TD3 CLIENTS /SERVEUR et notions associées

1 ) Technologie RAID

3 disque :

-160 GO

-100 Mo /s par disque en lecture

-80 Mo /s par disque en écriture

1. Pour RAID 0

50000 /3 = 16 666,66 par disque

16 666,66 / 80 = 208,33 second

Pour RAID 1

50 000 / 80 = 625 second

1. Pour RAID 0

50000 /3 = 16 666,66 par disque

16 666,66 / 60 = 277,776 second

Pour RAID 1

50 000 / 60 = 833,33 second

1. Pour RAID 0

160000000 / 50 = 3200000 fichier

3200000 \* 3 = 9600000 fichier

Pour RAID 1

160000000 / 50 = 3200000 fichier

1. Pour RAID 0

160000000 / 50 = 3 200 000 fichier

100000000 / 50 = 2 000 000 fichier

40000000 / 50 = 800 000 fichier

Addition des 3 = 6 000 000

Pour RAID 1

40000000 / 50 = 800 000 fichier

1. Raid 3

(160 \* 10^9 \*2) / 50\*10^3 = 6 400 000 Fichier

Raid 3

(40 \* 10^9 \*2) / 50\*10^3 = 1 600 000 Fichier

1. 25 \* 1000\*1000 / 80 = 312,5s et 625 s au total

2) Firewall IPTables

2.1)

a) iptables –A INPUT –p icmp –j DROP\_LOG

-t table (filter par défaut)

-A ajouter une règle à la fin d’une chaîne (chaîne : INPUT, OUTPUT, FORWARD)

-P définir une politique par défaut pour une chaîne

-j actions à prendre si un paquet répond aux critères de la règle : ACCEPT, REJECT, DROP, LOG

Dans la table en entrer et avec la politique ICMP on effectue l’action DROP\_LOG

b) –s adresse IP source à vérifier

Dans la table avec comme entrer une adresse IP à vérifier on effectue l’action de la REJECT

c) –i interface physique d’entrée

Dans la table avec comme entrer la politique TCP avec comme interface physique ETH0 on effectue l’action ACCEPT

–o interface physique de sortie

Dans la table avec comme Sortie la politique TCP avec comme interface physique de sortie ETH0 on effectue l’action ACCEPT

d) --dport port destination

Dans la table avec comme entrer le port destination 1024 :65535 on effectue l’action LOG

e) -- sport port source

Dans la table avec comme entrer la politique UDP le port destination 53 on effectue l’action ACCEPT

Dans la table avec comme sortie la politique UDP le port source 53 on effectue l’action ACCEPT

f) Dans la table avec comme sortie la politique UDP le port destination 53 on effectue l’action ACCEPT

Dans la table avec comme Entrer la politique UDP le port source 53 on effectue l’action ACCEPT

2.2)

A)

iptables –A FORWARD –I ETH1 –O ETH2 -J ACCEPT

iptables –A FORWARD –I ETH2 –O ETH1 -J ACCEPT

OU

IPTABLES –A FORWARD –S 192.168.2.0 –O ETH2 -J ACCEPT

B)

iptables –a FORWARD –s 192.168.2.0 /24 –p TCP -O eth0 –dport 80 -J ACCEPT

iptables –a FORWARD –d 192.168.2.0 /24 –p TCP –I eth0 –sport 80 -J ACCEPT

c)

iptables –p forward drop \_ log

3) Détection d’intrusions : SNORT

3.1)a) Alert

B) C) Si n’importe qui au port 80 touche a CGI-bin:PHF on lui dit le msg

D) si des machines de mon réseau reçoive du contenu pour adulte on bloque

3.2)

a) alert udp any 7 <=> 135.58.0.0/16 19 (msg:”spoof”; react: block;)

b) alert tcp any 22 -> any any (msg:”stop”; content:” USER root”;nocase;react)

c) alert tcp any 7 -> 135 58 0 0/16 any (msg:” a couvers SMURFING“; threshold: seconds 1, count 3, type: both;)

d) alert tcp 135.58.0.0/16 any ⬄ any any( flags:R ; msg :”msg RST”;)

e) alert tcp any any -> 135.58.0.0/16 qny ( flags : A; ack;