OSSEC, détection d'intrusion libre et plus encore

Nicolas Sulek

25 septembre 2014

Séminaire RAISIN/CEPAGE

OSSEC est un Host based IDS ou système de détection d'intrusion machine

Deux modes de fonctionnement possibles

- local
- client-serveur

Communication client-serveur

- chiffrée par blowfish
- compressée avec la zlib
- UDP 1514

Méthodes d'audits

- analyse des journaux de logs locaux ou distants (plus de 100 décodeurs)
- processus de scan en temps réel ou programmable

Serveurs Unix only

- GNU/Linux
- *BSD

Agents quasi-universels

- GNU/Linux
- Windows
- VMWare ESX
- *BSD
- Unix propriétaires (Solaris, AIX, HP-UX, Mac OSX)

Licence

Logiciel sous licence Gnu General Public Licence v2

Bref historique

- 2004 : logiciel rendu public
- 2008 : achat par Third Brigade (applications de sécurité pour serveur)
- 2009 : achat de Third Brigade par Trend Micro (solutions de sécurité)

Projet actif

- 26 contributeurs
- plus de 3000 commits depuis 2005
- version 2.8.1 sortie le 09/09/2014

Installation sous GNU/Linux et *BSD

```
wget http://www.ossec.net/files/ossec-hids-2.8.1.tar.gz
tar xfz ossec-hids-2.8.1.tar.gz
cd ossec
sh install.sh
(répondre à quelques questions)
/var/ossec/bin/ossec-control start
```

Installation sous Windows

```
Internet Explorer->www.ossec.net->Downloads-> Agent 2.8 - Windows
ossec-agent-win32-2.8.exe->Next->I agree->Next->Install->Next
->Finish
```

- en temps réel ou à une fréquence définie
- droits des fichiers et répertoires
- taille
- propriétaire
- somme de contrôle (MD5, SHA1)

- signatures et anomalies
- fichiers dans /dev qui ne sont pas des devices
- répertoires cachés
- fichiers SUID
- fichiers avec droits root et écriture pour tous
- processus en cours non visibles avec ps
- ports en écoute non visibles avec netstat
- interfaces en mode promiscuous

- identification des situations pouvant créer une brèche
- benchmark de sécurité suivant les standards du Center for Internet Security ou personnalisés
- fichiers, registre ou processus qui doivent exister ou pas
- vérification de l'état de l'antivirus et du pare-feu

Pour un niveau d'alerte défini, possibilité d'exécuter un script qui :

- ajoute une règle au pare-feu
- utilise TCP Wrapper
- redémarre OSSEC
- désactive un compte
- ...

sur

- l'agent qui a levé l'alerte
- un agent choisi arbitrairement
- le serveur
- tous les agents et le serveur

- Règles relativement simples écrites en XML
- Définitions de niveau d'alerte de 0 (ignoré) à 15 (attaque critique)
- Plus de 1000 règles fournies
- Règles complétement personnalisables

```
[root@moscou ~]# cd /var/ossec/rules/
[root@moscou rules]# ls *.xml
apache_rules.xml        ms-exchange_rules.xml  smbd_rules.xml
arpwatch_rules.xml      ms_ftpd_rules.xml      solaris_bsm_rules.xml
asterisk_rules.xml      ms-se_rules.xml        sonicwall_rules.xml
attack_rules.xml        mysql_rules.xml        spamd_rules.xml
bro-ids_rules.xml       named_rules.xml        squid_rules.xml
cimserver_rules.xml     netscreenfw_rules.xml  sshd_rules.xml
cisco-ios_rules.xml     nginx_rules.xml        symantec-av_rules.xml
clam_av_rules.xml       openbsd_rules.xml      symantec-ws_rules.xml
courier_rules.xml       ossec_rules.xml        syslog_rules.xml
dovecot_rules.xml       pam_rules.xml          telnetd_rules.xml
dropbear_rules.xml      php_rules.xml          trend-osce_rules.xml
firewall_rules.xml      pix_rules.xml          vmpop3d_rules.xml
ftpd_rules.xml          policy_rules.xml       vmware_rules.xml
hordeimp_rules.xml      postfix_rules.xml      vpn_concentrator_rules.xml
ids_rules.xml           postgresql_rules.xml   vpopmail_rules.xml
imapd_rules.xml         proftpd_rules.xml      vsftpd_rules.xml
local_rules.xml         pure-ftpd_rules.xml    web_appsec_rules.xml
mailscanner_rules.xml   racoon_rules.xml       web_rules.xml
mcafee_av_rules.xml     roundcube_rules.xml    wordpress_rules.xml
msauth_rules.xml        rules_config.xml       zeus_rules.xml
ms_dhcp_rules.xml       sendmail_rules.xml
[root@moscou rules]#
```

Alerte niveau 10 pour nom de fichier ou URI trop long

```
<rule id="30117" level="10">
 <if_sid>30101</if_sid>
 <match>File name too long|request failed: URI too long</match>
 <description>Invalid URI, file name too long.</description>
 <group>invalid_request,</group>
</rule>
```

Alerte niveau 6 pour blocage par ModSecurity

```
<rule id="30118" level="6">
 <if_sid>30101</if_sid>
 <match>mod_security: Access denied|ModSecurity: Access
 denied</match>
 <description>Access attempt blocked by Mod Security</description>
 <group>access_denied,</group>
</rule>
```

Alerte niveau 5 pour connexion d'un utilisateur non autorisé

```
<rule id="5718" level="5">
 <if_sid>5700</if_sid>
 <match>not allowed because</match>
 <description>Attempt to login using a denied user.</description>
 <group>invalid_login,</group>
</rule>
```

Alerte niveau 10 pour déclenchement régulier de la règle précédente

```
<rule id="5719" level="10" frequency="6" timeframe="120"
ignore="60">
 <if_matched_sid>5718</if_matched_sid>
 <description>Multiple access attempts using a denied user.
 </description>
 <group>invalid_login,</group>
</rule>
```

Avantages

- gratuit et libre
- installation facile
- peu gourmand en ressources et en compétences
- visibilité des activités systèmes (kernel, daemons internes, ...)
- n'importe quel logiciel ou système peut être intégré tant qu'il y a des logs

Inconvénients

- peut générer beaucoup de mails -> exceptions sur les règles
- support Windows inférieur au reste -> net progrès avec la dernière version
- agrégation de mails pas toujours respectée

- Site web d'OSSEC : `www.ossec.net`
- Documentation officielle : `http://ossec-docs.readthedocs.org/en/latest/index.html`
- Dépôt GIT : `https://github.com/ossec`
- Liste de diffusion utilisateurs : `ossec-list@googlegroups.com`
- Liste de diffusion développeurs : `ossec-dev@googlegroups.com`