

TP Netfilter

Le plus important dans ce TP est de définir une procédure de tests pour chaque exercice. Des tests inappropriés ou insuffisants peuvent vous faire croire que vous avez obtenu le résultat attendu alors qu'il n'en est rien.

1 Exercice 1 : ping

Le poste de travail ne peut que "pinguer" les machines du réseau. Il peut être "pingué" lui-même.

1. Effacez toutes les règles qui pourraient exister
2. Définissez vos stratégies par défaut (vous les conserverez pendant tout le TP)
3. Écrivez les règles correspondantes
4. Testez

2 Exercice 2 : surf

Le poste de travail peut seulement surfer sur le web, il ne peut pas pinguer ni être pingué

1. Effacez les règles précédentes
2. Écrivez les règles correspondantes
3. Testez

3 Exercice 3 : serveur

Maintenant le poste de travail devient serveur web exclusivement. Il ne peut rien faire d'autre.

1. Effacez les règles précédentes
2. Vérifiez que l'on peut se connecter sur le poste de travail par ssh
3. Vérifiez que l'on peut se connecter sur le poste de travail sur un serveur web (au besoin installez-le)
4. Ecrivez les règles correspondantes
5. Testez

4 Exercice 4 : prévenir le "Deny of Service"

Le DoS est une attaque qui consiste à noyer une machine sous une avalanche de paquets dans le but de la mettre à genoux. Une parade est de limiter certains trafic. Essayez de limiter les "ping".

5 Exercice 5 : "logger"

Enregistrez dans le journal les pings reçus (le journal est dans /var/log/message, vous le visualisez facilement avec tail ou mieux tail -f). Vous pouvez limiter la fréquence.