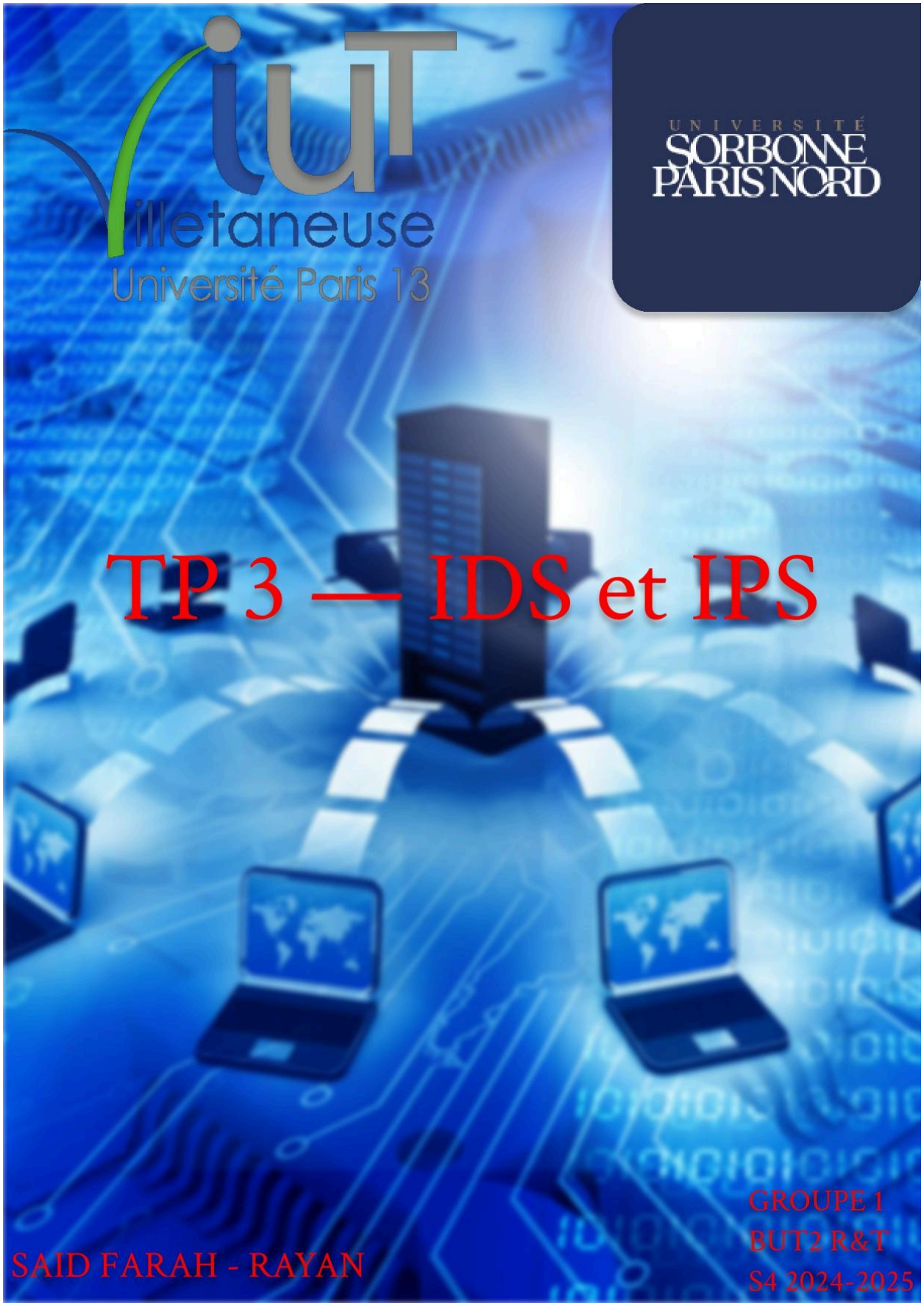


TP 3 — IDS et IPS

SAID FARAH - RAYAN

GROUPE 1
BUT2 R&T
S4 2024-2025

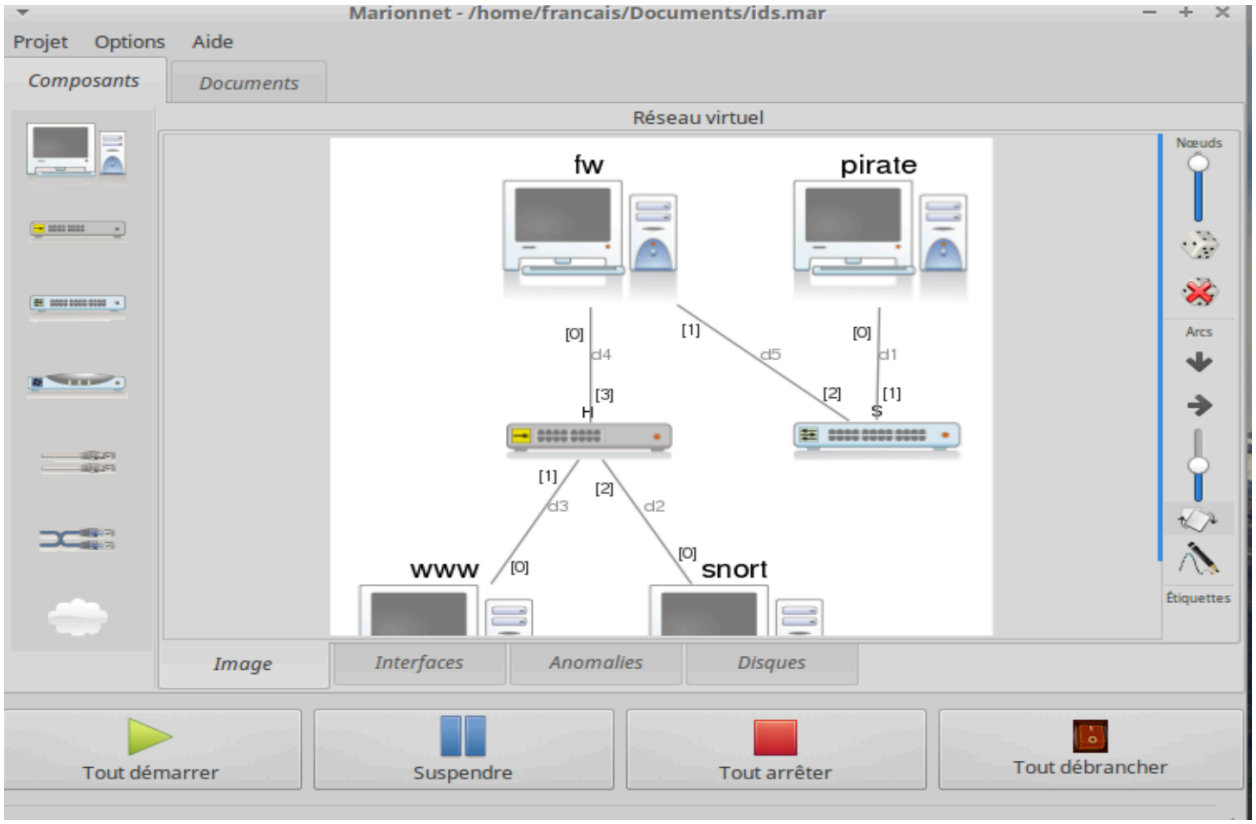
Table des matières

Exercice 1 — Configuration des interfaces et routes

I1.1 Téléchargez le projet à l'adresse https://lipn.univ-paris13.fr/~evangelista/cours/R401/ids.mar.

```
francais@ubuntu1604:~/Documents$ wget https://lipn.univ-paris13.fr/~evangelista/
cours/R401/ids.mar
--2025-03-09 16:50:08--  https://lipn.univ-paris13.fr/~evangelista/cours/R401/id
s.mar
Résolution de lipn.univ-paris13.fr (lipn.univ-paris13.fr)… 194.254.163.36
Connexion à lipn.univ-paris13.fr (lipn.univ-paris13.fr)|194.254.163.36|:443… con
necté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 12127742 (12M)
Enregistre : «ids.mar»

ids.mar             100%[===================>]  11,57M  27,2MB/s    ds 0,4s

2025-03-09 16:50:09 (27,2 MB/s) - «ids.mar» enregistré [12127742/12127742]

francais@ubuntu1604:~/Documents$ ls
ids.mar  TP2.mar
francais@ubuntu1604:~/Documents$
```

I 1.2 Ouvrez le projet dans marionnet et démarrez tous les équipements.



I 1.3 Attribuez des IP à fw(eth0), snort et www sur le réseau 10.0.0.0/24.

www (debian-wheezy-08367)

```
  GNU nano 2.2.6          File: /etc/network/interface

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

iface eth0 inet static
        address 10.0.0.1
        netmask 255.255.255.0
        gateway 10.0.0.254
```

snort (debian-wheezy-08367)

```
  GNU nano 2.2.6          File: /etc/network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

iface eth0 inet static
        address 10.0.0.2
        netmask 255.255.255.0
        gateway 10.0.0.254
```

fw (debian-wheezy-08367)

```
 GNU nano 2.2.6          File: /etc/network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

iface eth0 inet static
        address 10.0.0.254
        netmask 255.255.255.0

iface eth1 inet static
        address 1.2.3.254
        netmask 255.255.255.0
```

I 1.4 Attribuez des IP à pirate et fw(eth1) sur le réseau 1.2.3.0/24.

pirate (debian-wheezy-08367)

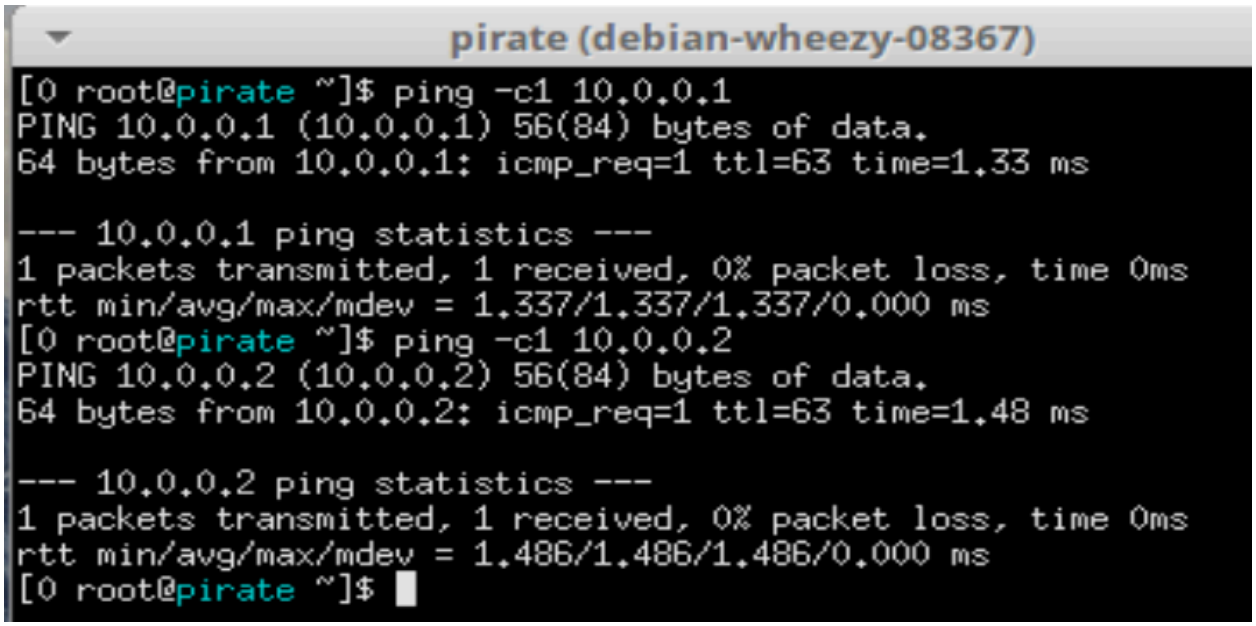
```
 GNU nano 2.2.6          File: /etc/network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

iface eth0 inet static
        address 1.2.3.1
        netmask 255.255.255.0
        gateway 1.2.3.254
```

I 1.5 Sur pirate, www et snort : ajoutez une route par défaut.

I 1.6 Sur fw : modifiez le paramètre système net.ipv4.ip_forward pour que fw accepte de router les paquets.

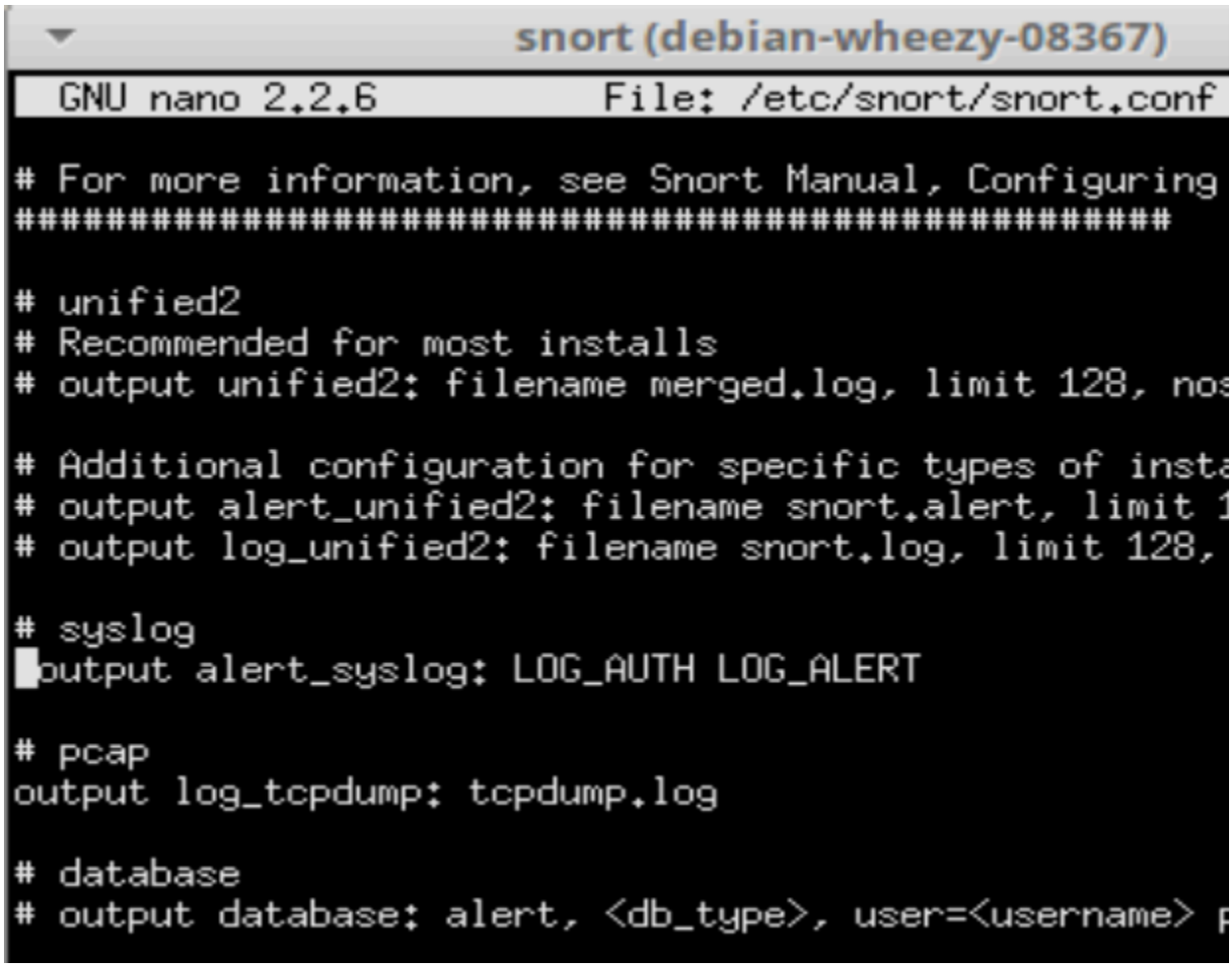
```
[0 root@fw ~]$ sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[0 root@fw ~]$
```

I 1.7 Vérifiez que les pings passent entre les hôtes pirate et www et entre pirate et snort.

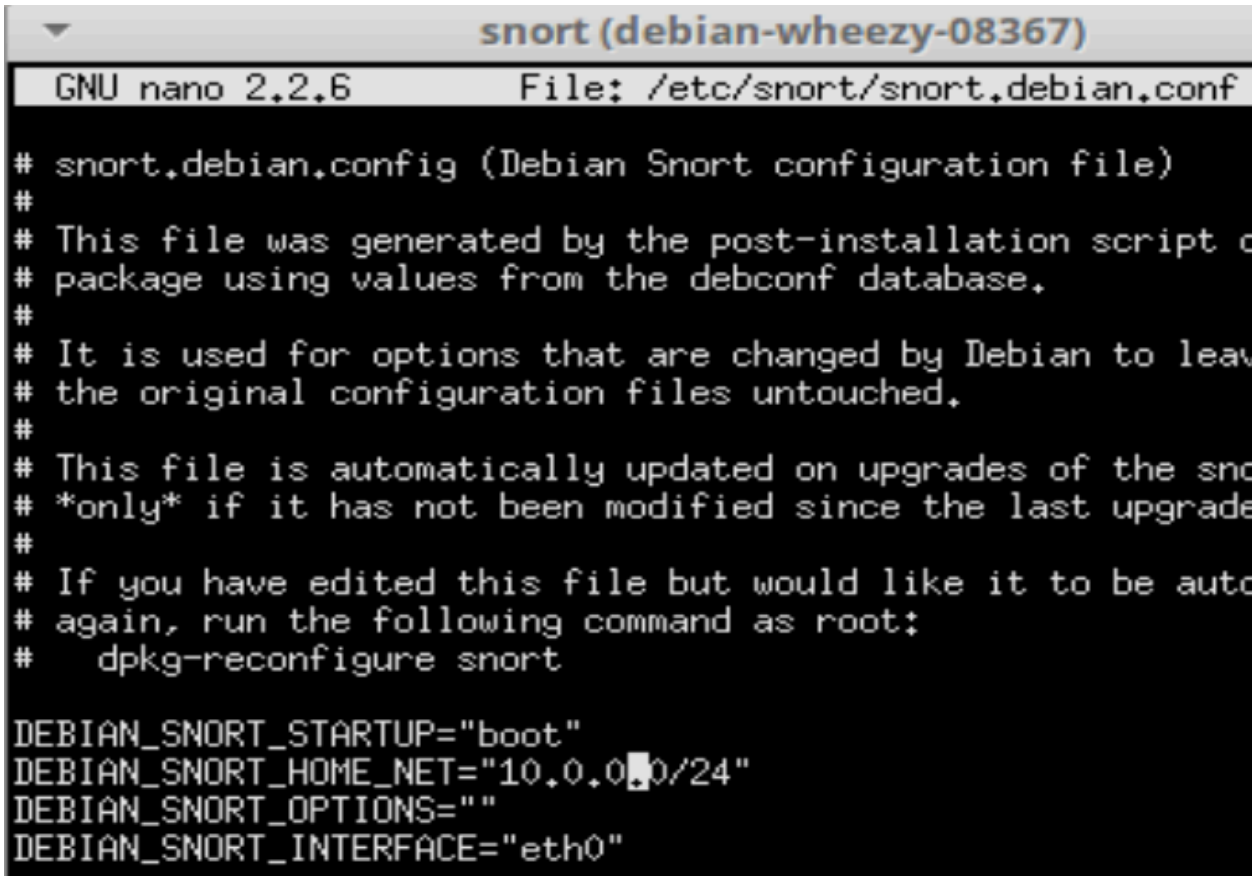

pirate (debian-wheezy-08367)
[0 root@pirate ~]$ ping -c1 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_req=1 ttl=63 time=1.33 ms
--- 10.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.337/1.337/1.337/0.000 ms
[0 root@pirate ~]$ ping -c1 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_req=1 ttl=63 time=1.48 ms
--- 10.0.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.486/1.486/1.486/0.000 ms
[0 root@pirate ~]$

Exercice 2 — Prise en main de snort

I 2.1 Décommenter la ligne commençant par # output alert_syslog dans le fichier snort.conf.



I 2.2 Dans /etc/snort/snort.debian.conf, modifiez la valeur du paramètre DEBIAN_SNORT_HOME_NET.



I 2.3 Démarrez les services snort et rsyslog sur snort.

I 2.4 Sur pirate : envoyez, avec nmap, un balayage XMAS vers le port 20 de www. (snort est installé avec de nombreuses règles qui permettent, entre autres, de détecter certains balayages nmap.)

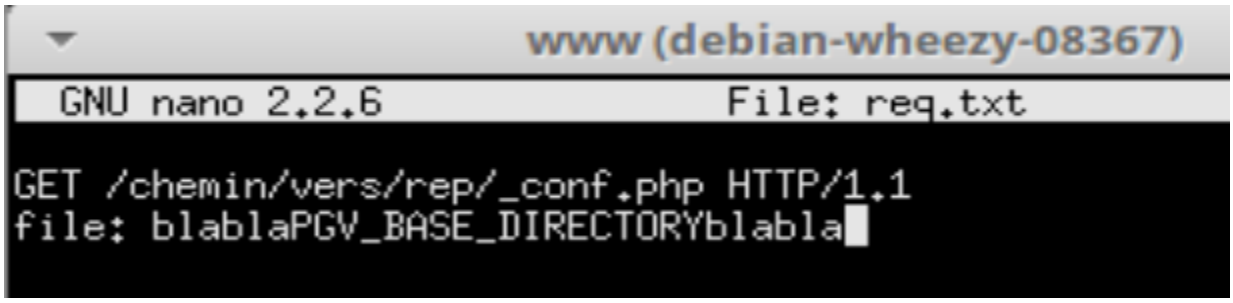
```
pirate (debian-wheezy-08367)
[0 root@pirate ~]$ nmap -sX -p 20 10.0.0.1

Starting Nmap 6.00 ( http://nmap.org ) at 2025-03-09 17:12 UTC
Nmap scan report for 10.0.0.1
Host is up (0.0028s latency).
PORT   STATE  SERVICE
20/tcp closed ftp-data

Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds
[0 root@pirate ~]$
```

I 2.5 Vérifiez que l'alerte est présente dans le fichier /var/log/auth.log : le mot XMAS devrait y apparaître.

```
snort (debian-wheezy-08367)
[0 root@snort ~]$ cat /var/log/auth.log
Mar  9 17:12:56 snort snort[1773]: [1:469:3] ICMP PING NMAP [Classification: Att
empted Information Leak] [Priority: 2] {ICMP} 1.2.3.1 -> 10.0.0.1
Mar  9 17:12:56 snort snort[1773]: [1:384:5] ICMP PING [Classification: Misc act
ivity] [Priority: 3] {ICMP} 1.2.3.1 -> 10.0.0.1
Mar  9 17:12:56 snort snort[1773]: [1:453:5] ICMP Timestamp Request [Classificat
ion: Misc activity] [Priority: 3] {ICMP} 1.2.3.1 -> 10.0.0.1
Mar  9 17:13:09 snort snort[1773]: [1:1228:7] SCAN nmap XMAS [Classification: At
tempted Information Leak] [Priority: 2] {TCP} 1.2.3.1:46561 -> 10.0.0.1:20
[0 root@snort ~]$
```

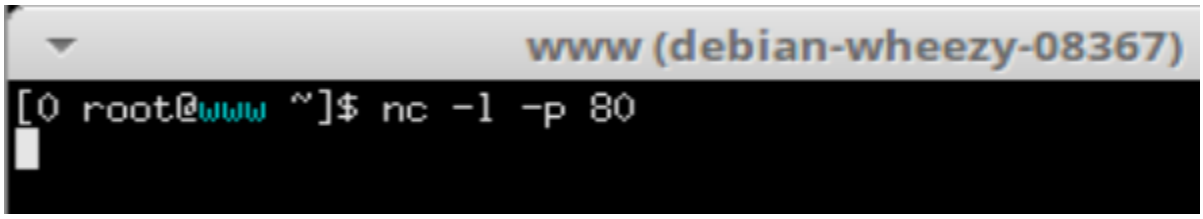
I 2.6 Éditez le fichier req.txt pour avoir le contenu ci-dessus. (N'oubliez pas la ligne vide en fin de fichier pour que la requête soit bien formée.)

```
pirate (debian-wheezy-08367)
 GNU nano 2.2.6                File: req.txt

GET /chemin/vers/rep/_conf.php HTTP/1.1
file: blablaPGV_BASE_DIRECTORYblabla

```



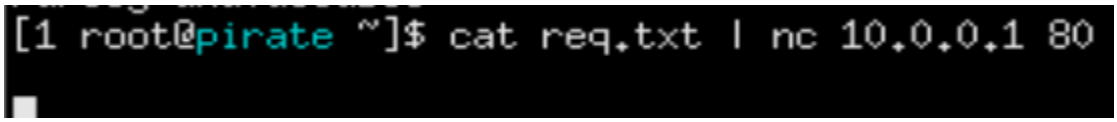
I 2.7 Sur www, démarrez un serveur TCP sur le port 80 :

$ nc -l -p 80

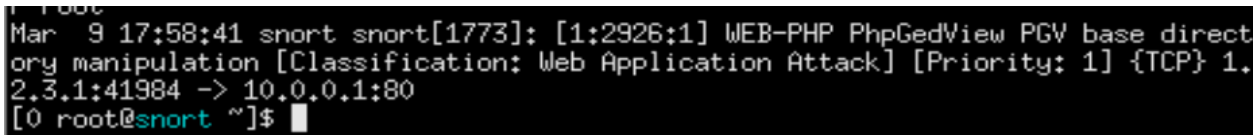


I 2.8 Sur pirate, envoyez la requête sur le port 80 de www :

$ cat req.txt | nc @ip -de -www 80



I 2.9 Vérifiez que le journal de snort contient bien une nouvelle ligne contenant le message Web-PHP ....



I 2.10 En suivant la même procédure, générez une alerte pour l'identifiant de signature 100000691.

On retrouve cette signature dans le fichier community-sql-injection.rules :

```
pirate (debian-wheezy-08367)
 GNU nano 2.2.6                File: req2.txt

GET /category.php?id=1' UNION SELECT * FROM admin-- HTTP/1.1
file: blablaPGV_bASE_DIRECTORYblabla
```

```
Mar  9 18:32:25 snort snort[1773]: [1:10000745:1] COMMUNITY WEB-PHP Diesel Joke
 Site category.php SQL injection attempt [Classification: Web Application Attack
] [Priority: 1] {TCP} 1.2.3.1:41990 -> 10.0.0.1:80
[0 root@snort /etc/snort/rules]$
```

Exercice 3 – Prise en main de fail2ban

I 3.1 Arrêtez le service fail2ban sur fw.

```
fw (debian-wheezy-08367)
[0 root@fw ~]$ service fail2ban stop
[ ok ] Stopping authentication failure monitor: fail2ban.
[0 root@fw ~]$
```

I 3.2 Démarrez les service ssh et rsyslog sur fw.

```
[0 root@fw ~]$ service ssh start
[ ok ] Starting OpenBSD Secure Shell server: sshd.
[0 root@fw ~]$ service rsyslog start
[ ok ] Starting enhanced syslogd: rsyslogd.
[0 root@fw ~]$
```

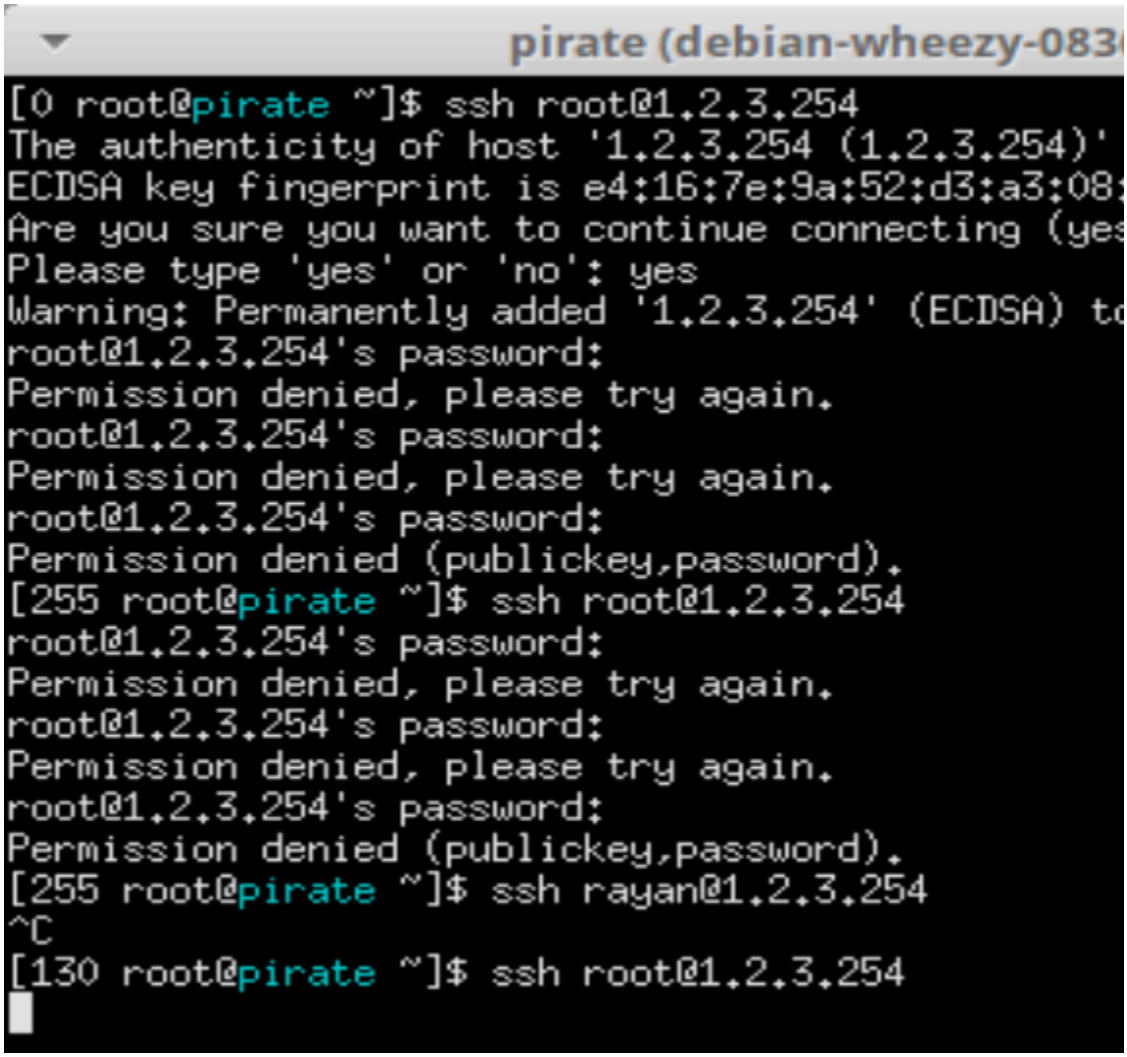
I 3.3 Démarrez le service fail2ban sur fw.

```
[0 root@fw ~]$ service fail2ban start
[ ok ] Starting authentication failure monitor: fail2ban.
[0 root@fw ~]$
```

I 3.4 Affichez de nouveau le contenu de la table filter sur fw..

```
[0 root@fw ~]$ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-ssh  tcp  --  anywhere             anywhere            multiport dport
s ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain fail2ban-ssh (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
[0 root@fw ~]$
```

I 3.5 Sur pirate : lancez successivement 6 tentatives de connexion ssh sur fw avec un login ou un mot de passe incorrect.



Lors de la 6 ième tentative, ssh devrait se bloquer car fail2ban aura alors bloqué l'adresse IP de pirate.

I 3.6 Vérifiez, sur fw, qu'une règle iptables a bien été ajoutée dans la chaîne créée par fail2ban.

```
[0 root@fw ~]$ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-ssh  tcp  --  anywhere             anywhere             multiport dport
s ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain fail2ban-ssh (1 references)
target     prot opt source               destination
DROP       all  --  1.2.3.1              anywhere
RETURN     all  --  anywhere             anywhere
[0 root@fw ~]$
```

I 3.7 Dans 10 minutes vous vérifierez que la règle a été retirée par fail2ban.

Q 3.1 En consultant les fichiers jail.conf et iptables-multiport.conf donnez la commande exécutée pour la geôle ssh lors du bannissement d'un hôte d'IP A.B.C.D. Pour cela, remplacez les paramètres par leurs valeurs effectives. Décrire l'effet de cette commande.

La commande exécutée pour bannir un hôte d'IP A.B.C.D dans la geôle SSH est définie dans le fichier iptables-multiport.conf. Cette commande est générée en remplaçant les paramètres de la variable actionban par les valeurs spécifiées dans la geôle SSH du fichier jail.conf. La commande finale est : iptables -I INPUT -p tcp -m multiport --dports ssh -j DROP -s A.B.C.D. Cette commande ajoute une règle iptables pour bloquer toutes les connexions TCP entrantes sur le port SSH (port 22) provenant de l'adresse IP A.B.C.D. L'option -I INPUT insère la règle en tête de la chaîne INPUT, et l'option -j DROP supprime les paquets correspondants sans envoyer de réponse à l'hôte.

Q 3.2 Même question pour la sortie d'un hôte d'IP A.B.C.D de la geôle.

La commande exécutée pour lever le bannissement d'un hôte d'IP A.B.C.D est définie dans la variable actionunban du fichier iptables-multiport.conf. La commande finale est : iptables -D INPUT -p tcp -m multiport --dports ssh -j DROP -s A.B.C.D. Cette commande supprime la règle iptables qui bloquait les connexions TCP entrantes sur le port SSH (port 22) provenant de l'adresse IP A.B.C.D. L'option -D INPUT supprime la règle correspondante de la chaîne INPUT.

Q 3.3 En analysant les motifs contenus dans le fichier /etc/fail2ban/filter.d/sshd.conf et en les comparant au contenu du fichier /var/log/auth.log, trouvez dans le journal les lignes qui ont mené au bannissement.

Les motifs à rechercher pour la geôle SSH sont définis dans le fichier /etc/fail2ban/filter.d/sshd.conf. Ces motifs, sous forme d'expressions régulières, correspondent à des échecs d'authentification SSH. Par exemple, un motif courant est : ^%(__prefix_line)s(?:error: PAM:)?Authentication failure for .* from <HOST>$. Fail2ban analyse le fichier /var/log/auth.log pour trouver des lignes correspondant à ces motifs. Lorsqu'une ligne de log correspond à un motif, Fail2ban incrémente un compteur pour l'adresse IP concernée. Si le nombre d'échecs atteint maxretry (défini dans la geôle SSH), Fail2ban exécute l'action de bannissement. Par exemple, des lignes de log comme Failed password for invalid user admin from A.B.C.D port 12345 ssh2 peuvent déclencher le bannissement après plusieurs occurrences.

Exercice 4 — Filtrage dynamique

I 4.1 Sur snort : ajoutez dans le fichier /etc/snort/rules/local.rules une règle snort permettant de lever une alerte en cas de requête DELETE sur un fichier du répertoire /upload/files. Vous utiliserez un message (propriété msg de votre règle snort) permettant de décrire précisément l'attaque afin qu'il puisse être facilement reconnu par fail2ban. Vous donnerez à votre signature un identifiant (propriété sid) compris entre 106 et 108. Cet intervalle est celui dans lequel les utilisateurs de snort peuvent choisir leurs identifiants.

on ajoute cette règle dans le fichier local.rules :

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"HTTP DELETE attempt on /upload/files"; flow:to_server,established; content:"DELETE"; http_method; content:"/upload/files"; http_uri; sid:1000077; rev:1;)

Puis on redémarre le service snort :

```
[0 root@snort /etc/snort]$ service snort restart
```

I 4.2 Sur pirate : envoyez une requête permettant de générer l'alerte.

```
pirate (debian-wheezy-08367)
 GNU nano 2.2.6                File: req3.txt

DELETE /upload/files/fichier_test HTTP/1.1
file: blablaPGV_bASE_DIRECTORYblabla
```

I 4.3 Sur snort : vérifiez qu'une alerte a effectivement été générée dans le fichier /var/log/auth.log.

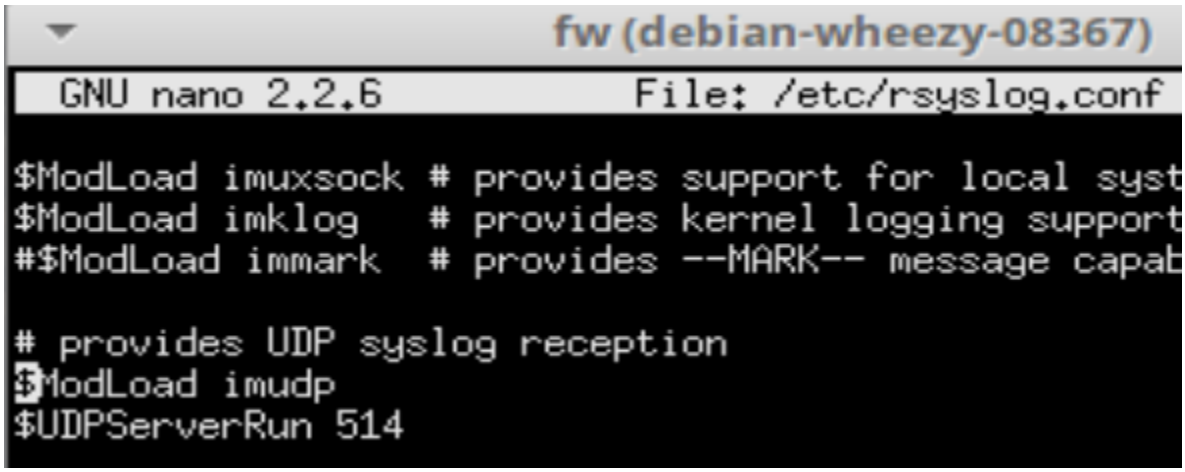
```
Mar  9 21:14:15 snort snort[2918]: [1:1000077:1] HTTP DELETE attempt on /upload/
files {TCP} 1.2.3.1:42024 -> 10.0.0.1:80
```

I 4.4 Sur snort : configurez le serveur rsyslog afin qu'il redirige les messages d'alerte vers le serveur rsyslog de fw. Il faut pour cela ajouter la ligne suivante à la fin du fichier /etc/rsyslog.conf : auth .* @10 .0.0.254 # à remplacer par l'IP de fw(eth0).

On modifie le fichier /etc/rsyslog.d afin d'envoyer les alertes Snort à fw:

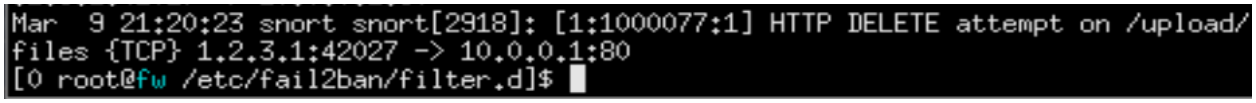
```
snort (debian-wheezy-08367)
 GNU nano 2.2.6              File: /etc/rsyslog.conf

        *.=debug;*.=info;\
        *.=notice;*.=warn       |/dev/xconsole

auth.* 10.0.0.254
```

I 4.5 Sur fw : activez la réception de messages syslog sur le port UDP/514. Il faut pour cela trouver et décommenter deux lignes dans le fichier /etc/rsyslog.conf.

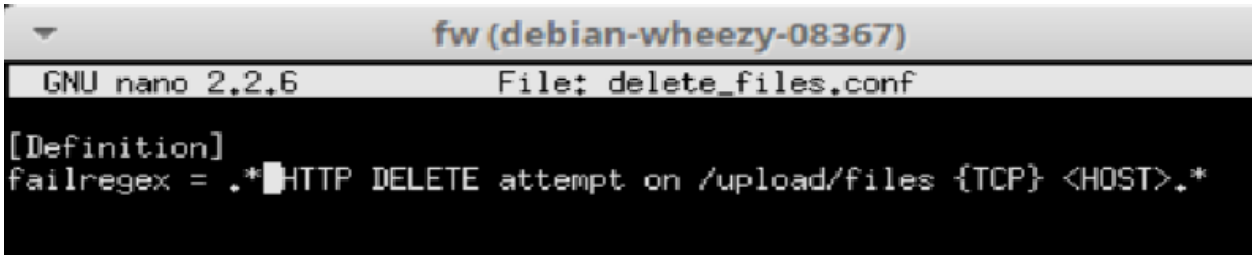


I 4.6 Sur pirate : envoyez de nouveau une requête permettant de générer l'alerte.

I 4.7 Sur fw : vérifiez qu'une alerte est bien présente dans le fichier /var/log/auth.log.



I 4.8 Sur fw : créez un fichier /etc/fail2ban/filter.d/delete_files.conf dont le contenu sera le suivant :



I 4.9 Sur fw : créez une geôle [delete_files] dans le fichier /etc/fail2ban/jail.local :

```
[delete_files]
enabled = true
bantime = -1
chain = FORWARD
maxretry = 1
logpath = /var/log/auth.log
port = 80
filter = delete_files
```

I 4.10 Sur pirate : envoyez de nouveau une requête permettant de générer l'alerte

```
[255 root@pirate ~]$ cat req3.txt | nc 10.0.0.1 80
```

```
pirate (debian-wheezy-08367)
 GNU nano 2.2.6                File: req3.txt

DELETE /upload/files/fichier_test HTTP/1.1
file: blablaPGV_bASE_DIRECTORYblabla
```

I 4.11 Sur fw : affichez le contenu des chaînes iptables pour vérifier qu'une nouvelle règle permettant de bloquer pirate est bien présente.

```
[2 root@fw /etc/fail2ban/filter.d]$ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-ssh  tcp  --  anywhere             anywhere            multiport dport
s ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
fail2ban-delete_files  tcp  --  anywhere             anywhere            multip
ort dports http

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain fail2ban-delete_files (1 references)
target     prot opt source               destination
DROP       all  --  1.2.3.1              anywhere
RETURN     all  --  anywhere             anywhere

Chain fail2ban-ssh (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
[0 root@fw /etc/fail2ban/filter.d]$
```

```
[0 root@fw /etc/fail2ban/filter.d]$ fail2ban-client status delete_files
Status for the jail: delete_files
|- filter
|  |- File list:        /var/log/auth.log
|  |- Currently failed: 0
|  `- Total failed:     1
`- action
   |- Currently banned: 1
   |  `- IP list:       1.2.3.1
   `- Total banned:     1
```

I 4.12 Sur pirate : vérifiez qu'il est maintenant impossible d'accéder au serveur web de www.

```
[1 root@pirate ~]$ cat req3.txt | nc 10.0.0.1 80
(UNKNOWN) [10.0.0.1] 80 (http) : Connection timed out
[1 root@pirate ~]$
```