TP 7 : Parfeu linux : Iptables

1. Vérifier l'existence du parfeu linux
2. Consulter le manuel de iptables
3. Quelles sont les tables contenues dans iptables. C'est quoi le rôle de chacune des tables ?
4. Que fait l'option –L d'iptables ?
5. Que fait la commande : **iptables –L -n –v**
6. Que fait la commande **iptables -t nat -L**
7. Faites un ping du dns google (8.8.8.8 et 8.8.4.4)
8. Que fait la commande **iptables –I INPUT -s 8.8.8.8 -j DROP . il y a aussi 8.8.4.4**
9. Refaire le ping du dns google. Qu'est ce que vous remarquez ?
10. On veut cette fois bloquer le trafic local sortant vers l'adresse IP 8.8.8.8
11. Faites un ping de google.com
12. Pour trouver l'adresse IP du dns utilisé, il suffit de taper la commande :
    a. grep "nameserver" /etc/resolv.conf
    b. Vous aurez par exemple : nameserver 109.78.164.20 (dans ce cas l'ip du serveur DNS est 109.78.164.20)
13. Bloquez le traffic sortant vers cette adresse IP du DNS ensuite refaites le ping du google.com. Qu'est ce que vous remarquez ?
14. Que retourne la commande :
    nc -vvv -z -w 3 172.217.171.206 80 (avec 172.217.171.206 est l'adresse ip du serveur google)
15. Bloquer le port 80 en sortant sur le protocole TCP, sur l'interface eth0 et à destination de l'adresse IP de Google, avec la commande :

iptables -I OUTPUT -o eth0 -d 172.217.171.206 -p tcp --dport 80 -j DROP

(on suppose que l'interface réseau utilisée est eth0, utilisez la votre)

16. Retapez la commande nc de la question 14. Qu'est-ce que vous remarquez ?
17. On remplace cette fois DROP de la question 15 par REJECT
18. Retapez la commande nc de la question 14. Qu'est-ce que vous remarquez cette fois ?
19. Expliquez les commandes :
    a. **iptables -A INPUT -i eth0 -p tcp -m multiport --dports 80,443 -j DROP** (443 port de https)
    b. **iptables -A INPUT -p tcp -m iprange --src-range 192.168.1.13-192.168.2.19 –j DROP**

Commandes supplémentaires :

20. Limiter le syn-Flood à une seconde. Le SYN flood est une forme d'attaque par déni de service dans laquelle un attaquant initie rapidement une connexion à un serveur sans finaliser la connexion. Le serveur doit dépenser des ressources en attente de connexions à moitié ouvertes, ce qui peut consommer suffisamment de ressources.
    Exemple : Limiter le nombre de connexions sortantes vers le port 80 à 4 IP avec la commande :
    iptables -A INPUT -p tcp --syn --dport http -m connlimit --connlimit-above 4 -j REJECT.

21. Jouer sur la taille des paquets avec length, pour limiter les paquets ICMP supérieurs à 1000 octets :

a. iptables -A INPUT -p icmp --icmp-type echo-request -m length --length 1000:0xffff -j DROP