx:xx
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System ethX"
```

Config statique

```
DEVICE=ethX
TYPE=Ethernet
#UUID
ONBOOT=yes
NM_CONTROLLED=no  No Network Manager
BOOTPROTO=none    no boot protocol
HWADDR=08:00:27:xx:xx:xx
IPADDR=192.168.1.10
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
DNS1=192.168.1.1
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System ethX"
```

Voir §9.2.1 du Deployment Guide (dossier partagé) pour le détail des paramètres

```
service network restart
```

Remarque Pour la résolution des FQDN, le système utilise en premier lieu les informations contenues dans le fichier /etc/hosts puis il va utiliser le(s) serveur(s) DNS du fichier /etc/resolv.conf.

But 4.6 **Ajouter le dossier partagé `nfs_share` sur le serveur `10.2.1.1`**

Vbox : configurer le réseau en mode bridge

```
yum –y install nfs-utils      Ajouter le package
mkdir /mnt/extern
mount -t nfs4 10.2.1.1:/nfs_share /mnt/extern
```

Tester

5	Au cœur du système	30 min

a) **Commande ps (process status)**

```
[root@centos ~]# ps
```
lister les processus associés au terminal courant

```
  PID TTY          TIME CMD
 1428 pts/0    00:00:00 bash
 1519 pts/0    00:00:00 ps
```

Deux processus sont affichés : celui du shell par défaut et celui de la commande ps

- PID → Process Identifier — Identifiant du processus
- TTY → Teletype — Terminal
- TIME — Temps CPU consommé
- CMD → commande

b) `ps –ef ¦ more` Lister tous les processus

Remarque –e (exhaustive) liste tous les processus Ils sont listés
–f (full) affiche UID (User ID), PID, PPID (Parent PID), C (CPU), STIME (cumulative System Time), TTY, TIME, CMD

c) `ps –ef ¦ grep sshd` Le processus sshd est-il actif ?

```
UID        PID  PPID  C STIME TTY          TIME CMD
root      1155     1  0 09:47 ?        00:00:00 /usr/sbin/sshd
root      1424  1155  0 09:51 ?        00:00:00 sshd: root@pts/0
root      1524  1428  0 10:48 pts/0    00:00:00 grep sshd
```

d) **Commande top**

```
top
top - 10:51:15 up  1:04,  2 users,  load average: 0.00, 0.00, 0.00
Tasks:  69 total,   1 running,  67 sleeping,   1 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   1020540k total,   129168k used,   891372k free,     6392k buffers
Swap:  2064376k total,        0k used,  2064376k free,    38376k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    7 root      20   0     0    0    0 S  0.3  0.0   0:11.90 events/0
    1 root      20   0 19228 1476 1212 S  0.0  0.1   0:00.94 init
```

1 **Temps abs & relatif** **Nb user** **Charge moyenne sur 1 – 5 – 15 min**
2 **69 processus**
3 **Charge CPU**
4 **Occupation RAM**
5 **Occupation du Swap**

e) **Commande simple dont le résultat se trouve dans top**

```
free
```
occupation RAM

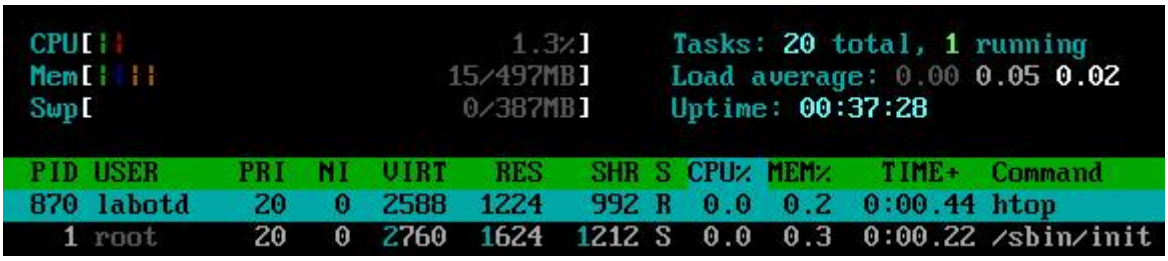
```
             total       used       free     shared    buffers     cached
Mem:       1020540     129912     890628          0       6568      38396
-/+ buffers/cache:      84948     935592
Swap:      2064376          0    2064376
[root@centos ~]#
```

```
uptime
11:09:35 up  1:22,  2 users,  load average: 0.00, 0.00, 0.00
```

f) **Commande htop**

Cette commande n'est pas installée

```
yum install wget
http://pkgs.repoforge.org/htop/htop-1.0.2-1.el6.rf.x86_64.rpm
rpm -i  htop-1.0.2-1.el6.rf.x86_64.rpm        installer
htop
```



Ligne CPU

Ligne Mem RAM **15 MB occupés / 497 MB disponibles**

Ligne Swap **0 MB occupé / 387 MB disponibles**

Ligne 4 **PID USER PRI**

Action Lister selon l'occupation RAM **<F6> MEM% <Enter>**
Lister selon l'utilisateur **<F6> USER <Enter>**
Lister selon la charge CPU **P**
Lister selon l'occupation RAM **M**
Lister (ou supprimer) les processus noyau (Kernel) **K**
Avec les processus noyau affichés (Tasks: 61), utiliser les curseurs pour vous déplacer
Sans les processus noyau affichés (Tasks: 20), typer plusieurs fois sur **<F5>** pour activer/désactiver l'arborescence père-fils

g) **Quels sont les fichiers ouverts par alice ?**

```
[root@centos ~]# lsof -u alice
COMMAND  PID  USER   FD   TYPE DEVICE SIZE/OFF   NODE NAME
bash    6736 alice  cwd    DIR  253,0     4096 130713 /home/alice
bash    6736 alice  rtd    DIR  253,0     4096      2 /
bash    6736 alice  txt    REG  253,0   903272    280 /bin/bash
bash    6736 alice  mem    REG  253,0 99158576 262663 /usr/lib/locale/locale-...
bash    6736 alice  mem    REG  253,0    65928 130340 /lib64/libnss_files-2.12.so
bash    6736 alice  mem    REG  253,0  1916568 130324 /lib64/libc-2.12.so
bash    6736 alice  mem    REG  253,0    19536 130330 /lib64/libdl-2.12.so
bash    6736 alice  mem    REG  253,0   135896 130366 /lib64/libtinfo.so.5.7
bash    6736 alice  mem    REG  253,0   154464 130317 /lib64/ld-2.12.so
bash    6736 alice  mem    REG  253,0    26060 392479 /usr/lib64/gconv/gconv-...
bash    6736 alice    0u   CHR    4,2      0t0   5097 /dev/tty2
bash    6736 alice    1u   CHR    4,2      0t0   5097 /dev/tty2
bash    6736 alice    2u   CHR    4,2      0t0   5097 /dev/tty2
bash    6736 alice  255u   CHR    4,2      0t0   5097 /dev/tty2
```

h) **Etat des processus**

Action Afficher l'état des processus : **`ps –ax ¦more`**

Remarque Valeurs possibles du champ STAT :

```
R    Running or runnable (on run queue)
S    Interruptible sleep (waiting for an event to complete)
D    Uninterruptible sleep (usually IO)
Z    Defunct ("zombie") process, terminated but not reaped by its parent.
T    Stopped, either by a job control signal or because it is being traced.
W    paging (not valid since the 2.6.xx kernel)
X    dead (should never be seen)
<    high-priority (not nice to other users)
N    low-priority (nice to other users)
L    has pages locked into memory (for real-time and custom IO)
s    is a session leader
l    is multi-threaded (using CLONE_THREAD, like NPTL pthreads do)
+    is in the foreground process group
```

i) **Relation père fils des processus**

Action Dans le terminal 2, typer **`cat ¦ tail ¦ pr ¦ wc`**

Remarque Utiliser http://ss64.com/bash/ pour connaître le détail de chaque commande

Action Dans le terminal 1, typer **`ps –f –t tty2`**
Etudier les champs PID et PPID
Variante avec **`ps –fx –t tty2`**

j) **Exécution d'un programme Set-UID**

Action Dans le terminal 2, typer **`ps -ef`**
Dans le terminal 1, typer **`passwd`**
Dans le terminal 2, typer **`ps –ef`** pour constater que l'UID de **`passwd`** = **`root`**

k) **Chronologie des services démarrés**
`pstree`
Voir http://doc.ubuntu-fr.org/init_d

l) **Commande `vmstat`**
Quelle est son utilité ? **`man vmstat`**

m) **Pseudo-fichiers /proc**
Le noyau exporte des données utiles (CPU, mémoire, …) en RAM (pseudo-fichiers analogues à la base de registre Windows) dans une arborescence accessible depuis /proc

Comprendre l'intérêt des commandes :

```
cat /proc/version
cat /proc/cpuinfo
cat /proc/uptime
```

`cat /proc/xxx/stat` choisir une valeur de PID,
utiliser http://man7.org/linux/man-pages/man5/proc.5.html

```
ls /proc/net
cat /proc/net/dev
cat /proc/net/route
```
les données sont en hexa little endian

n) **`shutdown –h now`** Eteindre le système

o) **`reboot`** Redémarrer

p) **Afficher les logs lors du démarrage**

<F1> Touche F1 lors du démarrage pour voir les logs

```
               Welcome to CentOS
Starting udev: piix4_smbus 0000:00:07.0: SMBus base address uninitialized - upgr
ade BIOS or use force_addr=0xaddr
                                                           [  OK  ]
Setting hostname centos:                                   [  OK  ]
Setting up Logical Volume Management:   2 logical volume(s) in volume group "vg_
centos" now active
                                                           [  OK  ]
Checking filesystems
/dev/mapper/vg_centos-lv_root: clean, 18497/887696 files, 244651/3549184 blocks
/dev/sda1: clean, 38/128016 files, 48110/512000 blocks
                                                           [  OK  ]
Remounting root filesystem in read-write mode:             [  OK  ]
Mounting local filesystems:                                [  OK  ]
Enabling /etc/fstab swaps:                                 [  OK  ]
Entering non-interactive startup
Starting monitoring for VG vg_centos:   2 logical volume(s) in volume group "vg_
centos" monitored
                                                           [  OK  ]
ip6tables: Applying firewall rules:                        [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:
Determining IP information for eth0..._
```

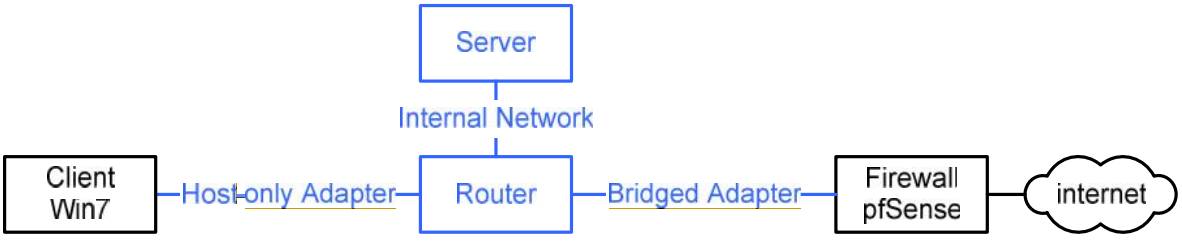
q) **`dmesg`** Message du noyau

r) **`cat ~/.bash_history`** Historique des commandes entrées
`ctrl r` Rechercher commande dans l'historique

s) **Intérêt de la commande**
`who -l`
`who --help`

6	**Travail personnel**	**30 min**

Objectifs
Configurer cette infrastructure sur le PC (la partie Vbox est en bleu)
Produire les VMs Router et Server en effectuant un clone de **CentOS_NoFW.ova**
Etablir un **schéma détaillé** avec adresses IP, …
Définir les **étapes** en tenant compte des dépendances



Rendu **Chaque groupe rend son schéma**
Enumérer les étapes configurées et testées