SAMBA и ClamAV - антивирусная защита.

Автор: lissyara.
Оригинал: http://www.lissyara.su/articles/freebsd/programms/samba_+_clamav/

На фрёвой машине, хранились кое какие доки пользователей, также она же использовалась для обмена документами. Решил привернуть проверку на вирусы к самбе. Порыскав по портам, по ключевому слову `samba`, нашёл антивирь - samba-vscan. Почитал - сойдёть. Будем ставить. В качестве антивируса поставим
ClamAV:/usr/home/lissyara/>cd /usr/ports/security/clamav
/usr/ports/security/clamav/>make && make install && make clean

Вылезет окно - где ничё не надо выбирать.[ ] MILTER  Compile the milter interface
[ ] CURL  Support URL downloading
[ ] LIBUNRAR  Support for external Unrar library

После сборки обновляем антивирусные базы:/usr/ports/security/clamav/>cd /usr/local/etc/
/usr/local/etc/>freshclam
ClamAV update process started at Tue Jan 24 16:30:46 2006
main.cvd is up to date (version: 35, sigs: 41649, f-level: 6, builder: tkojm)
Downloading daily.cvd [*]
daily.cvd updated (version: 1248, sigs: 852, f-level: 7, builder: diego)
Database updated (42501 signatures) from database.clamav.net (IP: 62.181.41.8)
ERROR: Clamd was NOT notified: Can't connect to clamd through /var/run/clamav/clamd
connect(): No such file or directory
/usr/local/etc/>

Добаляем строку в /etc/rc.conf, запускаем clamd и проверяем, запустился ли:
/usr/local/etc/>echo '' >> /etc/rc.conf
/usr/local/etc/>echo 'clamav_clamd_enable="YES"' >> /etc/rc.conf
/usr/local/etc/>
/usr/local/etc/>/usr/local/etc/rc.d/clamav-clamd.sh start
Starting clamav_clamd.
/usr/local/etc/>ps -ax | grep clam
63829  ??  Ss  0:00.00 /usr/local/sbin/clamd
63831  p0  S+  0:00.01 grep clam
/usr/local/etc/>

После чего можно переходить к самбе.

Для начала, неплохо бы, эту самую самбу обновить, какая-то старая версия у меня стоит:/usr/ports/>pkg_info | grep samba
samba-3.0.14a,1 A free SMB and CIFS client and server for UNIX
/usr/ports/>portupgrade samba-3.0.14a,1
[Updating the portsdb <format:bdb1_btree> in /usr/ports ...
- 14052 port entries found .....1000.....14000 ..... done]
** Port marked as IGNORE: net/samba3:
broken dependency between OpenSSL, OpenLDAP and
Heimdal for FreeBSD 4.x. Disable ADS support
/usr/ports/>
/usr/ports/>cat /var/db/ports/samba3/options
# This file is auto-generated by 'make config'.
# No user-servicable parts inside!
# Options for samba-3.0.14a,1
_OPTIONS_READ=samba-3.0.14a,1
WITH_LDAP=true
WITH_ADS=true
WITH_CUPS=true
WITH_WINBIND=true
WITHOUT_ACL_SUPPORT=true
WITH_SYSLOG=true
WITHOUT_QUOTAS=true
WITH_UTMP=true
WITHOUT_MSDFS=true
WITHOUT_SAM_XML=true
WITHOUT_SAM_MYSQL=true
WITHOUT_SAM_PGSQL=true
WITHOUT_SAM_OLD_LDAP=true
WITHOUT_PAM_SMBPASS=true
WITHOUT_EXP_MODULES=true
WITH_POPT=true
/usr/ports/>

Обновляться не захотела - пришлось отрихтовать файл /var/db/ports/samba3/option - заменить строчку:
WITH_ADS=true
на:
WITHOUT_ADS=true
После чего она прекрасно обновилась. Затем собираем антвирусный модуль:/usr/ports/>cd /usr/ports/security/samba-vscan
/usr/ports/security/samba-vscan/>make && make install && make clean

После инсталляции вылазиет инструкция по применению:
You have installed the samba-vscan package.

The vfs object's is in /usr/local/lib/samba.

The configuration files is in /usr/local/etc/samba-vscan.

Edit /usr/local/etc/smb.conf and add the following entry if you are using samba 2.X (that's only an example):

```
 [vscan]
 comment = virus-protected /tmp directory
 path = /tmp
 vfs object = /usr/local/lib/samba/vscan-oav.so
 vfs options = config-file = /usr/local/etc/samba-vscan/vscan-oav.conf
 writeable = yes
 browseable = yes
 guest ok = yes
```

If you are using samba 3.X:

Edit /etc/smb.conf and add the following entry (that's only an example):

```
 [vscan]
 comment = virus-protected /tmp directory
 path = /tmp
 vfs object = vscan-oav
 vscan-oav: config-file = /usr/local/etc/samba-vscan/vscan-oav.conf
 writeable = yes
 browseable = yes
 guest ok = yes
```

Basically you have to add a vfs object line to your shares
which should be virus-protected by this module. If you'd like to use the
run-time configuration file, simply add the
vfs options = config-file = /path/config-file
(different settings for several shares can be achieved by using a different
name of the configuration file for each share). If you want to protect _all_
shares your Samba server offers, simply add the vfs object line (and the
vfs options line, if you like) to the [global] section.

Then restart samba.

По ней всё и делаем - рихтуем /usr/local/etc/smb.conf[global]

```
 workgroup = main_workgroup_name
 netbios name = FREEBSD
 server string = BSD_4-11
 interfaces = sis0
 bind interfaces only = Yes
```

```
 security = SHARE
 encrypt passwords = No
 lanman auth = No
 ntlm auth = No
 client lanman auth = No
 client plaintext auth = No
 announce version = 4.11
 wins support = Yes
 ldap ssl = no
 create mask = 0666
 security mask = 0666
 directory mask = 0777

[main_bsd_share]
 comment = примечание к шаре
 path = /usr/local/smb_fs
 # добавлены следующие две строки:
 vfs object = vscan-clamav
 vscan-clamav: config-file = /usr/local/etc/samba-vscan/vscan-clamav.conf
 read only = No
 guest ok = Yes
```

После чего приводим конфиг vscan к такому виду:
/usr/local/etc/samba-vscan/vscan-clamav.conf

```
[samba-vscan]

max file size = 0
; не забудте, после отладки, поставить
; следующую строчку в `no`
verbose file logging = yes
scan on open = yes
scan on close = yes
deny access on error = no
deny access on minor error = no
send warning message = yes
; в карантин у мя не перемещает -
; порылся в инете - не я один такой. Так и оставил.
; а хотел уже новую коллекцию вирей собирать...
infected file action = delete
quarantine directory  = /tmp/smb_infected
quarantine prefix = vir-
max lru files entries = 100
lru file entry lifetime = 5
exclude file types =
clamd socket name = /var/run/clamav/clamd
```

libclamav max files in archive = 1000
libclamav max archived file size = 10485760
libclamav max recursion level = 5

Ну и всё. Перезапускаем самбу (у меня она остановилась в результате обновления :))
/usr/local/etc/>/usr/local/etc/rc.d/samba.sh restart
Stopping /usr/local/sbin/nmbd.
Waiting for PIDS: 56778.
Stopping /usr/local/sbin/smbd.
Starting SAMBA: removing stale tdbs :
/var/db/samba/connections.tdb
/var/db/samba/messages.tdb
/var/db/samba/sessionid.tdb
/var/db/samba/unexpected.tdb
/var/db/samba/brlock.tdb
/var/db/samba/locking.tdb
Starting nmbd.
Starting smbd.
/usr/local/etc/>

и наблюдаем следующую активность в /var/log/messages: Jan 24 14:17:50 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/A4-2a.jpg is clean
Jan 24 14:17:50 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/A4-1ob.jpg'
Jan 24 14:17:51 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/A4-1ob.jpg is clean
Jan 24 14:17:51 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/Vnytr1.jpg'
Jan 24 14:17:51 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Vnytr1.jpg is clean
Jan 24 14:17:51 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/Vnutr.jpg'
Jan 24 14:17:52 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Vnutr.jpg is clean
Jan 24 14:17:52 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/Vkatalog1.tif'
Jan 24 14:17:53 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Vkatalog1.tif is clean
Jan 24 14:17:53 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/Vkatalog.tif'
Jan 24 14:17:53 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Vkatalog.tif is clean
Jan 24 14:17:53 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/RazvRod.tif'

Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/RazvRod.tif is clean
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/A5Kolle.tif was not modified - not scanned
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/A5.jpg was not modified - not scanned
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/A4-2a.jpg was not modified - not scanned
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/A4-2.jpg was not modified - not scanned
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/A4-1ob.jpg was not modified - not scanned
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Vnytr1.jpg was not modified - not scanned
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Vnutr.jpg was not modified - not scanned
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/RazvRod.jpg'
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/RazvRod.jpg is clean
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Vkatalog1.tif was not modified - not scanned
Jan 24 14:18:05 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Vkatalog.tif was not modified - not scanned
Jan 24 14:18:06 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/Razvorot2.jpg'
Jan 24 14:18:06 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Razvorot2.jpg is clean
Jan 24 14:18:06 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/Razvorot1.jpg'
Jan 24 14:18:07 mail2 smbd_vscan-clamav[58022]: INFO: file /usr/smb/Nastia/Razvorot1.jpg is clean
Jan 24 14:18:07 mail2 smbd_vscan-clamav[58022]: INFO: Scanning file : '/usr/smb/Nastia/Razvorot.tif'

Всё пучком. :) Меняем `verbose file logging` на `no` и перезапускаем самбу ещё раз.
Конечно же, стало медленней - но не так уж и сильно. Работать можно.

P.S. У меня почему-то на заражённые файлы ругается так: ERROR: string overflow by 1 (24 - 23) in safe_strcpy [main_bsd_share]

Пока не разобрался, но - ещё не вечер...