

Firewall : iptables

1. Désactivez firewalld et installez iptables-services
2. Affichez les règles du firewall, ensuite supprimez les règles préexistantes.
 - Affichez toutes les règles des tables de votre FW.
 - Affichez toutes les règles de la chaîne OUTPUT de la table filter
 - Effacez toutes les règles de la chaîne INPUT.
3. Listez les ports ouverts d'une machine (**nmap**)
4. Sauvegarder et charger une configuration (**iptables-save** et **iptables-restore**)
5. Créez les règles suivantes
 - Ajoutez la règle OUTPUT -j DROP (Appelez ensuite le professeur)
 - Autorisez le sous-réseau 10.1.0.0/16 à envoyer des informations à votre machine
 - Autorisez tout sauf l'hôte 10.1.10.1 à envoyer des informations à votre dans la machine
 - Refuser les pings en entrée
 - Acceptez les données envoyées par un site web et un ftp
 - Interdisez l'adresse MAC d'un ordinateur de la classe en entrée.
6. Créez une nouvelle chaîne ayant une règle qui accepte toutes les connexions de la localloop. Testez la règle, ensuite supprimez la chaîne créée.
<https://www.tutos.eu/5686>
7. Ecrivez un script pour votre FW tel que :
 - Celui-ci doit être démarré pour les cibles graphique multi-users et non graphique multi-user.
 - Il accepte uniquement les pings provenant de votre réseau local