Projet linux
15h de theorie
35h de labo (ou +)

Objectif : réaliser un serveur Linux par groupe de 2 ou 3
→ rendre un rapport
→ on sera questionné sur la securité, …
→ 15 min oral
→ utiliser des bonnes methodologies
→ Journal de bord à jour
→ argumenter ses choix

Que va faire le serveur ?
C'est un serveur :
- web
- ftp
-fichier
-Ntp (temps)
-DNS

(Tout mettre sur le meme serveur c est degueulasse, mais on a pas le choix.
On pourrait faire 5vm mais faut les faire tourner en meme temps, c'est de la merde.)

→ script d'install + automatiser les taches
→ rendre le tout administrable à distance

→ Voir liste des services à installer

1) **pour le serveur de fichier** :
→le serveur devra contenir un partage NFS qui permettra aux users du reseau local d'y stocker des fichiers
Note : pas obligatoire de faire une db mais on peut

→ un partage SAMBA, permettant d'acceder au meme dossier que celui partagé en NFS.
Note : pas de regles precisé

Pour le samba : faire une db pour login + mdp

Comme c est un serveur de fichier, il faut mettre en place certaines politiques.
C'est à dire :
→ faire attention à ce que certains users ne foutent pas la merde
→ empecher les users de remonter jusqu au dossier parent
→ faire un backup regulierement des fichiers qui sont stockés sur le serveur
→ …

2) pour le reste

Mettre en place un serveur :
→ web
→ FTP
→ MySQL
→ DNS

Serveur web : apache ou Nginx
note : le prof ne fournit pas le support sur Nginx
Malaise ne connait pas les virtual Host, il est pas à l'aise avec ça.

Permettre un hebergement multi user.
Ex : on est un peu comme OVH
On est un fournisseur de stockage de site web
Le client il va arriver et va demander :
→ 1 nom de domaine
→ 1 espace pr stocker le site
→ 1 serveur pr qu il soit accessible

Bordel pr config

Pour cela :
→ Dans le DNS, creer une zone qui va permettre d'avoir l'url pour le site
→ config un virtual host (façon dont apache/Nginx peut gerer plusieurs sites differents avec url different)
→ acces FTP au dossier de l'user (login + mdp)
Il va avoir droit à un login + mdp ftp
Une DB mySQL
Un site : toto.toto
Avoir un virtual host de cree

Et en plus de ça, il faudra automatiser les taches
A l'examen, il va arriver en tant que new user.
→cree moi un serveur web
→ cree moi un ftp
→ montre moi que tu sais t'y connecter
→ stocke y une page web
→ montre moi que j'ai acces à partir d'une machine client que j'ai acces à la page web grace à l'url qu'on a cree

→ impossible de faire ça manuellement le jour de l'exam, donc AUTOMATISER tout ce bordel.
Il faudra donc
→ creer des scripts
→ se connecter en ssh à la machine (par defaut il est installé)
ça serait mieux de l'utiliser avec une cle asynchrone (il faut la generer)

→ il va nous donner : un login + un mdp
→ on lance nos scripts via ssh et il faut qu' a la fin tout soit config automatiquement

3) Le DNS fera office de DNS cache

c 'est un dns qui retient dans une db stocké dans le ram, les differentes requetes qui ont deja ete faites pour accelerer les recherches suivantes du dns.
(facile)

4**) Mettre en place un serveur de temps (NTP)**
→ il doit pouvoir se sync avec un serveur sur internet
→ ET il doit permettre à des clients de sync sur notre ntp

Pourquoi s'amuser à ce qu'il y ait un serveur ntp ?
→ taches planifiés
→ bourse (acheter des actions)
→ gestion des vols (controleur aerien)
→ bcp de systeme qui necessite une gestion du temps

5)**Pour effectuer des config le jour de l'exam, il faudra creer un compte**

est ce qu'on se connecte en root directement à la machine ? Avec un user sudo ?
Et a distance on se connecte comment ? En root directement ?
On peut, avec une clé asynchrone

On peut aussi faire un user et le mettre dans la liste des sudo user
Et lui mettre des droits restreints …

Bloquer les connexion SSH en dehors du reseau local ? (c est une façon de securiser)
….

On est les admin du serveur, il faut donc agir en consequence :

Le jour de l'exam il faudra rendre :
→ fichier de config des services cree
→ justification pq on a choisi ça (quel distro? Pq ?)
→ automatiser les taches (scripts) proactif
→ gerer les backups
→ securiser (TRES ATTENTION)
Mettre en place un firewall (Selinux)
Systeme de securité intégré

il lie des dossiers avec des taches
Certains process n'ont acces qu' a certains fichiers

Par exemple on veut deplacer un fichier :
var/www/html

page où sont stockés les pages web

Si on essaye de les mettre dans un autre dossier, SE Linux va nous en empecher car il considere que les autre dossiers ne sont pas consideres à gerer ce genre de fichier.

ls -e
ou
ls -x

permet d'afficher les users SeLinux qui ont acces à certains dossier
On peut creer des nouveaux dossiers et donner acces aux utilisateurs d'apache à un autre dossier
(C'est barbare et ça vaut qu' 1 point)

Creer une politique des users
Quand on cree un user qui a acces au serveur web est ce qu'on va aussi lui donner acces en ssh à la machine ?
A nous de voir, c'est possible

Mettre des quotas
serveur de fichier : empecher les user, à foutre en l air le serveur de fichier en saturant le bordel.
Serveur web : quota aussi, au moins sur le ftp

Partitionnement des disk
lvm, raid1

Gestion de backup
comment ? Quel utilitaire ?
Deporter sur un serveur distant ?
A quel moment ?
Comment les automatiser

Maj de l'OS
Desactiver services inutiles
Installer desktop et puis retirer au fur à mesure ?
Commencer avec une v core et installer les services un par un ?

Configurer un noyau?

Mettre en place un firewall

Mettre en place un atv

Securité …

Comment se passe l'evalutation ?
Evalué par Malaise
machine cliente :
→ windows (utilisation de samba) ou linux + samba (en client)
→ ftp
→web
→ ntp
A tester pour que ça soit fonctionnel

Demontrer le fonctionnement des services en 15 minutes

Montrer le fichier de config rapidement

Redirection de port
Rechercher les port pour le NFS (ça a l'air chiant)
Samba : on sait bloquer les ports
Pour apache : on sait bloquer les ports
Pour Dns : on sait bloquer les ports

Pour ntp : port 123
Pour ssh : port 22 (c'est mieux de changer le port par defaut)

Grille d'evaluation ?

1)La premiere commande qu 'il va taper à l'examen :
→ se status
pour voir si on a activé ou pas seLinux (1point ou 0)

2) Verification que le firewall est bien demarré et activé
3) verification du nfs (verification qu'il marche)
4) verification de la config dans le rapport
5) mise en place de quota
6) droit cree pour les fichiers
7) parametre samba
(protégé contre le chroot ? Je comprends pas ce qu'il dit)
8) web fonctionnement (conf par defaut, securité pas defaut → pas grand chose à faire)
9) droit, user par defaut d'apache ou cree un autre
10) ftp ; quota, securisé
est ce que la connexion est chiffré, mise en place du TSL
User virtuel ou chaque user a un home ?
11)SSH connexion en root ou sudo user
clé de connexion asynchrone
12)execution des scripts ok
13)est ce qu'il peut foutre la merde ?
14) avec root en local uniquement ?

15) Securité : mdp sur bootloader
mdp bios ; pas obligatoire car logiquement le serveur est mis dans une salle securisé avec un cadenas
16) option de montage securisé pour chaque point de montage
17)partitionnement correct
Ne pas melanger serveur Web avec partage de fichier …
LVM ou pas et pourquoi
18) mise en place d'un atv
19) empecher les user web à se logger
20) pour le mysql il verifie juste qu'il est fonctionnel et verification de l'installation
Avec mySecure install il fait tt tout seul, il config automatiquement la securité

tout ce bordel ça vaut 17 ou 18 points
le reste c 'est ce qu'on aura ajouté comme fct

rapport (c'est moins important dans la cotation mais on sera penalisé si on le rend pas)
→ il aimerait bien avoir les rapports avant pr qu il puisse nous poser les questions le jour de l exam

fichier de config (il va les verifier, et c est sur ça qu'il cotera)
justification