```
Auteur: SRIKANTHAN Sabiran
```

Partie 2: Protection des fichiers et des logs sous Linux

1. Créer un fichier de test

On va créer un fichier de test fichier_critique.txt

```
sudo touch /home/glpi/fichier_critique.txt
ls
```

Le fichier critique à bien était créer

---

2. Appliquer la restriction sur le fichier_critique.txt avec chattr

> La commande chattr rend un fichier inéditable il peut être ni modifier ni supprimé et ni renommé

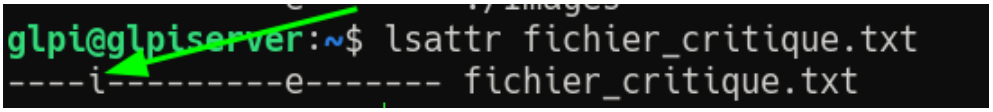
On va rendre le fichier “fichier_critique” inéditable avec la commande :

```
chattr -i /home/glpi/fichier_critique.txt
```

Puis après on fait :

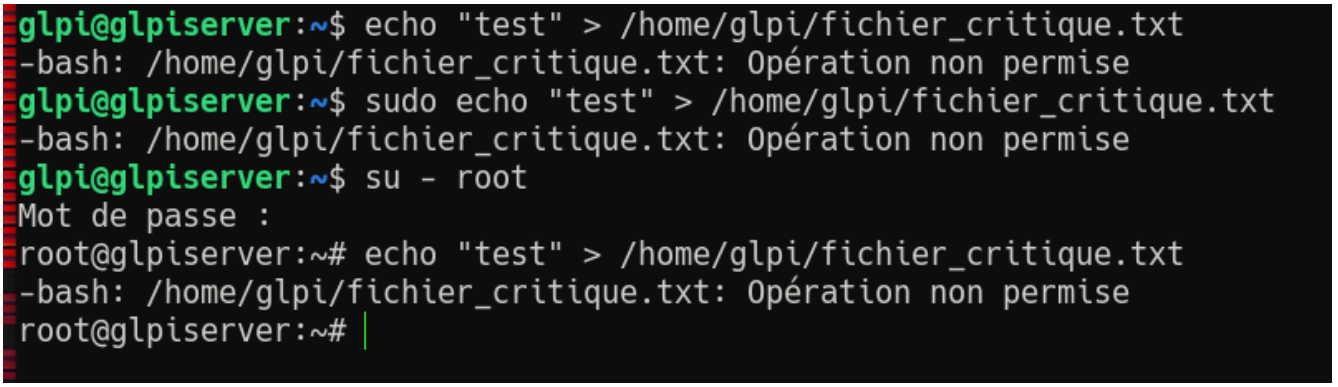
```
lsattr /home/glpi/fichier_critique.txt
```

On voit que le fichier_critique.txt



On voit bien que le fichier à l'option "-i" qui veut dire que le fichier est immuable.

On va voir si le chattr marche



On voit que autant que simple utilisateur avec le droit admin et ainsi que au root je ne peux pas écrire dans le fichier.

---

3. Configurer la surveillance avec auditd

Installation des paquets auditd :

```
sudo apt install auditd
```

On va ajouter une règle pour surveiller le fichier du test :

```
    sudo auditctl -w /home/glpi/fichier_critique.txt  -p wa -k
test_surveillance

    # -w Surveille le fichier "fichier_critique"
    # -p wa Surveille les permissions d'écriture & d'accès
    \#-k fichier_test pour retrouver cette règle plus facilement
dans les logs
```

On va vérifier si les règles ont bien été appliqué

```
sudo auditctl -l
```

```
glpi@glpiserver:~$ sudo auditctl -l
-w /home/glpi/fichier_critique.txt -p wa -k test_surveillance
glpi@glpiserver:~$
```

---

4. Vérifier les logs de surveillance

On va tenter d'accéder au fichier_critique pour générer des logs:

```
sudo echo "test" > /home/glpi/fichier_critique.txt
```

On va tenter de lire pour générer une activité

```
cat /home/glpi/fichier_critique.txt
```

Puis pour verfier les log au tape la commande suivante:

```
sudo ausearch -k test_surveillance
```

```
time->Mon Feb 10 16:14:46 2025
type=PROCTITLE msg=audit(1739200486.541:193): proctitle="-bash"
type=PATH msg=audit(1739200486.541:193): item=1 name="/home/glpi/fichier_critique.txt" inode=391759 dev=08:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0
cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1739200486.541:193): item=0 name="/home/glpi/" inode=391683 dev=08:01 mode=040700 ouid=1000 ogid=1000 rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe
=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1739200486.541:193): cwd="/home/glpi"
type=SYSCALL msg=audit(1739200486.541:193): arch=c000003e syscall=257 success=no exit=-1 a0=ffffff9c a1=55c879802160 a2=241 a3=1b6 items=2 ppid=2407 pid=4590 auid=1000 uid=1
000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4 comm="bash" exe="/usr/bin/bash" subj=unconfined key="test_surveillance"
---
```

On voit que on a pas réussit a accéder sur le fichier "fichier_critiques.txt"
