

Sécurisation d'un serveur d'hébergement

Projet tutoré de seconde année GTR

Tuteur : M.Bourgeois

Romain Bouleis

Thomas Cottier

PLAN

- Introduction
- Sécurité globale
- La sécurité des services
 - SSH
 - Apache
 - Php
 - MySQL
 - FTP
- Phpsysinfo : conclusion sécurité
- Confrontation
- Conclusion

INTRODUCTION

- Porte d'accès à de nombreux sites.
- Cible de nombreux hackers.
- Nécessité pour le client de disposer de plusieurs services.
- Nécessité de sécuriser ces services sans nuire à leur interactivité.

SECURITE GLOBALE

- Partitionnement:
 - / : partition des fichiers systèmes.
 - /home : là où sont stockées les données des utilisateurs
 - /var : partition utilisée par certains processus utilisateurs
 - /tmp : tout le monde peut écrire dans ce répertoire

SECURITE GLOBALE

- PAM (Pluggable Authentication Modules):
 - Ensemble de petits modules s'exécutant lors de certaines actions de l'utilisateur:
 - Ouverture et fermeture de session
 - Utilisation des fichiers utilisateurs
 - Schéma global d'authentification
 - Actions à effectuer lors du changement de mot de passe

SECURITE GLOBALE

- Firewall : Blocage des ports inutilisés.
- Ports laissés libres:
 - 20 et 21 pour FTP
 - 22 pour SSH
 - 80 pour HTTP
 - 2121 pour l'accès FTP admin
 - 8080 pour l'accès HTTP admin

SECURITE GLOBALE

- Limitations des ressources matérielles:
 - Les quotas
 - Empêche un utilisateur de dépasser la limite de place qui lui a été allouée
 - PAM_limits
 - Limitations de ressources utilisées par un utilisateur (CPU, nombre de processus,...)

SECURITE DES SERVICES

- SSH (Secure Shell):
 - Permet d'avoir un shell à distance.
 - Les utilisateurs sont chrootés
 - Leur répertoire, au lieu de se trouver dans `/home/user` se trouve dans `/home/chroot/home/user`
 - Ils n'ont donc pas accès à la racine et ne voient pas les processus systemes.
 - Montages des répertoires `/home/data/clients/user` dans `/home/chroot/home/user`

SECURITE DES SERVICES

■ Apache

- Serveur web qui répond aux requêtes HTTP.
- Apache est chrooté et répond sur le port 80 mais un Apache, non chrooté répond sur le ports 8080 pour les admins

SECURITE DES SERVICES

■ PHP

- Langage dynamique qui permet des commandes potentiellement dangereuses.
- Importance de le restreindre.
- Il est donc chrooté (c'est d'ailleurs en partie à cause de PHP que Apache est chrooté)
- Suppression de nombreuses commandes à risque.

SECURITE DES SERVICES

■ MySQL

- Base de données simple à utiliser et intégration facile à PHP.

■ Eskuel

- Outils PHP permettant de gérer la base MySQL.

■ Privilèges

```
MySQL --password=rootPass --exec "GRANT ALL PRIVILEGES ON $1.* TO  
$1@localhost.localdomain IDENTIFIED BY '$2' WITH MAX_QUERIES_PER_HOUR 2000  
MAX_UPDATES_PER_HOUR 2000 MAX_CONNECTIONS_PER_HOUR 200"
```

SECURITE DES SERVICES

- FTP (File Transfer Protocol):
 - Utilisation d'un serveur FTP Sécurisé: vsFTP.
 - FTP est chrooté.
 - Utilisation d'un serveur FTP non chrooté pour l'admin sur le port 2121.

Phpsysinfo : conclusion sécurité

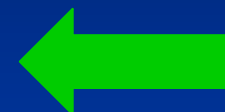
Information Système : N.A. (192.168.0.10)

Système		Information Matériel	
Nom d'hôte canonique	N.A.	Processeurs	N.A.
IP	192.168.0.10	Modèle	N.A.
Version du noyau	N.A.	Fréquence	N.A. Mhz
Distro Name	Debian 3.1	Taille Cache	N.A.
Uptime	0 minutes	Bogomips	N.A.
Utilisateurs	5	Périph. PCI	aucun
Charge système	N.A. N.A. N.A.	Périph. IDE	aucun

Réseau			
Périphérique	Réception	Envoi	Err/Drop
lo	60.50 Mo	12.18 Mo	0/0
eth0	297.57 Ko	297.57 Ko	0/0

Utilisation mémoire				
Type	Utilisation	Libre	Utilisé	Taille
Mémoire Physique	0%	0.00 Ko	0.00 Ko	0.00 Ko
Swap disque	0%	0.00 Ko	0.00 Ko	0.00 Ko

Systemes de fichiers montés						
Point	Type	Partition	Utilisation	Libre	Utilisé	Taille
			Totaux :	0.00 Ko	0.00 Ko	0.00 Ko



Aperçu du système vu « utilisateur »

Modèle : Langue :

Créé par phpsysInfo-2.3 on Mar 12, 2005 at 12:20:57 AM

Information Système : localhost.localdomain (192.168.0.10)

Système		Information Matériel	
Nom d'hôte canonique	localhost.localdomain	Processeurs	1
IP	192.168.0.10	Modèle	Mobile Intel(R) Pentium(R) 4 - M CPU 2.20GHz
Version du noyau	2.4.27-1-386	Fréquence	2193.57 MHz
Distro Name	Debian 3.1	Taille Cache	512 KB
Uptime	1 jours 7 heures 51 minutes	Bogomips	4377.8
Utilisateurs	2	Périph. PCI	0000:00:1f:1 IDE interface: Intel Corp. 82801DBM 0000:00:1f:5 Multimedia audio controller: Intel Corp. 82801DB/DBL/DBM 0000:00:1f:6 Modem: Intel Corp. 82801DB/DBL/DBM 0000:01:00:0 VGA compatible controller: ATI Technologies Inc Radeon R250 LE [Radeon Mobility 9000 M9] 0000:02:00:0 Ethernet controller: Broadcom Corporation BCM4401 100base-T 0000:02:01:1 FireWire: Texas Instruments PCI4510 IEEE-1394 Controller
Charge système	0.00 0.00 0.00	Périph. IDE	hda: HITACHI_DK23EB-40 (Capacité: 37.26 Go) hdc: Samsung CD-RW/DVD-ROM SN-324B
		Périph. USB	Linux 2.4.27-1-386 eth0_hcd Intel Corp. 82801D8 USB2 00:1d:7 USB UHCI Root Hub bf20 USB UHCI Root Hub bf40 USB UHCI Root Hub bf80

Réseau			
Périphérique	Réception	Envoi	Err/Drop
lo	60.50 Mo	12.18 Mo	0/0
eth0	297.57 Ko	297.57 Ko	0/0

Utilisation mémoire				
Type	Utilisation	Libre	Utilisé	Taille
Mémoire Physique	38%	310.65 Mo	193.36 Mo	504.01 Mo
Swap disque	0%	760.85 Mo	0.00 Ko	760.85 Mo

Systemes de fichiers montés						
Point	Type	Partition	Utilisation	Libre	Utilisé	Taille
/	ext3	/dev/hda8	63%	287.00 Mo	561.95 Mo	896.80 Mo
/dev/shm	tmpfs	tmpfs	0%	252.00 Mo	0.00 Ko	252.00 Mo
/home	xfs	/dev/hda9	75%	236.76 Mo	715.49 Mo	952.25 Mo
/home/chroot/tmp	xfs	/dev/hda11	0%	473.05 Mo	720.00 Ko	473.75 Mo
/var	xfs	/dev/hda10	15%	809.98 Mo	142.27 Mo	952.25 Mo
/home/chroot/home/rabbit	xfs	/home/data/clients/rabbit	75%	236.76 Mo	715.49 Mo	952.25 Mo
/home/chroot/home/benji	xfs	/home/data/clients/benji	75%	236.76 Mo	715.49 Mo	952.25 Mo
/home/chroot/home/user	xfs	/home/data/clients/user	75%	236.76 Mo	715.49 Mo	952.25 Mo
			Totaux :	2.70 Go	3.48 Go	6.23 Go

Modèle : Langue :

Créé par phpsysInfo-2.3 on Mar 12, 2005 at 12:13:50 AM



Aperçu du système vu « root »

Confrontation

Services	Fonctionnement	Sécurité
Apache	OK	Bonne
SSH	OK	Mauvaise
PHP	OK	Mauvaise
FTP	OK	Très bonne
MySQL (local)	OK	Mauvaise
MySQL (PHP)	NO	-----

Confrontation

Folder list and tools.

List folder :
Empty space : 1910.51Mo

/

Commande NUX :
/
 Visualizer la sortie de la commande
(/tmp/tmp.tmp)

Remove File :
/

Send file :
/
directory :
/

File	dl	Size (ko)	Last Modification	Perms	Owner
lost+found	#	48	09/03/2005 21:08:22	drwxr-xr-x	root
home	#	4	10/03/2005 17:34:59	drwxrwsr-x	root
etc	#	4	10/03/2005 18:38:20	drwxr-xr-x	root
media	#	4	09/03/2005 21:08:57	drwxr-xr-x	root
cdrom	#	4	09/03/2005 21:08:57	drwxr-xr-x	root
var	#	4	09/03/2005 22:20:13	drwxr-xr-x	root
usr	#	4	09/03/2005 22:36:06	drwxr-xr-x	root
bin	#	4	09/03/2005 21:58:25	drwxr-xr-x	root
boot	#	4	09/03/2005 21:14:38	drwxr-xr-x	root
dev	#	24	10/03/2005 17:23:51	drwxr-xr-x	root
lib	#	4	09/03/2005 21:56:27	drwxr-xr-x	root
mnt	#	4	09/03/2005 21:09:58	drwxr-xr-x	root
proc	#	0	10/03/2005 17:22:50	dr-xr-xr-x	root
root	#	4	10/03/2005 17:06:00	drwxr-xr-x	root
sbin	#	4	09/03/2005 22:25:22	drwxr-xr-x	root
tmp	#	4	10/03/2005 18:39:55	drwxrwxrwt	root
sys	#	0	10/03/2005 17:22:50	drwxr-xr-x	root
srv	#	4	09/03/2005 21:10:14	drwxr-xr-x	root
opt	#	4	09/03/2005 21:10:14	drwxr-xr-x	root
initrd	#	4	09/03/2005 21:10:14	drwxr-xr-x	root
initrd.img	#	4312	09/03/2005 21:13:45	-rw-r--r--	root
vmlinuz	#	1071.04	09/03/2005 21:13:19	-rw-r--r--	root
firewall.sh	#	0	10/03/2005 00:37:02	-rw-r--r--	root

phpinfo

CONCLUSION

- La sécurité est essentielle pour la protection des données des utilisateurs qui font confiance à un hébergeur.
- Même s'il existe des moyens de protections, il n'y aura jamais de sécurité absolue.
- Projet très intéressant qui nous a permis d'approfondir l'univers des serveurs UNIX.