

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

Utilisation de Kon-boot pour se logger en tant que root / administrateur sans connaître 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 même connaître le mot de passe.

1/ Kon-boot: présentation et explications

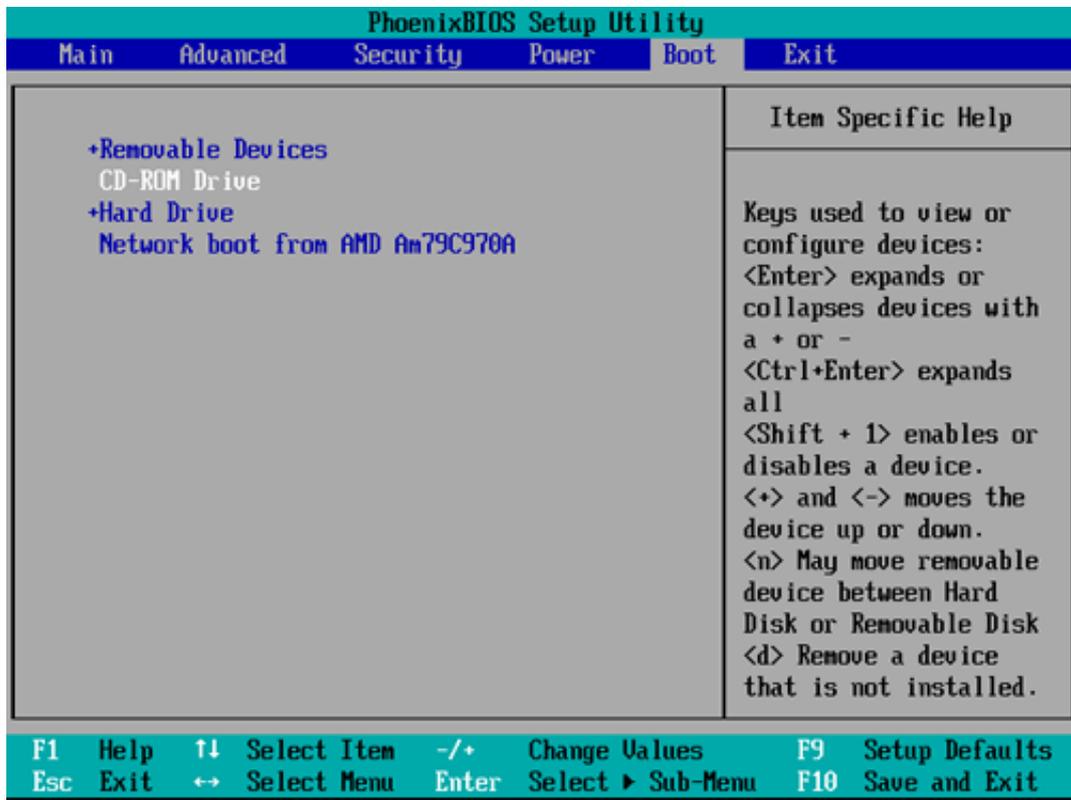
Kon-boot est un logiciel qui permet de modifier le contenu d'un noyau Linux ou Windows à la volée pendant le boot. Sous Linux, il permet de se logger en tant que root sans connaître le mot de passe. Sous Windows, il permet de se logger en utilisant n'importe quel compte utilisateur ou administrateur, toujours sans connaître 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 connaître le mot de passe (un accès physique à la machine est bien sûr 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 réglages des périphériques, et nous renseignons le CDRom avec le chemin vers le fichier image:

Devices	
 Memory	600 MB
 Hard Disk (SCSI 0...	6.0 GB (Pre-allocate
 CD-ROM (IDE 1:0)	Using file C:\Users\<
 Ethernet	Bridged
 USB Controller	Present
 Sound Adapter	Auto detect
 Display	Auto detect
 Processors	1

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

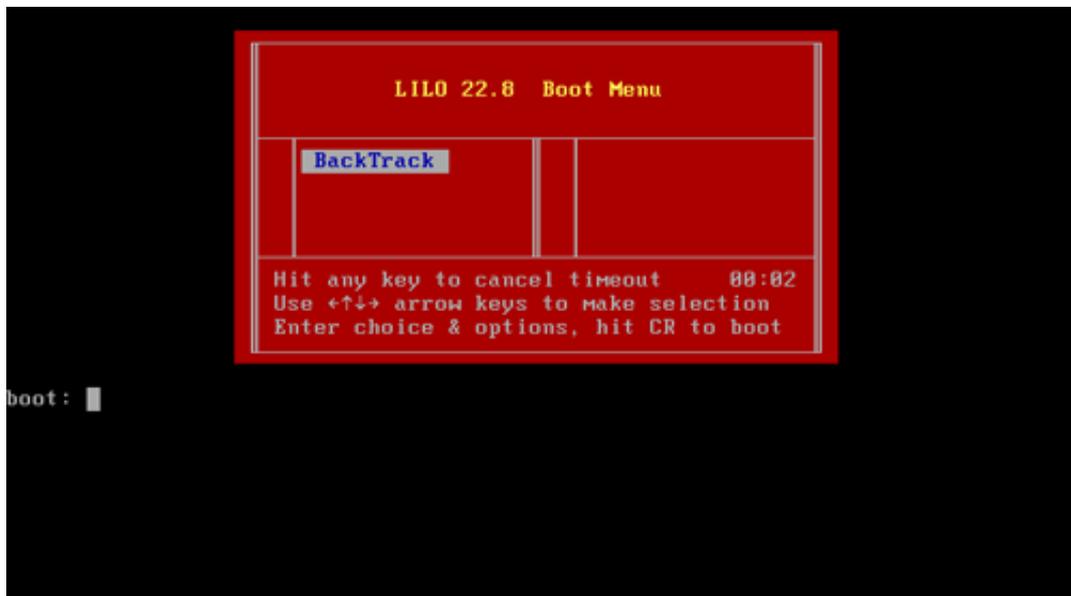
Nous pouvons démarrer notre ordinateur. Au boot, nous commençons par voir sur l'écran une image inhabituelle:



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:

```
lp0: using parport0 (interrupt-driven).
lp0: console ready
Use 'slax noapp' boot parameter to skip the following step:
fuse init (API version 7.8)
Capability LSM initialized
Checking non-root filesystems:
fsck 1.1.11 (21-May-2006)
usbfs on /proc/bus/usb type usbfs (rw)
Mounting non-root local filesystems:
Original command line: "/sbin/mount.ubifs -o rw,ttl=5 .host:/mnt/ubifs"
Host component of share name is ".host"
Directory component of share name is "/"
Parsing option string: rw,ttl=5
Setting mount read-write
Setting maximum attribute TTL to 5
ubifs: module license 'unspecified' taints kernel.
UBIFS: ubifs: UBI is disabled in the host
Error: cannot mount filesystem: Protocol error
Using /etc/random-seed to initialize /dev/random.
INIT: Entering runlevel: 3
Doing multiuser...
Starting PCMCIA services:
  <Probing for PCIC: edit /etc/rc.d/rc.pcmcia>
Intel ISA PCIC probe: not found.
Database TCIC:~ PCMCIA probe: not found.
Starting syslogd daemons: /usr/sbin/syslogd /usr/sbin/klogd -o 3 -x
Triggering udev events: /sbin/udevtrigger --retry-failed
Auto Configure IP address for eth0: /sbin/dhclient -t 60 eth0 &
Starting ACPI daemon: /usr/sbin/acpid
```

Arrivés au login, il nous suffit de valider:

kon-usr

```
=====
Welcome to BackTrack 3 Beta Edition
=====

The system is up and running now.

Login as "root" with password "toor", both without quotes,

After you login, try the following commands:

mc ..... to start Midnight Commander (edit/copy/move/crea
startx ... to run Xwindow system with KDE in VESA mode 1024
flux ... to run Xwindow system with FluxBox in VESA mode 10
xconf .... to autoconfigure your graphics card for better p

Other commands you may find useful (for experts only!):

uslivemod ... to insert (install) Slax module into the sys
mkfileswap ... to create a special file on your harddisk fo
mkchanges .... to create a special file on your disk/USB to

When finished, use "poweroff" or "reboot" command and wait
=====

bt login: kon-usr
sh-3.1# _
```

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:

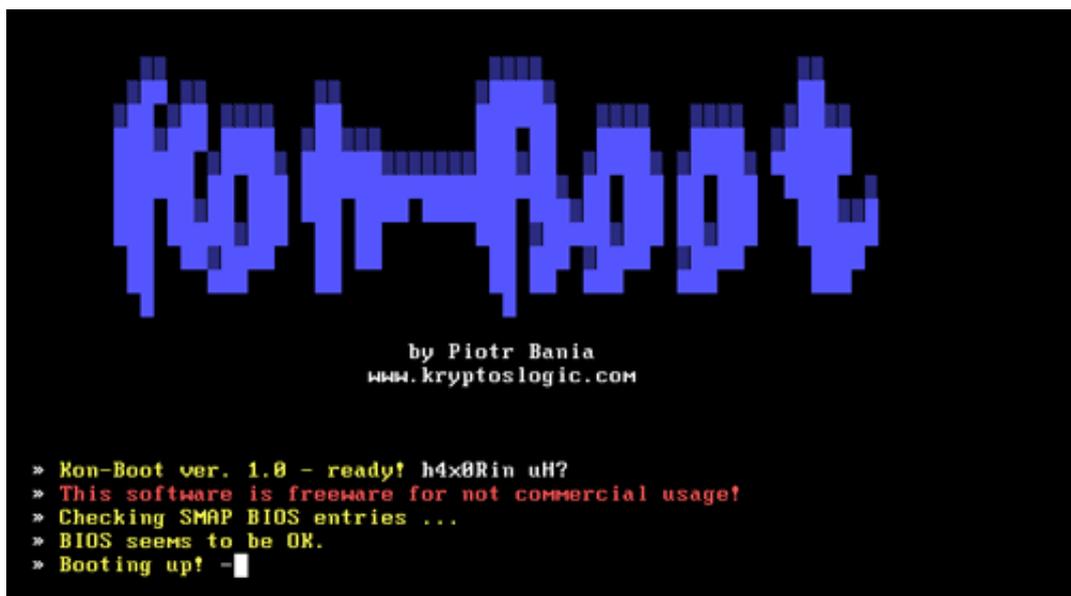
```
When finished, use "poweroff" or "reboot" command and wait until
=====

bt login: kon-usr
sh-3.1# cd /root
sh-3.1# ls
Backup-Nessus  Set IP address  aircrack-ptw  sample_scripts
Desktop        Videos         root          umware-tools-distrib
sh-3.1# kon-fix
sh: kon-fix: command not found
sh-3.1# cd /root/Desktop
sh-3.1# ls
Backups  Crack-wep  Home  Pack-Tecon  System  en-cours
sh-3.1# _
```

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

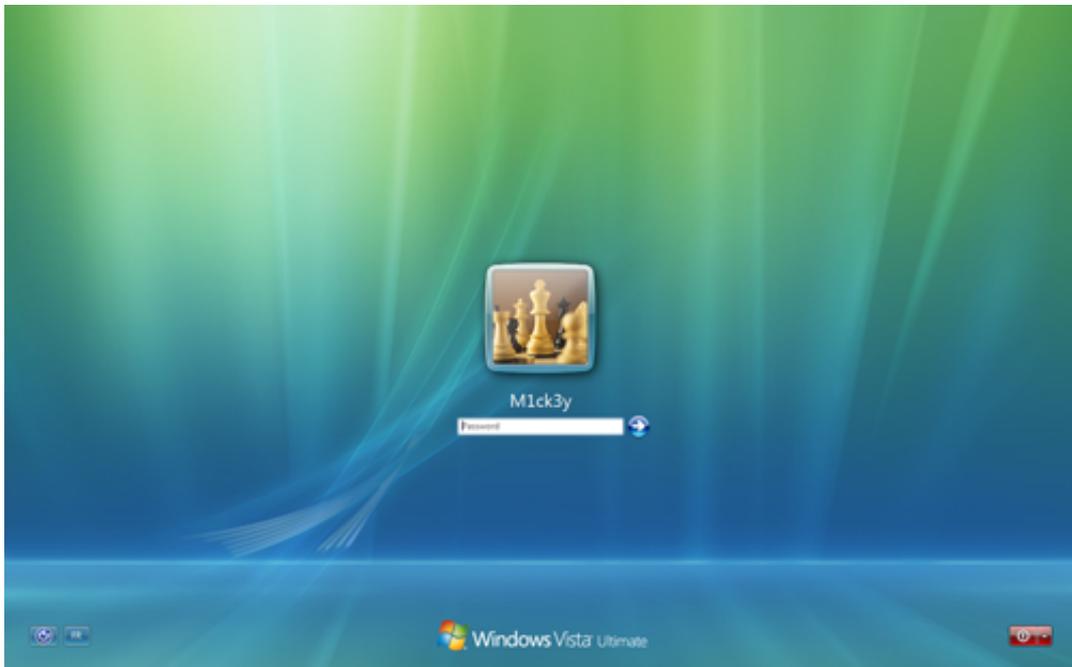
Toujours sur une machine virtuelle pour le besoin du test, nous nous attaquons cette fois ci à une machine tournant sous Windows Vista Ultimate. Nous avons toujours droit à nos petits screens sympathiques avant le boot:



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:

