sshblack

• préambule

Cette présentation est juste un retour d'expérience sur une solution (parmi d'autres) au problème de comment se prémunir des attaques dites "brute force" à l'encontre d'un serveur "ssh" dans les conditions suivantes:
- pas d'accès aux réglages du "pare-feu" qui est géré par le "CRI" de l'institution,
- seul le port 22 ("ssh") est ouvert vers la machine qui est à protéger.

Pour résoudre ce problème, ma solution a été d'utiliser "sshblack"

http://www.sshblack.com/ © Charlie Pettinger 

sshblack

- **qu'est-ce qu'une attaque "brute force" ?**

C'est quand on trouve, les lignes suivantes, dans le fichier de "logs" de "ssh"

```
Failed password for root from a.b.c.d port 47529 ssh2
Failed password for invalid user test from a.b.c.d port 47719 ssh2
Failed password for invalid user staff from a.b.c.d port 34604 ssh2
Failed password for invalid user sales from a.b.c.d port 35012 ssh2
Failed password for invalid user recruit from a.b.c.d port 35971 ssh2
Failed password for invalid user alias from a.b.c.d port 35992 ssh2
Failed password for invalid user office from a.b.c.d port 36410 ssh2
Failed password for invalid user samba from a.b.c.d port 36849 ssh2
Failed password for invalid user tomcat from a.b.c.d port 36863 ssh2
Failed password for invalid user webadmin from a.b.c.d port 37279 ssh2
Failed password for invalid user spam from a.b.c.d port 37289 ssh2
Failed password for invalid user virus from a.b.c.d port 37709 ssh2
Failed password for invalid user cyrus from a.b.c.d port 38146 ssh2
Failed password for invalid user oracle from a.b.c.d port 38162 ssh2
Failed password for invalid user michael from a.b.c.d port 38993 ssh2
Failed password for invalid user ftp from a.b.c.d port 39007 ssh2
Failed password for invalid user postmaster from a.b.c.d port 39851 ssh2
Failed password for invalid user postfix from a.b.c.d port 39867 ssh2
Failed password for invalid user postgres from a.b.c.d port 40277 ssh2
Failed password for invalid user paul from a.b.c.d port 40296 ssh2
Failed password for invalid user guest from a.b.c.d port 40730 ssh2
Failed password for invalid user admin from a.b.c.d port 40747 ssh2
Failed password for invalid user linux from a.b.c.d port 41166 ssh2
```

pré-requis

- **ssh**

  Bien évidement une machine sur laquelle est installé un serveur "ssh"

- **pare-feu**

  Ajouter un "pare-feu" en local:
  - Linux " ipchain" "iptables"
  - BSD "ipf" "pf"
  - Solaris "ipf"

- **perl**

  Ensuite "perl" si il n'est pas déjà installé et "sshblack"

principe 1/3

C'est un "script" en "perl" qui à la particularité de ne pas avoir à modifier l'installation de "ssh" sur la machine où il est installé et exécuté, il "monitor" avec un "tail -f" le fichier de "logs" de "ssh" et tient à jour un fichier ("ssh-blacklist-pending") des adresses considérées, selon certains critères paramétrables, comme pouvant être à l'origine d'attaques dites "brute force".

```
# The log file you want to monitor
my($LOG) = '/var/adm/sshd.log';
# The text database file to keep track of attackers
my($CACHE) = '/var/tmp/ssh-blacklist-pending';
# Regex of reasons to get firewalled. Separate with pipe (|).
# This VARIES BASED ON THE VERSION OF SOFTWARE YOU ARE RUNNING
# Look at your logs and adjust as necessary.
# Most ssh daemons will list "Failed Password" even if it is
# an illegal user. If you put both Illegal and Failed here
# you might get double hits.
my($REASONS) = '(Failed password|Failed none)';
# Maximum time (sec) before they are removed from the database
# unless they are already blacklisted
my($AGEOUT) = 600;
# Time delay (day) before they are released from the blacklist in DAYS!
my($RELEASEDAYS) = 1;
# Time delay (sec) to check the database for cleanup
my($CHECK) = 300;
# Maximum number of booboos before they get listed
my($MAXHITS) = 4;
```

principe 2/3

A chaque ajout ou retrait d'une adresse dans ce fichier ("ssh-blacklist-pending"), le "script" lance une commande appropriée pour ajouter ou retirer cette adresse des règles du "pare-feu".

```
# Set $ADDRULE to the complete command line instruction for ADDING
# attackers to the blacklist with the following change:
# - Substitute the literal string 'ipaddress' in the location where
# you want the attacker's IP address to be
#
# ######### ############ IPF VERSION ############# ############
#
 my($ADDRULE) = 'echo "block return-rst in log quick on dmfe0 proto tcp from ipaddress to any port = 22" | /usr/sbin/ipf -f -';

# Set $DELRULE to the complete command line instruction for REMOVING
# attackers from the blacklist with the following change:
# - Substitute the literal string 'ipaddress' in the location where
# you want the attacker's IP address to be.
#
# ######### ############ IPF VERSION ############# ############
#
 my($DELRULE) = 'echo "block return-rst in log quick on dmfe0 proto tcp from ipaddress to any port = 22" | /usr/sbin/ipf -rf -';
```

Ces commandes sont facilement modifiables et je les ai adaptées pour fonctionner avec "IP Filter". Sur le site "web" il y a des exemples pour "ipchain", "pf", ...

principe 3/3

J'ai même réussi à ajouter quelques lignes (par copier-coller) à ce "script" pour insérer les adresses "black" listées, contenues dans le fichier "ssh-blacklist-pending", dans les règles du "pare-feu" au moment du "boot" (lancement du "script"), cela manquait alors que le fichier "ssh-blacklist-pending" est persistant.

Pour cela j'ai défini une nouvelle commande (et écris le code qui va avec), qui permettra au "script" de vérifier l'absence ou la présence des adresses "black" listées dans les règles du "pare-feu" et de les insérer si nécessaire.

```
# Set $CHKRULE to the complete command line instruction for CHECKING
# if attackers from the blacklist exist in the firewall rules with the following change:
# - Substitute the literal string 'ipaddress' in the location where
# you want the attacker's IP address to be
#
# ######### ############ IPF VERSION ############# ############
#
 my($CHKRULE) = '/usr/sbin/ipfstat -i | grep ipaddress 2>&1 > /dev/null';
```

Cette modeste contribution devrait être intégrée dans la version suivante de "sshblack" (3.0, la version actuelle est 2.7), qui sera réalisée, par son auteur, dans les prochains mois.

démarrage au "boot"

- **le fichier de "démarrage"**

Le plus simple est encore de modifier le fichier de démarrage de "ssh"

```
#!/sbin/sh
...
case $1 in
'start')
        [ -x /usr/local/sshblackv27/sshblack.pl ] && /usr/local/sshblackv27/sshblack.pl >>/var/log/sshblack.log 2>&1 &
      ...
      ;;
'stop')
      ...
       /usr/bin/pkill -f sshblack
      ;;
...
```

les "logs"

- **le fichier de "logs"**

Ce fichier (défini dans le fichier de démarrage) permet de suivre l'activité

```
SSHBLACK is Starting...
a.b.c.d being synchronized  to the  firewall
a.b.c.d being synchronized  to the  firewall
Monitoring your log file for future attacks
Watching a.b.c.d as potential attacker
Watching a.b.c.d as potential attacker
Freeing a.b.c.d
Watching a.b.c.d as potential attacker
Watching a.b.c.d as potential attacker
Watching a.b.c.d as potential attacker
a.b.c.d being blocked because of Failed password
Watching a.b.c.d as potential attacker
Freeing a.b.c.d
```

en guise de conclusion

- **résultats**

  Cela a été facile à mettre en place et fonctionne parfaitement (diapo suivante).

- **pourquoi "sshblack" ?**

  Avant d'utiliser "sshblack" j'avais trouvé et regardé plusieurs "scripts" du même genre, mais la plupart, incluant "bruteforceblocker" (dont nous avions parlé sur "Mathrice"), sont orientés "Linux" et plus ou moins facilement adaptables (selon moi) à ma situation ("Solaris" et "IP Filter").

  De toute façon, l'esprit et le principe de fonctionnement étant le même pour tous ces programmes, ...

Et pour finir ...

• Statistiques

A partir des fichiers de "logs" **(12 Mars)** :
- ssh nombre de lignes avec "Failed password" (sshd.log)
- ipf nombre d'accès bloqués sur le port "22" (ipmon.log)

	Machine N° 1		Machine N° 2	
	ssh **(8 Nov)**	ipf **(25 Jan)**	ssh **(23 Nov)**	ipf **(6 Fev)**
"attaques"	56333	53585	41678	26313
Novembre	592		269	
Décembre	11883		10053	
Janvier	43511	22340	29707	
Février	296	24283	1606	18777
Mars	51	6962	43	7536