



The Search for a Title

Travaux Pratiques

Axel LE BOT | Andrew LENC



Copyright © 2017-2018 Axel LE BOT

Licensed under the Creative Commons Attribution-NonCommercial 3.0 Unported License (the “License”). You may not use this file except in compliance with the License. You may obtain a copy of the License at <http://creativecommons.org/licenses/by-nc/3.0>. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.



Table des matières

I	Réseau	
1	TP1	7
2	TP2	9
3	TP3	11
4	TP5	13
4.1	Exercice 3	13
4.1.1	1.	13
4.1.2	2.	13
4.1.3	3.	13
4.1.4	4.	13
II	Autres	
4.2	Figure	17
	Bibliography	19
	Books	19
	Articles	19
	Index	21



Réseau

1	TP1	7
2	TP2	9
3	TP3	11
4	TP5	13
4.1	Exercice 3	

A photograph of a computer lab with multiple rows of desktop computers. Each workstation includes a monitor, a keyboard, and a mouse. The image is taken from a low angle, looking down the length of the desk. A semi-transparent blue overlay covers the bottom half of the image. In the upper part of this overlay, the text "1. TP1" is displayed in white, enclosed within a thin orange rounded rectangular border.

1. TP1



2. TP2

A photograph of a computer lab with multiple rows of desktop computers. Each workstation includes a monitor, a keyboard, and a mouse. The image is overlaid with a semi-transparent blue gradient that covers the bottom two-thirds of the frame. In the upper part of the blue area, the text '3. TP3' is displayed in white, enclosed within a thin orange rounded rectangular border.

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'autres éléments, comme l'adresse IP de la source, donc oui.

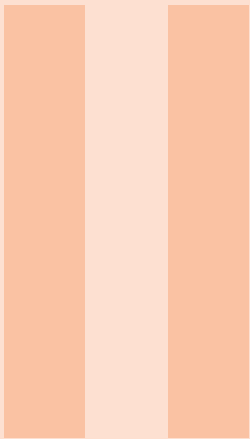
4.1.3 3.

-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.



Autres

4.2 Figure

Bibliography 19
Books
Articles

Index 21

4.2 Figure

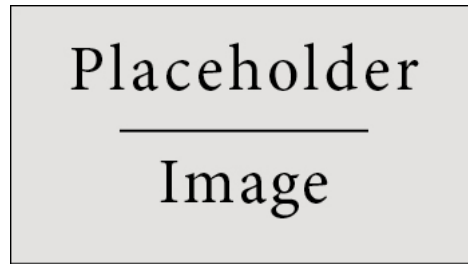


FIGURE 4.1 – Figure caption



Bibliography

Books

Articles



Index

F

Figure 17