Sécurité

En plus des règles de sécurité sur le firewall nous avons mis en place quelques règles de sécurité supplémentaires sur notre VPS.

I - Mettre à jour votre système d'exploitation

Les développeurs de distributions et de systèmes d’exploitation proposent de fréquentes mises à jour de paquets, très souvent pour des raisons de sécurité. Faire en sorte que votre distribution ou système d'exploitation est à jour est un point essentiel pour sécuriser votre VPS. Cette mise à jour passera par deux étapes .

La mise à jour de la liste des paquets : sudo apt update

La mise à jour des paquets à proprement parler : sudo apt upgrade

Cette opération doit être effectuée régulièrement afin de maintenir un système à jour.

II - Modifier le port d'écoute SSH par défaut

L'une des premières actions à effectuer sur votre serveur est la configuration du port d'écoute du service SSH. Par défaut, celui-ci est défini sur le port 22 donc les tentatives de hack du serveur par des robots vont cibler ce port en priorité. La modification de ce paramètre, au profit d'un port différent, est une mesure simple pour renforcer la protection de votre serveur contre les attaques automatisées.

Pour cela, modifiez le fichier de configuration du service avec l'éditeur de texte de votre choix (nano est utilisé dans cet exemple) :~$ sudo nano /etc/ssh/sshd\_config

Vous devriez trouver les lignes suivantes ou équivalentes :

# What ports, IPs and protocols we listen for

Port 22

Remplacez le nombre 22 par le numéro de port de votre choix (ici 50005). Veillez toutefois à ne pas renseigner un numéro de port déjà utilisé sur votre système. Pour plus de sécurité, il est recommandé d’utiliser un numéro entre 49152 et 65535.

III - Modifier le mot de passe associé à l'utilisateur "root"

Il est fortement recommandé de modifier le mot de passe de l'utilisateur root afin de ne pas le laisser à sa valeur par défaut sur un nouveau système. Pour cela :

Passwd

Puis renseigner le nouveau mot de passe.

IV - Créer un utilisateur avec des droits restreint

En général, les tâches qui ne requièrent pas de privilèges root doivent être effectuées via un utilisateur standard.

Vous pouvez créer un nouvel utilisateur avec la commande suivante :

sudo adduser NomUtilisateurPersonnalisé

Renseignez ensuite les informations demandées par le système : mot de passe, nom, etc. Le nouvel utilisateur sera autorisé à se connecter en SSH. Lors de l'établissement d'une connexion, utilisez les informations d'identification spécifiées. Une fois connecté, tapez la commande suivante pour effectuer des opérations nécessitant des autorisations root :su root

Dans notre cas nous avons créé l’utilisateur cookmaster.

V - Désactiver l'accès au serveur via l'utilisateur root

L'utilisateur root est créé par défaut sur les systèmes GNU/Linux. Il s'agit du niveau d'accès le plus élevé à un système d'exploitation .Il est déconseillé et même dangereux de laisser votre VPS accessible uniquement en root, car ce compte peut effectuer des opérations irréversiblement dommageables .Il est recommandé de désactiver l'accès direct des utilisateurs root via le protocole SSH.

**N'oubliez pas de créer un autre utilisateur avant de suivre les étapes ci-dessous.**

Vous devez modifier le fichier de configuration SSH de la même manière que décrit précédemment : sudo nano /etc/ssh/sshd\_config

Repérez la section suivante :

# Authentication:

LoginGraceTime 120

PermitRootLogin yes

StrictModes yes

Remplacez yes par no sur la ligne PermitRootLogin. Pour que cette modification soit prise en compte, vous devez redémarrer le service SSH :sudo systemctl restart sshd

Par la suite, les connexions à votre serveur via l'utilisateur root seront rejetées.

VI - Installer Fail2ban

Fail2ban est un framework de prévention contre les intrusions dont le but est de bloquer les adresses IP depuis lesquelles des bots ou des attaquants tentent de pénétrer dans votre système. Ce paquet est recommandé, voire indispensable dans certains cas, pour protéger votre serveur des attaques de types Brute Force ou Denial of Service.

Pour installer le package logiciel, utilisez la commande suivante : sudo apt install fail2ban

Vous pouvez personnaliser les fichiers de configuration Fail2ban pour protéger les services exposés à l'Internet public contre les tentatives de connexion répétées. Comme le recommande Fail2ban, créez un fichier de configuration local de vos services en copiant le fichier "jail" : sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Ouvrez ensuite le fichier avec un éditeur de texte :sudo nano /etc/fail2ban/jail.local

**Prenez soin de lire les informations en haut du fichier, notamment les commentaires sous [DEFAULT].**

Les paramètres [DEFAULT] sont globaux et s'appliqueront donc à tous les services définis pour être activés (enabled) dans ce fichier

Prenons pour exemple ces lignes sous [DEFAULT] :

bantime = 10m

maxretry = 5

enabled = false

Cela signifie qu'une adresse IP à partir de laquelle un hôte tente de se connecter sera bloquée pendant dix minutes après la cinquième tentative d'ouverture de session infructueuse.

De plus, tous les paramètres spécifiés par [DEFAULT] et dans les sections suivantes restent désactivés sauf si la ligne enabled = true est ajoutée pour un service (listée ci-dessous # JAILS).

À titre d’exemple d’utilisation, le fait d’avoir les lignes suivantes dans la section [sshd] activera des restrictions uniquement pour le service OpenSSH :

[sshd]

enabled = true

port = 50005

filter = sshd

maxretry = 3

findtime = 5m

bantime = 30m

Dans cet exemple, si une tentative de connexion SSH échoue trois fois en cinq minutes, la période d’interdiction des IP sera de 30 minutes. Vous pouvez remplacer "ssh" par le numéro de port réel si vous l'avez modifié. La meilleure approche consiste à activer Fail2ban uniquement pour les services qui sont réellement exécutés sur le serveur.

VII - Sauvegarder votre système et vos données

Le concept de sécurité ne se limite pas à la protection d'un système contre les attaques.

La sécurisation de vos données est un élément clé, c'est pourquoi nous mettons en place régulièrement des snapshots du VPS en question.