14/10/2015

Installation du service PortSentry

V1

Lecaudey Etienne

Tutoriel 1.1 : Installation du service Portsentry		
Lecaudey Etienne	Version 1.0	14/10/2015

SOMMAIRE :

Table des matières

Table des matières 2
Objectifs :..... 3
Information sur les versions: 3
Installation des services :..... 3
Configuration de base : 4

Tutoriel 1.1 : Installation du service Portsentry		
Lecaudey Etienne	Version 1.0	14/10/2015

Objectifs :

L'objectif de cette procédure est de procéder à l'installation du service Portsentry

Portsentry est une application qui permet à un serveur de détecter un scan de port mais aussi d'agir

- Les attaques seront inscrites dans des logs
- Le scanneur est automatiquement bloqué car l'ip sera rajouté dans /etc/host_deny
- Avec ipchains, toutes les communications venant de l'hôte « attaquant » seront bloquées
- L'interface de communication peut-être coupée en cas d'attaque

Il est donc très utile d'installer et configurer Portsentry pour sécuriser nos serveurs

Information sur les versions:

VM	Debian 8.1	Jessie	192.168.1.127

Installation des services :

Avant toute Installation, il faut réaliser une mise à jour des paquets :

```
apt-get update
```

Pour installer le paquet lancez la commande suivante :

```
apt-get install portsentry
```

Configuration de base :

Lors de l'installation vous serez prévenu que par défaut Portsentry ne bloque rien. Il faudra donc modifier les fichiers de configuration, mais tout d'abord occupons-nous des hôtes qui seront ignorés afin de ne pas se faire soit bloquer même

```
nano /etc/portsentry/portsentry.ignore
```

Ajoutons la liste des ips que vous souhaitez ne jamais bloquer

```
# IPs from /etc/portsentry/portsentry.ignore.static:
127.0.0.1/32
0.0.0.0

# dynamically fetched IPs(via ifconfig -a):
192.168.1.125
127.0.0.1
```

Nous pouvons maintenant nous occuper de la configurer de Portsentry

```
nano /etc/default/portsentry
```

Maintenant, nous allons activer les modes « audp » et « atcp », Portsentry va alors vérifier les ports utilisés et automatiquement « lier » les ports disponibles. C'est l'options la plus efficace (« a » signifie avancé). Ainsi Portsentry établit alors une liste des ports d'écoute, TCP et UDP et bloque l'hôte se connectant sur ces ports, sauf s'il est présent dans le fichier portsentry.ignore

```
TCP_MODE="atcp"
UDP_MODE="audp"
```

Modifions maintenant le fichier de configuration principal :

```
nano /etc/portsentry/portsentry.conf
```

Mettez en place le blocage en modifiant la section Ignore options de la façon suivante :

```
##################
# Ignore Options #
##################
# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="1"
BLOCK_TCP="1"
```

Maintenant, dans la section dropping route, la ligne suivant ne doit pas être commenté

```
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
```

Même chose dans la section TCP wrappers doit être commenté.

```
KILL_HOSTS_DENY="ALL: $TARGET$ : DENY"
```

Dans la section external command ajouter cette ligne :

```
KILL_RUN_CMD="/sbin/iptables -I INPUT -s $TARGET$ -j DROP && /sbin/iptables -I
INPUT -s $target$_
```

Enfin, nous pouvons redémarrer Portsentry qui nous protégera au mieux d'un scan des ports

```
service portsentry restart_
```