**PSAD**

PSAD (*Port Scan Attack Detector*) est un **ensemble de démons système légers** qui s'exécutent sur le système Linux et **analysent les messages de journal iptables** afin de **détecter les balayages** (*scans*) **de ports et autres trafics suspects**.

PSAD est **utilisé pour transformer un système de détection d'intrusion en un système de prévention d'intrusion**.   
PSAD **utilise les règles snort** pour la **détection des événements d'intrusion**.   
Il est **spécialement conçu pour fonctionner avec Linux iptables/firewalld** afin de **détecter le trafic suspect** tel que …

* les **analyses de ports** ;
* les **portes dérobées**   
  et
* les **commandes provenant d’un réseau de zombies** (*botnet*).

# Caractéristiques

PSAD ...

* **prend en charge** les **journaux IPv4 et IPv6 générés par iptables** ;
* **détecte les balayages** (scans) **TCP** **SYN**, FIN, **NULL**, **XMAS** et de **nombreuses règles de signature du** **snort** ;
* **envoie des notifications par courriels** avec caractéristiques d'analyse TCP/UDP/ICMP, DNS inversé et informations whois ;
* **valide les champ d'en-tête ICMP** ;
* **bloque automatiquement les adresses IP** suspectes à l’aide d’iptables et de tcpwrappers en fonction du niveau d'analyse ;
* est **distribué sous la licence publique générale GNU**.

**Remarque** …  
Pour ce document on prend pour acquis que le système utilise UFS (Uncomplicated FireWall).

# Installation de PSAD

Par défaut, PSAD est **disponible dans le référentiel Debian** …  
**>> sudo apt install psad**

# Configuration de PSAD

Par défaut, PSAD stocke ses **fichiers de configuration dans le répertoire /etc/psad**.

Par prudence on fait une **copie de sauvegarde du fichier de configuration de psad /etc/psad/psad.conf** …  
**>>** **sudo cp --archive /etc/psad/psad.conf /etc/psad/psad.conf-Copie-$(date +"%Y%m%d%H%M%S")**

On édite la configuration principale de PSAD dans le /etc/psad/psad.conf …  
**>>** **sudo nano /etc/psad/psad.conf**

On **vérifie et met à jour les options de configuration** dans /etc/psad/psad.conf.   
On **porte une attention particulière aux options** suivantes ...

|  |  |
| --- | --- |
| Paramètre | Valeurs |
| [EMAIL\_ADDRESSES](http://www.cipherdyne.org/psad/docs/config.html#EMAIL_ADDRESSES) | Adresse(s) de courriel |
| HOSTNAME | Nom du serveur |
| ENABLE\_PSADWATCHD | ENABLE\_PSADWATCHD Y; |
| [ENABLE\_AUTO\_IDS](http://www.cipherdyne.org/psad/docs/config.html#ENABLE_AUTO_IDS) | ENABLE\_AUTO\_IDS Y; |
| ENABLE\_AUTO\_IDS\_EMAILS | ENABLE\_AUTO\_IDS\_EMAILS Y; |
| EXPECT\_TCP\_OPTIONS | EXPECT\_TCP\_OPTIONS Y; |

On **spécifie également le réseau interne et externe** ...  
**HOME\_NET <Adresse du réseau>/<Masque CIDR>;   
HOME\_NET 192.168.1.0/24  
EXTERNAL\_NET any;**

On modifie (si cela est nécessaire) …  
Ceci **représente le nombre de paquets requis pour qu’un balayage** (*scan*) **atteigne un seuil considéré** comme dangereux.  
**DANGER\_LEVEL1 5; ### Number of packets.   
DANGER\_LEVEL2 15;   
DANGER\_LEVEL3 150;   
DANGER\_LEVEL4 1500;   
DANGER\_LEVEL5 10000;**

On **modifie la destination des journaux** …  
Par **défaut le fichier /var/log/messages** est utilisé.  
On peut le modifier pour /var/log/syslog …  
**IPT\_SYSLOG\_FILE /var/log/syslog;**

On active PSAD comme IDS/IPS …  
**ENABLE\_AUTO\_IDS Y;**

SI souhaité, on peut spécifier les ports qui doivent être ignorés …  
**IGNORE\_PORTS NONE;**

On sauvegarde et on quitte le fichier.

On apporte par la suite **quelques modifications à UFW pour qu'il fonctionne avec PSAD** en indiquant à UFW de consigner tout le trafic afin que PSAD puisse l'analyser.

Pour ce faire, on édite les **deux fichiers suivants et on ajoute ces lignes à la fin**, mais **avant la ligne COMMIT** …  
**/etc/ufw/before.rules  
/etc/ufw/before6.rules**

On effectue des **copies de sauvegarde des deux fichiers** …  
**>>** **sudo cp --archive /etc/ufw/before.rules /etc/ufw/before.rules-Copie-$(date +"%Y%m%d%H%M%S")  
>>** **sudo cp --archive /etc/ufw/before6.rules /etc/ufw/before6.rules-Copie-$(date +"%Y%m%d%H%M%S")**

On **ajoute ce qui suit à la fin des fichiers** … mais **avant la ligne COMMIT** …  
**# log all traffic so psad can analyze  
-A INPUT -j LOG --log-tcp-options --log-prefix "[IPTABLES] "  
-A FORWARD -j LOG --log-tcp-options --log-prefix "[IPTABLES] "**

**Remarque** …  
On **ajoute un préfixe de journalisation à tous les journaux iptables**.   
Cela est **utile afin de séparer les journaux iptables dans leur propre fichier**.

On doit maintenant **recharger/redémarrer UFW et PSAD** pour que les modifications prennent effet …  
**>>** **sudo ufw reload**  
**>>** **sudo psad --Restart**ou   
**>>** **sudo psad -R**

On **met ensuite à jour les signatures** afin qu'il puisse **reconnaître correctement les types d'attaques connus** …  
**>>** **sudo psad --sig-update**  
**[+] Archiving original /etc/psad/signatures -> signatures.old1  
[+] Downloading latest signatures from:  
 http://www.cipherdyne.org/psad/signatures  
--2021-07-26 15:46:31-- http://www.cipherdyne.org/psad/signatures  
Résolution de www.cipherdyne.org (www.cipherdyne.org)… 67.20.100.192  
Connexion à www.cipherdyne.org (www.cipherdyne.org)|67.20.100.192|:80… connecté.  
requête HTTP transmise, en attente de la réponse… 200 OK  
Taille : 45267 (44K)  
Sauvegarde en : « signatures »  
   
signatures 100%[=====================================>] 44,21K 290KB/s ds 0,2s   
   
2021-07-26 15:46:32 (290 KB/s) — « signatures » sauvegardé [45267/45267]**

**[+] New signature file /etc/psad/signatures has been put in place. You can restart psad (or use 'psad -H') to import the new sigs.**

On **envoie à tous les démons de PSAD un signal HUP pour qu'ils réimportent les configurations** …  
**>>** **psad -H**ou  
**>>** **psad --HUP**

On **analyse les règles iptables pour les erreurs** …  
**>> sudo psad --fw-analyze  
[+] Parsing INPUT chain rules.  
[+] Parsing INPUT chain rules.  
[+] Firewall config looks good.  
[+] Completed check of firewall ruleset.  
[+] Results in /var/log/psad/fw\_check  
[+] Exiting.**

**Remarque** …  
En cas de problème, on recevra un courriel contenant l'erreur.

# Démarrage de PSAD

Une fois que tout est configuré, on **redémarre le service psad pour implémenter les modifications de configuration** …  
**>>** **sudo systemctl redémarrer psad**

On peut maintenant **vérifier l'état actuel des événements détectés par PSAD** …  
**>>** **sudo psad -S  
[-] psad: pid file /var/run/psad/psadwatchd.pid does not exist for psadwatchd on debian-cli  
[+] psad\_fw\_read (pid: 35018) %CPU: 0.0 %MEM: 2.0  
 Running since: Mon Jul 26 15:48:45 2021**

**[+] psad (pid: 35009) %CPU: 0.1 %MEM: 2.2**

**Running since: Mon Jul 26 15:48:45 2021  
 Command line arguments: [none specified]  
 Alert email address(es): root@localhost**

**[+] Version: psad v2.4.3**

**[+] Top 50 signature matches:  
 [NONE]**

**[+] Top 25 attackers:  
 [NONE]**

**[+] Top 20 scanned ports:  
 [NONE]**

**[+] iptables log prefix counters:  
 [NONE]**

**Total protocol packet counters:**

**[+] IP Status Detail:  
 [NONE]**

**Total scan sources: 0  
 Total scan destinations: 0**

**[+] These results are available in: /var/log/psad/status.out**

# PSAD mis à l’épreuve

PSAD est maintenant opérationnel. Il est temps de le tester.

Sur une machine distante, on **balaie les ports du serveur à l'aide de l'utilitaire nmap** …  
**>>** **sudo nmap -sS -sU -T4 -A -v <Adresse IP du serveur>  
Balayage intensif avec port UDP  
>>** **sudo nmap -p 1-65535 -T4 -A -v <Adresse IP du serveur>**

**Remarque** …  
Si **nmap n'est pas installé** …  
**>>** **sudo apt install nmap**

Sur le serveur, on **vérifie l'état de PSAD** …  
**>>** **sudo psad -S**

On peut constater que **l’adresse IP de l'attaquant est bloquée** par le démon PSAD.

Il est possible également de **voir l'adresse IP de l'attaquant bloquée par une règle iptables** …  
**>>** **sudo iptables -L**

Si on souhaite **autoriser toutes les adresses IP bloquées par PSAD** …  
**>>** **sudo psad -F**

Si on **souhaite autoriser une adresse IP spécifique bloquée par PSAD** …  
**>>** **sudo psad --fw-rm-block-ip <Adresse IP>**

Pour en **savoir plus sur les exemples et options de commandes PSAD** …  
**>>** **sudo man psad**