TP n’9 : IDS : IPS

Introduction à FAIL2BAN

CONFIGURATION D’UN IPS /

1. A faire pour préparer le TP

Failban peut être installé sur le serveur rsyslog (apt install fail2ban)

Verifier que ssh est opérationnel

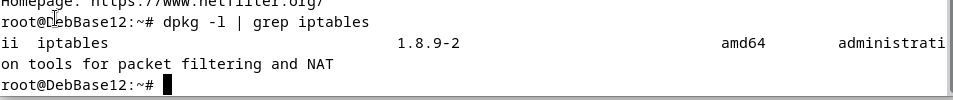
Paquet ssh installe

Connexion depuis la machine physique vers la machine virtuelle -> reussi mais pas l’inverse

Dans quels fichiers sont stockés les logs ?



Verifier si iptables est installé



1. Qu’est ce que FAIL2BAN

a)Architecture de l’application

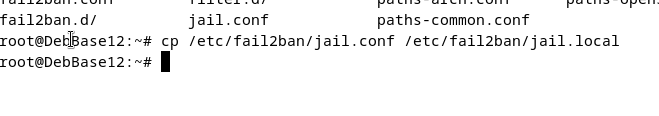
**/etc/fail2ban/**

**C) Personnaliser Fail2ban**

**Copie du fichier fail2ban.conf en .local**



**Copie du fichier jail.conf en .local**



b) Fichiers de configuration de Fail2ban

III.Parametrage du servuer

Mettre le temps de bannissement à 60 secondes,

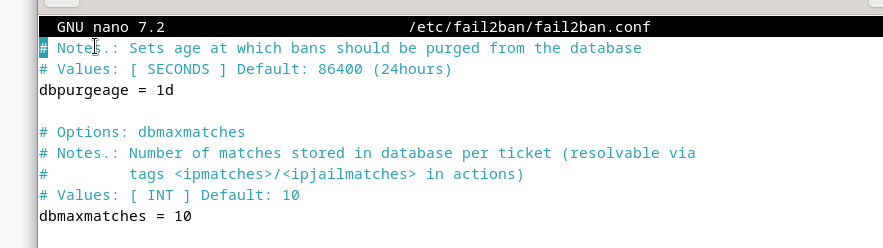
Le nomre maximum tentatives échoués ) 3

Redemarrer le service après le changement

Configuration du fichier jail

Dbpurgeage = le temps de banissement

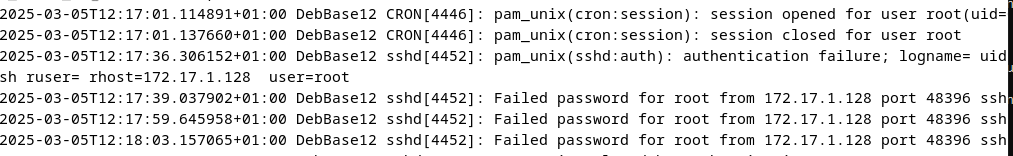
Dbmaxmatches = le nbr de tentatives



1. Identifier les lignes de logs qui traduisent une erreur de co

Logs pour verifier les tentatives de connexion :

Tail –f /var/log/auth.log

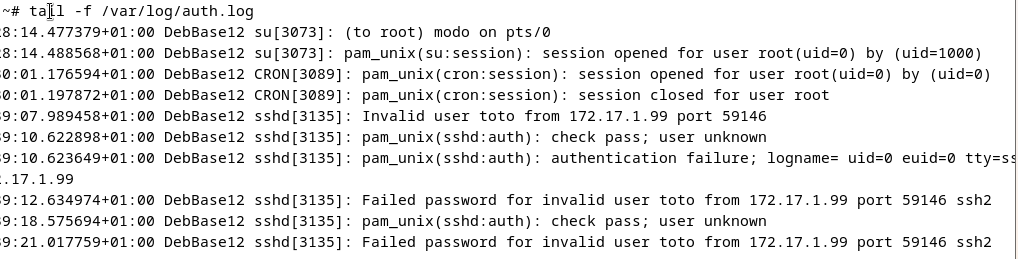


III.Parametrage du serveur

1. Identifier les lignes qui traduisent une erreur de connexion

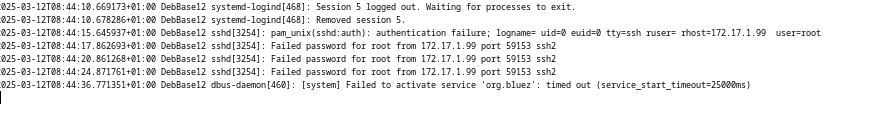
**Afficher les tentatives de connexion grâce à tail –f /var/log/auth.log**

Tentative de connexion avec un mauvais utilisateur

1. 

\

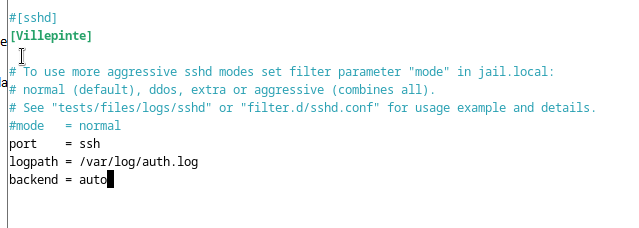
Tentative de connexion avec un bon utilisateur mais un mauvais de mot de passe



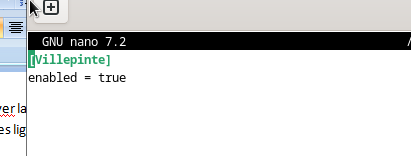
Creation d’une nouvelle prison (jail) :

5) Desactiver la prison sshd qui se trouve jail.local en commentant

6) Copier les lignes suivantes dans jail ?local agfin d’avoir le squelette de configuration



7) Activer votre prison dans un fichier

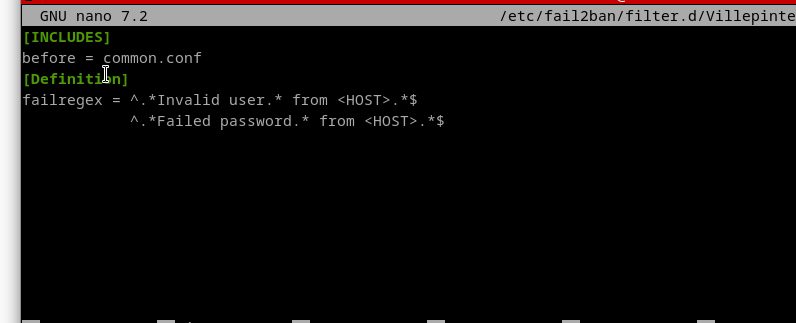


Puis redemarrez le service : systemctl restart fail2ban

C) Creation du filtre

8)Definir une expression régulière permettant de rejeter les hotes ayant fait une tentative de connexion

Ecrire une expression reguliere dans le fichier filter.d/villepinte.local



**Commande pour tester le filtre :**



