Haute Ecole Economique et Technique

Administration Système et Réseaux II

Rapport de sécurité

Groupe 2TL1-3

Romain Berger & Maxime De Cock

Risques encourus par le VPS

Les VPS d'OVH à notre (future) disposition ne seront protégés que par un simple mot de passe facilement crackable.
Il nous revient la responsabilité de les sécuriser rapidement afin de ne pas en perdre le contrôle, ce qui serait vraiment fâcheux.

Une fois la connexion sécurisée établie, nous n'aurons plus qu'à filtrer les tentatives d'accès avec Fail2Ban et notre VPS sera isolé de toute menace primaires.

Contre-mesures envisagées

- Mise à jour régulières du système
- Suppression de la connexion au VPS par mot de passe
- Suppression de la connexion au compte 'root'
- Authentification par Secure Shell (SSH)
- Modification du port d'écoute par défaut du service SSH
- Installation de Fail2Ban

Mesures mises en places

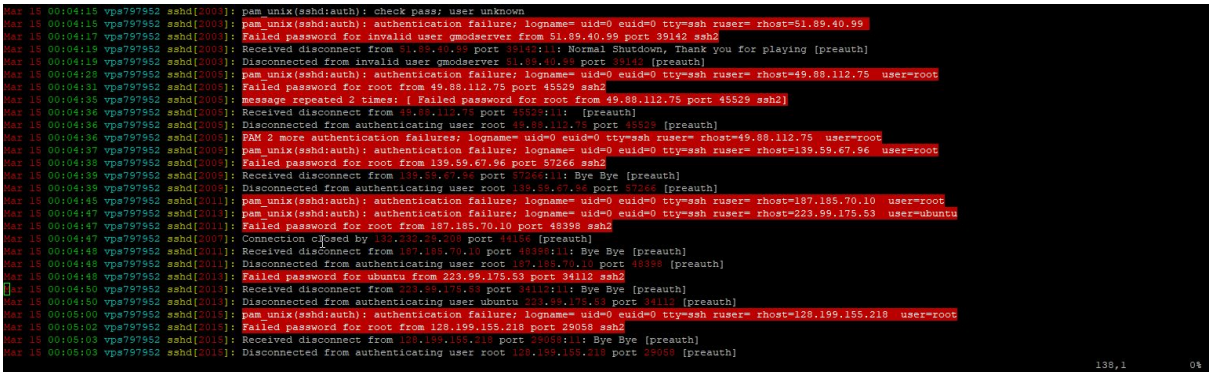
Utilisateurs et SSH

Avant tout chose, nous avons créé les différents users à savoir :

- *artyom (Romain Berger)*
- *maxime (Maxime De Cock)*
- *vvandens*

Ensuite nous avons généré les différentes clés publiques et privées et nous avons assigné la clé publique de chaque utilisateur dans son fichier ***authorized_keys****.*
Nous avons utilisé la norme de cryptage SSH-2 RSA avec une longueur de 2048 bits pour la génération des clés.

Une fois cela fait et la connection via tunnel sécurisé fonctionnel, nous avons désactivé l'authentification au root ainsi qu'aux utilisateurs via mot de passe.
Nous avons également changé le port SSH.
Malgré que certains articles et témoignages mentionnent l'inutilité de le changer nous l'avons tout de même fait car c'est toujours mieux d'avoir des logs de connexion "propres" de toutes tentatives futiles.*



*https://www.adayinthelifeof.nl/2012/03/12/why-putting-ssh-on-another-port-than-22-is-bad-idea/

Fail2Ban

Nous avons mis en place Fail2Ban avec une configuration assez simpliste :

```
[DEFAULT]
ignoreip = 127.0.0.1
findtime = 3600
bantime = 86400
maxretry = 3

[sshd]
enabled = true
port = 457
```

```
artyom@vps797952:/etc/fail2ban/jail.d$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```

Vérification de la configuration de fail2ban

LogRotate

Nous avons également mis en place logrotate qui permet l'archivage automatique des logs afin de limiter l'espace mémoire utilisé par les logs.
Voici un exemple avec fail2ban :

```
/var/log/fail2ban.log {
    weekly
    size 100M
    rotate 2
    compress
    delaycompress
    missingok
    postrotate
        fail2ban-client flushlogs 1>/dev/null
    endscript
}
```