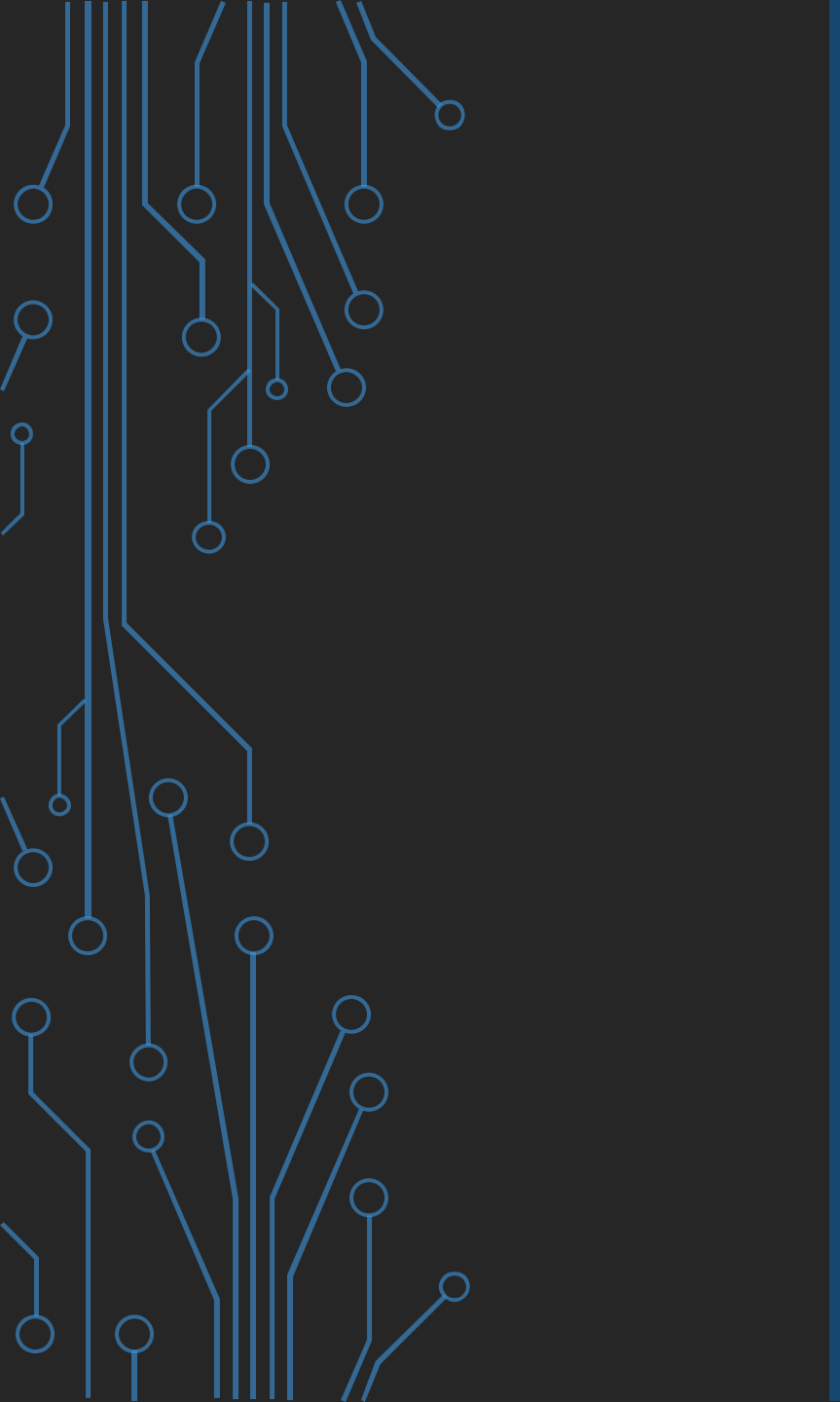


école supérieure de génie informatique

HARDENING LINUX SERVEUR

ARTHUR DUPUIS & BENJAMIN GERSCHEL

QU'EST CE QUE LE HARDENING ?

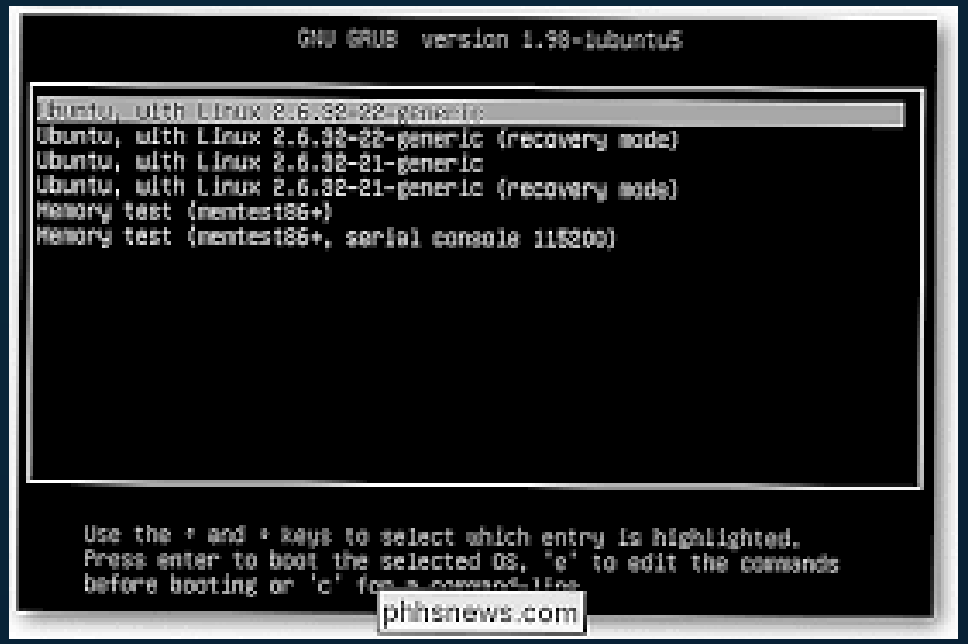
- Fortifier une machine, un serveur, un poste client, dans l'optique d'en augmenter le niveau de sécurité.

SÉCURISER LE BIOS

- Protégez le BIOS par mot de passe même si le mot de passe est volatile suite à l'enlèvement de la pile
- Désactivez le boot via CD/DVD, USB, Périphérique externe, le Boot live permet à quiconque ayant un accès physique à la machine d'accéder au système.

SÉCURISER LE GRUB

- GRUB est le chargeur de démarrage Linux, en démarrant en mode rescue quiconque ayant un accès physique à la machine peut modifier le mot de passe root..



CHIFFRER LE SYSTÈME

- Chiffrer ses données c'est important, en cas de vol ou d’intrusion un simple boot en live permet d'accéder aux données.

PARTITIONNER SON SYSTÈME

- Partitions = meilleure sécurité des données en cas de sinistre.
- un disque permet d'avoir des fonctionnalités supplémentaires (chiffrement, LVM, etc …)
- utilisez LVM afin d'agrandir/réduire les partition sans abîmer le FS.

```
#Exemple de partition
/
/boot
/usr
/var
/home
```

UTILISEZ SEULEMENT LES PAQUETS NÉCESSAIRE

- Éviter d'installer des paquets inutiles, ça minimise les risques de vulnérabilités

```
yum install list #Afficher le spaquets installés (CentOS & redhat)
chkconfig --list| grep '3:on' #afficher les services démarré en lvl 3
dpkg --list #afficher les paquets installés (debian)
```

SÉCURISER SSH

- Par défaut la sécurité de SSH peut-être amélioré (incontournable puisque SSH est un des services les plus attaqués !)

```
yum install list #Afficher le spaquets installés (CentOS & redhat)
chkconfig --list| grep '3:on' #afficher les services démarré en lvl 3
dpkg --list #afficher les paquets installés (debian)
```

INTERDIRE LES UTILISATEURS AU CRON

- Cron permet d'autoriser / interdire des utilisateurs via /etc/cron.allow et /etc/cron.deny

```
Pour interdire tout les utilisateurs et en autoriser certains
echo ALL >> /etc/cron.deny
echo user >> /etc/cron.allow
```

INTERDIRE LES PÉRIPHÉRIQUES USB

- Eviter la diffusion de malware via USB ou rubberDuck

```
echo "install usb-storage /bin/true" >> /etc/modprobe.d/no-usb
```

INTERDIRE LES PÉRIPHÉRIQUES USB

- Eviter la diffusion de malware via USB ou rubberDuck

```
echo "install usb-storage /bin/true" >> /etc/modprobe.d/no-usb
```

RENFORCER LE CONTROL D'ACCÈS NOYAU (SELINUX)

- SELinux est un mécanisme de sécurité du contrôle d'accès dans le noyau. Si le serveur est accessible depuis le net, je vous conseille de l'activer.
- Enforcing : Mode par défaut qui active et applique la stratégie de sécurité SELinux sur la machine.
- Permissive : SELinux n'appliquera pas la politique de sécurité, mais avertira seulement et enregistrera les actions. (Mettez au moins celui la pour avoir des traces)
- Désactivé

```
sestatus #pour avoir l'état du SELinux
setenforce permissive #Activer le SELinux en permissive

Se configure aussi dans /etc/selinux/config
```

SUPPRIMER L'INTERFACE GRAPHIQUE / BUREAU

- Hors de question de voir des serveurs linux avec un bureau ! C'est moche et sa ouvre des failles de sécurité potentielle

DÉSACTIVER IPV6 (SI NON UTILISÉ)

Dans /etc/sysctl.conf

# désactivation de ipv6 pour toutes les interfaces
net.ipv6.conf.all.disable_ipv6 = 1

# désactivation de l'auto configuration pour toutes les interfaces
net.ipv6.conf.all.autoconf = 0

# désactivation de ipv6 pour les nouvelles interfaces (ex:si ajout de carte réseau)
net.ipv6.conf.default.disable_ipv6 = 1

# désactivation de l'auto configuration pour les nouvelles interfaces
net.ipv6.conf.default.autoconf = 0

sysctl -p #Recharger la configuration

EMPÊCHER D'UTILISER UN ANCIEN MOT DE PASSE

#Copiez le fichier par sécurité en cas d'erreur : cp /etc/pam.d/common-password /root

#dans /etc/pam.d/common-password (Ajoutez à la fin du fichier)
auth sufficient pam_unix.so likeauth nullok

#Ajouter en dessous de la section password (se souvient des 5 derniers pass)
password sufficient pam_unix.so nullok use_authtok md5 shadow remember=5

APPLIQUER UNE POLITIQUE DE MOT DE PASSE FORT

apt-get install libpam-cracklib

#Copiez le fichier par sécurité en cas d'ereur : cp /etc/pam.d/common-password /root

#Dans /etc/pam.d/common-password (ajouter la ligne dans la section password)

password required pam_cracklib.so try_first_pass retry=3 minlen=12 difok=2 ucredit=-2 lcredit=-2 dcredit=-2 ocredit=-2 reject_username

Retry=3 (Autorise 3 essais pour la saisie du mot de passe
Minlen=12 (Longueur minimale de 12 caractères obligatoire)
Difok=3 (Nombre de caractères qui doivent être différents entre l'ancien et nouveau mot de passe)
ucredit=-2 (Doit contenir au moins 2 minuscules)
lcredit=-2 (Doit contenir au moins 2 majuscules)
dcredit=-2 (Doit contenir au moins 2 chiffres)
ocredit=-2 (Doit contenir au moins 2 symboles/caractères spéciaux)

ACTIVER LE PAREFEU

Un bon parefeu empêche les attaques DDOS


```
# Autoriser port 22,80 et 443
iptables -A INPUT -i eth0 -p tcp --dport 80,443,22 -j ACCEPT
iptables -A INPUT -i eth0 -j REJECT

# Anti FLOOD/DDOS
iptables -A INPUT -p tcp --syn -m limit --limit 1/second -j ACCEPT
iptables -A INPUT -p udp -m limit --limit 1/second -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/second -j ACCEPT
iptables -A INPUT -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT
```

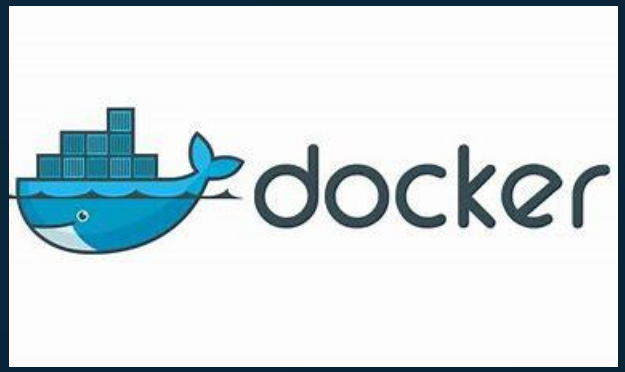
RENFORCER LA SÉCURITÉ AVEC FAIL2BAN

Fail2ban est un IPS et permet de bannir une IP temporairement lorsque plusieurs échecs d'authentification sont détectés

SÉPARER LES SERVICES DU SYSTÈME

Pour les services accessibles depuis le net, la bonne pratique est de les séparer du systèmes (éviter un FTP, Web, SQL sur le même système)

Aujourd'hui grace à la technologie de conteneur comme docker cela est tout à fait possible d'isoler les services du système principal.




MERCI


Linux