The Search for a Title

Travaux Pratiques

Axel LE BOT | Andrew LENC

Table des matières

Réseau

1. TP1

2. TP2

3. TP3

4. TP5

4.1 Exercice 3

4.1.1 1.

C'est possible avec l'option "-m limit –limit 1/h"

4.1.2 2.

–match permet aussi de faire correspondre d'autre éléments, comme l'adresse IP de la source, donc oui.

4.1.3 3.

–match permet de vérifier le port source aussi.

4.1.4 4.

-A INPUT -p tcp -m tcp –dport 22 -j LOGDROP Applique la police logdrop aux paquets tcp à destination du port 22. -A INPUT -p tcp -m tcp –dport 3389 -j DROP Applique la police drop aux paquets tcp à destination du port 3389. -A LGRDP -p tcp -m limit –limit 5/min -j LOG –log-prefix "Denied RDP : " –log-level 7 S'il y a plus de 5 paquets TCP, on enregistre l'essai en notant avant "Denied RDP : " -A LGRDP -j drop -A LOGDROP -p tcp -m tcp –dport 22 -m state –state NEW -m recent –set –name SSH –rsource -A LOGDROP -p tcp -m tcp –dport 22 -m state –state NEW -m recent –update – seconds 60 –hitcount4 –name SSH –rsource -j LOG –log-prefix "SSH SCAN blocked :" –log-level 6

Le port knocking consiste à envoyer des requêtes sur certains ports dans le bon ordre afin de modifier un pare-feu distant depuis l'extérieur.

II Autres

4.2 Figure

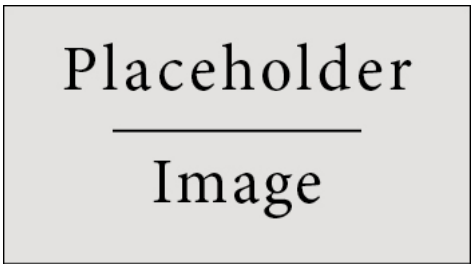

FIGURE 4.1 – Figure caption

Bibliography

Index

F