accès root/admin sans mot de passe sous XP, Vista & Linux

Utilisation de Kon-boot pour se logger en tant que root / administrateur sans connaitre le mot de passe sous Windows XP, Vista et Linux

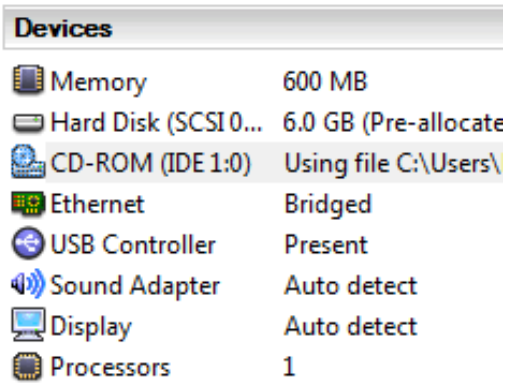
A travers ce tutoriel, nous allons utiliser Kon-boot afin de gagner un accès root / admin sur des machines sans meme connaitre le mot de passe.

1/ Kon-boot: présentation et explications

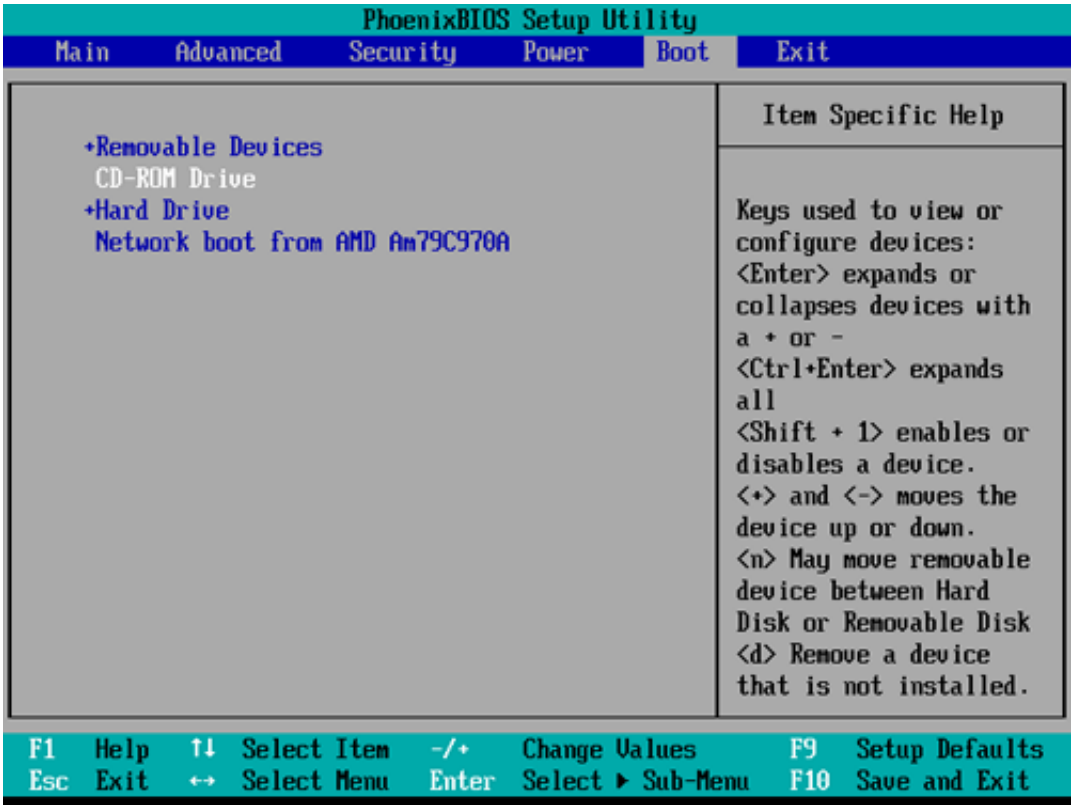
Kon-boot est un logiciel qui permet de modifier le contenu d'un noyau Linux ou Windows à la volée pendant le boot. Sous Linux, il permet de se logger en tant que root sans connaitre le mot de passe. Sous Windows, il permet de se logger en utilisant n'importe quel compte utilisateur ou administrateur, toujours sans connaitre le mot de passe. Kon-boot se présente sous la forme d'un fichier .iso faisant à peine 110 Ko une fois décompressé. Bien entendu, il s'agit d'une image disque servant à créer un cd ou une disquette afin de booter la machine sur laquelle vous avez besoin de vous logger sans connaitre le mot de passe (un accès physique à la machine est bien sur indispensable). Pour tester Kon-boot, nous allons l'utiliser sous un environnement VMWare Workstation (émulation d'OS, machines virtuelles) et nous logger sans mot de passe sur un OS Linux et un Vista. Avant de

commencer l'exercice, il faut télécharger le soft: KON-BOOT - ULTIMATE WINDOWS/LINUX HACKING UTILITY. Nous configurons maintenant notre machine virtuelle afin de la faire booter sur le fichier CD-konboot-v1.1-2in1.iso:

Tout d'abord, nous allons faire un tour dans les règlages des périphériques, et nous renseignons le CDRom avec le chemin vers le fichier image:



Ensuite, nous allons démarrer la machine virtuelle et nous rendre dans le BIOS en appuyant sur F2 juste après le démarrage. Dans la section Boot du BIOS, nous allons modifier l'ordre de Boot afin que la machine virtuelle boote directement sur le cd:



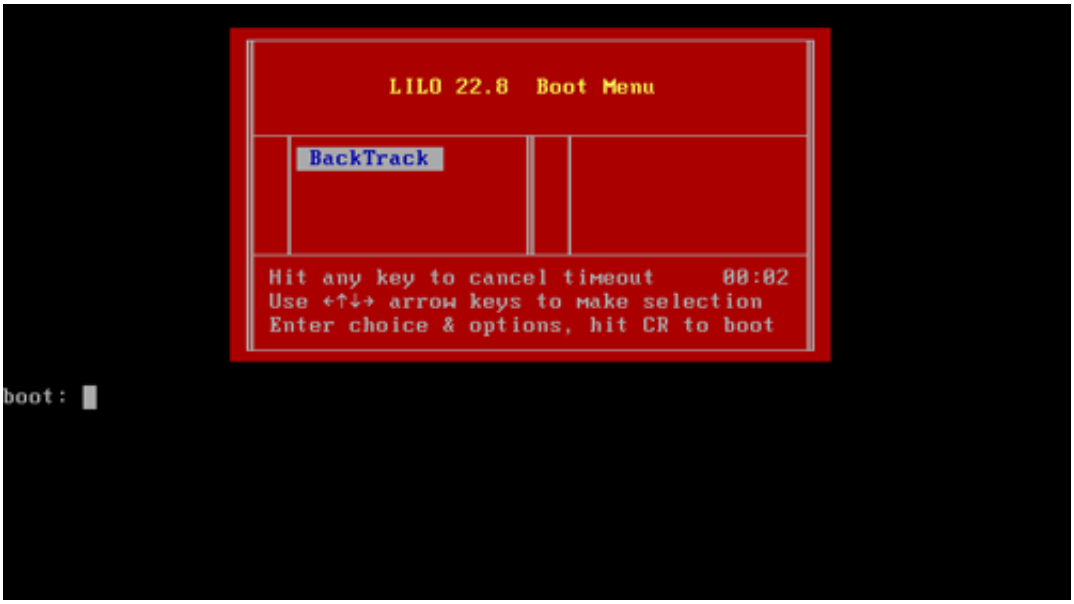
La config de test est prete, nous pouvons nous lancer.

2/ Test de Kon-boot sous environnement Linux: Backtrack 3 Beta

Nous pouvons démarrer notre ordinateur. Au boot, nous commençons par voir sur l'écran une image inhabituelle:

Et puis le soft va vérifier le BIOS et se lancer, en s'injectant dans le kernel:

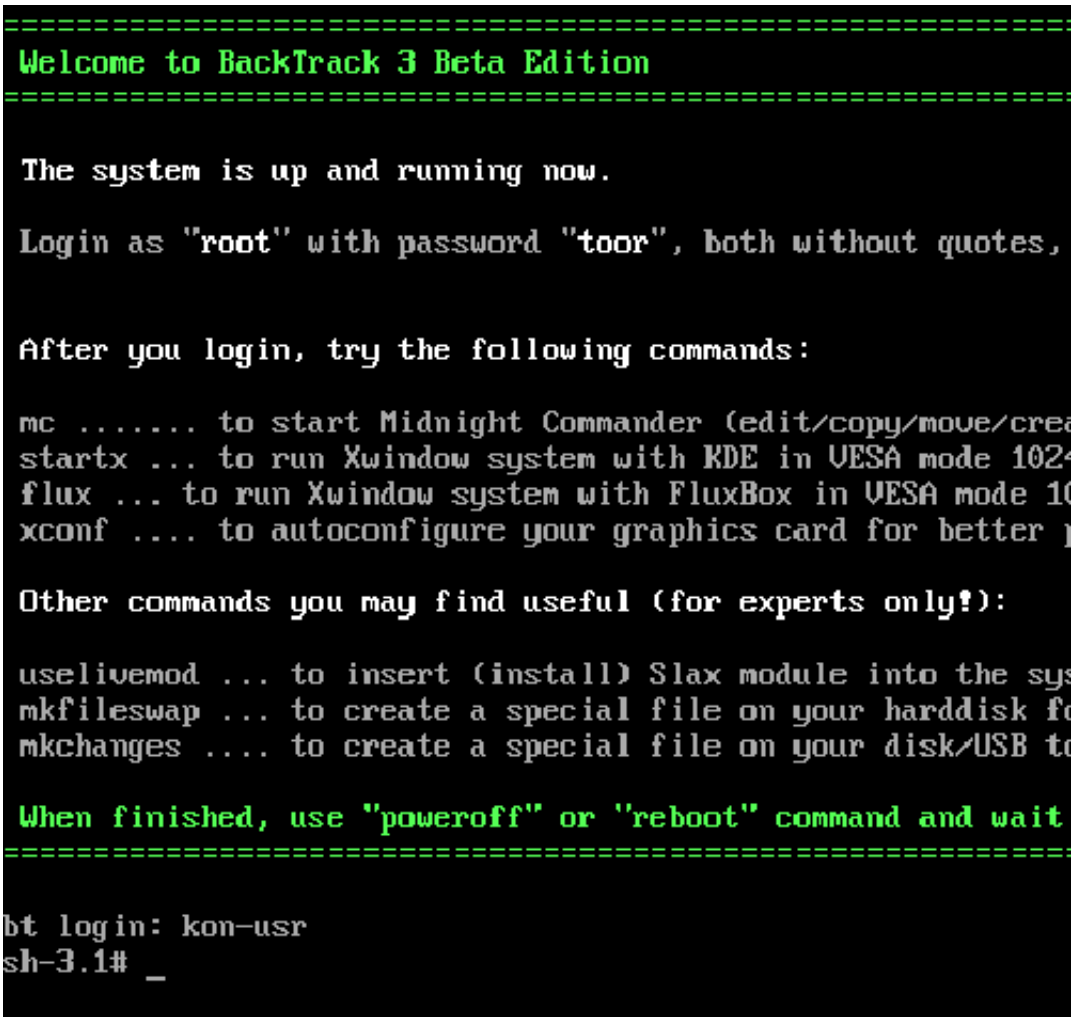
Après cela, nous retrouvons notre Lilo comme si de rien n'était:



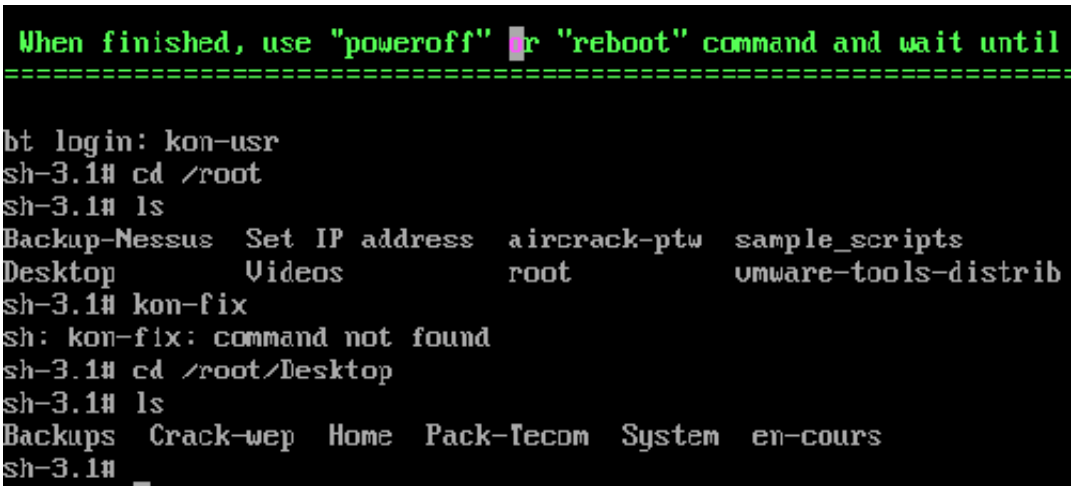
Et le système boote normalement:

Arrivés au login, il nous suffit de valider:

kon-usr



Vous noterez que nous n'avons pas eu a valider de mot de passe... Et pourtant, comme on peut le voir sur la capture d'écran qui suit, nous avons bel et bien un accès root:



Nous pouvons lister le contenu des dossiers, et faire ce que nous souhaitons sur la machine... C'est la fete!

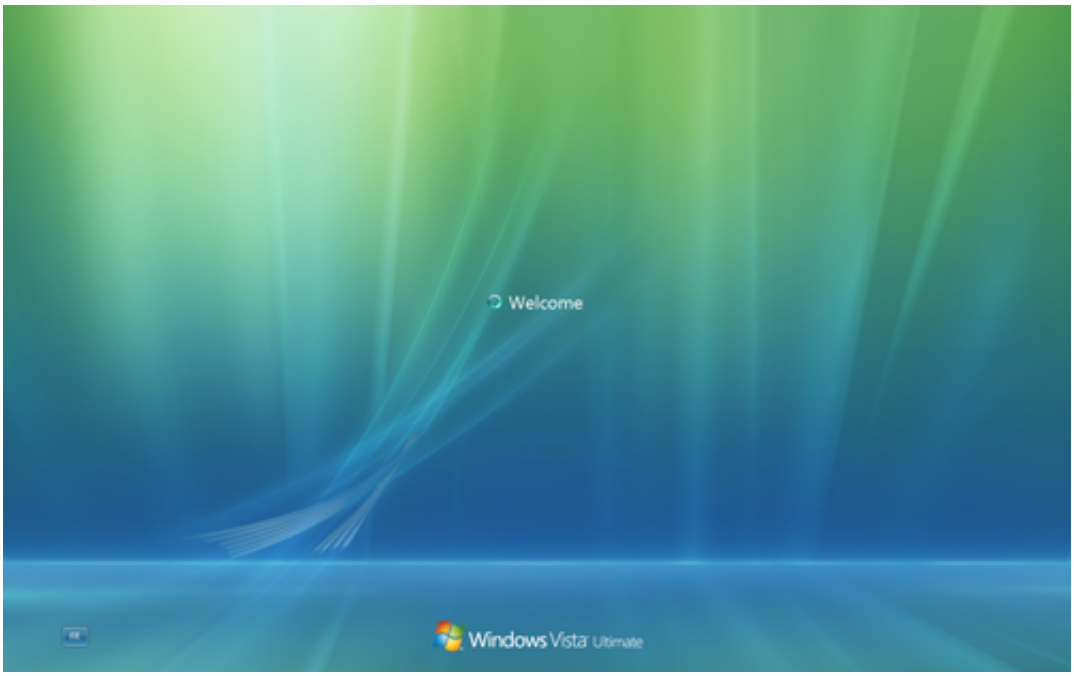
3/ Test de Kon-boot sous environnement Windows: Vista Ultimate

Toujours sur une machine virtuelle pour le besoin du test, nous nous attaquons cette fois ci à une machine tournant sous Windows Vista Ultimate. Nous avons toujours droit à nos petits screens sympathiques avant le boot:

Puis notre Vista Ultimate boote de façon classique:

Nous voici rendus à l'écran de login:

On y va? Je clique dans le champ "Password", mais je ne tape absolument rien, je me contente de valider avec entrée... Suspense...



Je vous le donne en mille: et bien oui, nous y sommes, loggé en tant qu'admin sans avoir validé de mot de passe:

Pour finir, voici une liste d'OS supportés par Kon-boot (liste non exhaustive):

Kernel	Grub
Gentoo 2.6.24-gentoo-r5	GRUB 0.97
Ubuntu 2.6.24.3-debug	GRUB 0.97
Debian 2.6.18-6-686[1]	GRUB 0.97
Fedora 2.6.25.9-76.fc9.i686[2]	GRUB 0.97

Tested Windows versions
Windows Server 2008 Standard SP2 (v.275)
Windows Vista Business SP0
Windows Vista Ultimate SP1
Windows Vista Ultimate SP0
Windows Server 2003 Enterprise
Windows XP
Windows XP SP1
Windows XP SP2
Windows XP SP3
Windows 7

Amusez vous bien

.