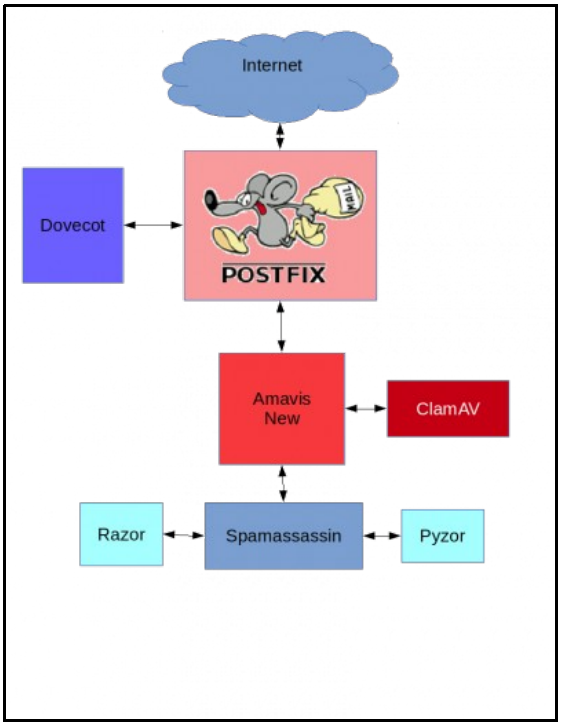
Email Server - MailScanner alapok

Contents

Áttekintés

Email szkennel?nek az AmavisNew programot fogjuk használni. Az AmaivsNew ...



ClamAV-0.98.5

Installálás

Két programot kell felrakni. Magát a clamav vírus keres? programot, és clamd démont, amin keresztül az amaivs hozzá fog csatlakozni a clamAV-hez.

A clamav-t meg kell hívni a megfelel? argumentumokkal, hogy átvizsgáljon egy fájlt vagy egy mappát, tehát nem egy futó démon. Ezzel szemben a clamd-t el kell indítani, hogy folyamatosan fogadja a hozzá beérkez? kéréseket, majd a megfelel? paraméterekkel meghívja a clamav programot, hogy vizsgálja át a neki átadott fájlt, pl. egy email-t.

Ehhez els?ként a EPEL repót hozzá kell adni a yum-hoz.

```
# rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm

# yum install clamav clamd
```

/etc/clamad.conf

```
DatabaseDirectory /var/lib/clamav
User clam

ScanMail yes
ScanArchive yes
```

Vírus definíciók frissítése

A vírus adatbázis frissítését a freshclam program végzi. Ennek van egy saját config fájlja. Ebben fontos, hogy a vírus adatbázis helye ugyan ott legyen, mint amit a clamav.conf-ban megadtunk. /etc/freshclam.conf

```
DatabaseDirectory /var/lib/clamav
DatabaseOwner clam
```

Így kell frissíteni:

```
# /usr/bin/freshclam --no-warnings
```

A telepítés létrehozott egy alap ClamAV frissít? fájlt a /etc/crond.daily-ben. Ezt egészítsük ki azzal, hogy küldje el email-ben a freshclam logját ha lefutott. Írjuk át úgy a freshclam futtatását, hogy ne írjon ki warning-okat, és, szedjük ki a quiet kapcsolót, és az output-ot irányítsuk egy fájlba, amit az emial mellékletéhez csatolni fogunk.

```
/etc/cron.daily/freshclam
!/bin/sh

### A simple update script for the clamav virus database.
### This could as well be replaced by a SysV script.

### fix log file if needed
LOG_FILE="/var/log/clamav/freshclam.log"
if [ ! -f "$LOG_FILE" ]; then
    touch "$LOG_FILE"
    chmod 644 "$LOG_FILE"
    chown clam.clam "$LOG_FILE"
fi

/usr/bin/freshclam \
    --no-warnings \
    --datadir="/var/lib/clamav" \
    --log="$LOG_FILE" \
    > /tmp/freshclam.log


/bin/echo "" | /bin/mail -a /tmp/freshclam.log -s "[SERVER] ClamAV database Refreshment" -r "root" root
```

A mail parancsnak a -r kapcsolóval megadhatjuk a küld?t, de nem szükséges, mert ha nem adunk meg semmit, akkor a küld? a root@system.berki2.org-lesz.

Automatikus fájlrendszer szkennelés

Letölthet? egy okos script, ami elvégzi a megadott mappák vírus vizsgálatát, majd az eredményt elküldi emailben. Hozzunk létre egy karantén mappát, és adjunk rá mindenkinek írási jogot:

```
# mkdir /var/local/virus_quaraintin/dailyScan
# chmod 722 /var/local/virus_quaraintin/dailyScan
```

Tegyük a cron.weekly mappába a szkennel? szkriptet.

/etc/cron.weekly/clam_scan_home.sh

```
#!/bin/bash

# Email alert cron job script for ClamAV
# Original, unmodified script by: Deven Hillard
#(http://www.digitalsanctuary.com/tech-blog/debian/automated-clamav-virus-scanning.html)
# Modified to show infected and/or removed files

# Directories to scan
SCAN_DIR="/home/adam2"

QUARANTINE_DIR="/var/local/virus_quaraintin/dailyScan"

# Location of log file
LOG_FILE="/var/log/clamav/manual_clamscan.log"

# Uncomment to have scan move files
AGGRESSIVE=1
# Uncomment to have scan not move files
#AGGRESSIVE=0

# Email Subject
SUBJECT="[SERVER] ClamAV virus scan result"
# Email To
EMAIL="root"

EMAIL_FROM="root"

SCAN_ARGUMENTS="--scan-archive=yes"

check_scan () {
    # If there were infected files detected, send email alert

    if [ `tail -n 12 ${LOG_FILE}  | grep Infected | grep -v 0 | wc -l` != 0 ]
    then
    # Count number of infections
        SCAN_RESULTS=$(tail -n 10 $LOG_FILE | grep 'Infected files')
        INFECTIONS=${SCAN_RESULTS##* }

        if [ $AGGRESSIVE = 1 ]
        then
                echo -e "\n`tail -n $((10 + ($INFECTIONS*2))) $LOG_FILE`" | /bin/mail -s "${SUBJECT}" -r "${EMAIL_FROM}" ${EMAIL}
        else
                echo -e "\n`tail -n $((10 + $INFECTIONS)) $LOG_FILE`" | /bin/mail -s "${SUBJECT}" -r "${EMAIL_FROM}" ${EMAIL}
        fi
```

```
    else
        /bin/echo "NO virus found" | /bin/mail -s "${SUBJECT}" -r "${EMAIL_FROM}" ${EMAIL}
    fi
}

if [ $AGGRESSIVE = 1 ]
then
        #/usr/bin/clamscan -ri --remove $SCAN_DIR >> $LOG_FILE
        /usr/bin/clamscan -ri --move=$QUARANTINE_DIR $SCAN_ARGUMENTS $SCAN_DIR >> $LOG_FILE


else
        /usr/bin/clamscan -ri $SCAN_ARGUMENTS $SCAN_DIR >> $LOG_FILE
fi

check_scan
```

Adjunk rá futási jogot:

```
# chmod +x /etc/cron.weekly/clam_scan_home.sh
```

Spamassassin

Note
Itt csak az alap Spamassassin konfigurációt végezzük el, ezt fogjuk kib?víteni a Kiterjesztett spam sz?rés cím? fejezetben.

```
# yum install spamassassin
```

Mi hol van

- DEF_RULES_DIR=/usr/share/spamassassin,
- LOCAL_RULES_DIR=/etc/mail/spamassassin
- LOCAL_STATE_DIR=/var/lib/spamassassin

Szabályok frissítése

Spam adatbázis

A Spamassassin szabály adatbázisa a **/var/lib/spamassassin/<verziószám>** mappában található, az esetünkben itt: **/var/lib/spamassassin/3.003001**

Ezen belül minden úgynevezett "csatornának" van egy saját almappája, amiben az adott csatorna szabálygy?jteménye található. A csatorna egy "szervezetnek" a saját szabálygy?jteménye. A hivatalos "gyári" csatorna/szabálygy?jteménye az **update_spamassassin_org** nevet viseli. Ezen felül még rengeteg egyéb nem hivatalos csatorna/szabálygy?jteménye létezik.

A **sa-update** parancsnak meg kell adni, hogy milyen csatornákat frissítsen ill. töltsön le. Ezt a **--channel** kapcsoló után tudjuk megadni, ahol a csatorna/szabálygy?jteménye URL-jét várja.

A hivatalos CentOS repository-ból telepített spamassassin esetében a **sa-update** parancsot a **/usr/share/spamassassin/sa-update.cron** script hívja meg. A csatornákat a /usr/share/spamassassin/sa-update.cron használata esetén a **/etc/mail/spamassassin/channel.d** mappában elhelyezett csatorna leíró fájlokból olvassa ki a script, és ezekkel a csatorna URL-ekkel hívja meg a sa-update parancsot.

Gyárilag két csatorna van a /etc/mail/spamassassin/channel.d mappában, a hivatalos **updates_spamassassin_org** és a széles körben elterjedt **sought_rules_yerp_org**:

```
[root@server channel.d]# ll /etc/mail/spamassassin/channel.d
total 12
-rw-r--r--. 1 root root 2572 Dec  5  2013 sought.conf
-rw-r--r--. 1 root root 4915 Dec  5  2013 spamassassin-official.conf
```

A csatorna leírók fájl elején található a csatorna URL-je, majd ezt követi az a kulcs amivel a frissítéseket aláírja a kibocsájtó. Pl. a **spamassassin-official.conf** fájl eleje az alábbi:

```
# http://wiki.apache.org/spamassassin/RuleUpdates
CHANNELURL=updates.spamassassin.org
KEYID=5244EC45
# Ignore everything below.
return 0

This is the GPG key that updates are signed with (currently,
as of Wed Dec 21 19:31:38 PST 2005.  Please contact <dev /at/
spamassassin.apache.org> with any questions.


-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.2 (SunOS)
.....
```

A **/usr/share/spamassassin/sa-update.cron** script kiolvassa innen az összes csatorna leíró fájlt, és hozzáf?zi a **--channel** paraméterhez a leírókból kiolvasott URL-eket.

Minden csatornának van egy saját almappája és egy csatorna leírója a **/var/lib/spamassassin/3.003001** szabály adatbázis gy?jt?mappában.

```
[root@server 3.003001]# ll /var/lib/spamassassin/3.003001
total 16
drwxr-xr-x. 2 root root 4096 Mar 12  2015 sought_rules_yerp_org
-rw-r--r--. 1 root root  123 Mar 12  2015 sought_rules_yerp_org.cf
drwxr-xr-x. 2 root root 4096 Sep  8 05:53 updates_spamassassin_org
-rw-r--r--. 1 root root 2851 Sep  8 05:53 updates_spamassassin_org.cf
```

Tip
Ezekr?l a mappákról teljesen felesleges biztonsági mentést csinálni, mivel a sa-update mindig a legfrissebb gy?jteményt hozza le.

Warning
Úgy t?nik, hogy a **sought** szabályokhoz már jó ideje nem jön frissítés. A sa-update ezt a választ adja manuális update esetén minden nap:

```
# /usr/bin/sa-update -v --channel sought.rules.yerp.org --gpgkey 6C6191E3
Update finished, no fresh updates were available
```

Amavis ? 2.9.1

Installáció

```
rpm -Uvh http://apt.sw.be/redhat/el6/en/x86_64/rpmforge/RPMS/rpmforge-release-0.5.3-1.el6.rf.x86_64.rpm

# yum install amavisd-new
```

/etc/amavisd/amavisd.conf

```
$daemon_user  = 'amavis';    # (no default;  customary: vscan or amavis), -u
$daemon_group = 'amavis';    # (no default;  customary: vscan or amavis), -g

$mydomain = 'berki2.org';
...
$myhostname = 'berki2.org';  # must be a fully-qualified domain name!

############################################################
# Virusok karantén mappába + értesítés=admin, felhasználó
############################################################
$QUARANTINEDIR = '/var/spool/amavisd/quarantine';
$virus_quarantine_method = 'local: virus-%m'; # Filename in $QUARANTINEDIR
$virus_quarantine_to = 'virus-quarantine';
$virus_admin = "adam\@berki.org";
$warnvirusrecip = 1;

$mailfrom_notify_admin     = "root\@berki.org";                    # notifications sender
$mailfrom_notify_recip     = "root\@berki.org";                    # notifications sender
$mailfrom_notify_spamadmin = "root\@berki.org";                    # notifications sender

############################################################
# Rossz fejléc karantén mappába + értesítés=adimin
############################################################
$bad_header_quarantine_method = 'local: bad_header-%m'; # Filename in $QUARANTINEDIR
$bad_header_quarantine_to = 'bad_header-quarantine';
$bad_header_admin = "adam\@berki.org";

#################################################################
# Tiltott formátum karantén mappába + értesítés=admin, felhasználó
#################################################################
$banned_files_quarantine_method = 'local: banned-%m'; # Filename in $QUARANTINEDIR
$banned_quarantine_to = 'banned-quarantine';
$banned_admin = "adam\@berki.org";
$warnbannedrecip = 1;
$warnbannedsender = 1;

#################################################################
# SPAM kezelés
#################################################################

#Spam értékek beállítása
#########################
$sa_spam_subject_tag = '***Spam*** ';
$sa_tag_level_deflt  = 2.0;  # add spam info headers if at, or above that level
$sa_tag_level_deflt  = -999;  # add 'spam detected' headers at that level
$sa_kill_level_deflt = 6.9;  # triggers spam evasive actions (e.g. blocks mail)
$sa_dsn_cutoff_level = 10;   # spam level beyond which a DSN is not sent
$sa_crediblefrom_dsn_cutoff_level = 18; # likewise, but for a likely valid From
# $sa_quarantine_cutoff_level = 25; # spam level beyond which quarantine is off
$penpals_bonus_score = 8;    # (no effect without a @storage_sql_dsn database)
$penpals_threshold_high = $sa_kill_level_deflt;  # don't waste time on hi spam
$bounce_killer_score = 100;  # spam score points to add for joe-jobbed bounces


#Spamek elküldése emailcímre értesítése nélkül.
################################################
$spam_quarantine_method = 'smtp:[127.0.0.1]:10025';
$spam_quarantine_to = 'system@berki2.org';


$sa_debug = 1;
$log_level = 5;


1;  # insure a defined return value
```

Szerintem ami már a config-ban fentebb is szerepelt, azt nem kell kiszedni, mert itt felülírjuk. Meg kell adni a mydomain és a myhostname paramétereket, szerintem nem fotnos, hogy mit írunk oda.

A **$sa_tag_level_deflt = -999;** beállításával rákényszerítjük az amavis-t hogy mindig belerakja a header-be a spam sz?rés végeredményét, még akkor is ha nem gondolja spam-nek az üzenetet.

A **$sa_debug = 1;** és a **$log_level = 5;** el maximálisra emeltük az amavis + spamassassin logolását. Ez a kísérletez? id?szakban nagyon praktikus.

Note
Az amavis azért tudja kiküldeni a figyelmeztetéseket is publikus email címekre, mert meg van adva a sneder mind három esetre:

```
$mailfrom_notify_admin     = "root\@berki.org";                  # notifications sender
$mailfrom_notify_recip     = "root\@berki.org";                  # notifications sender
$mailfrom_notify_spamadmin = "root\@berki.org";                  # notifications sender
```

Ha ez nem lenne megadva, akkor a publikus email szerverek eldobálnák a figyelmeztet? leveleket.

/etc/cron.daily/amavisd

```
/usr/sbin/tmpwatch 24 /var/spool/amavisd/tmp
/usr/sbin/tmpwatch -d 720 /var/spool/amavisd/quarantine
```

A tmpwatch kitörli azokat a fájlokat, amihez egy megadott ideig nem nyúlt senki. A conrtab-ban az van beállítva, hogy törölje a tmp mappából azokat a fájlokat, amiket 24 óráig senki nem nyúlt hozzá, és a karanténból azokat a fájlokat, amiket 720 óráig (30 nap) senki nem nézett meg.

```
# mkdir -p /var/spool/amavisd/quarantine
# chown amavis:amavis /var/spool/amavisd/quarantine
# chmod 750 /var/spool/amavisd/quarantine
```

Indítsuk el:

```
# service amavisd start
# chkconfig amavisd on
```

Vírus sz?rés - clamd

A clamd démon fogadja a kéréseket a Amavis-töl, és meghívja a ClamAV-t a levelek átvizsgálására. A clamd és az amaivs egy socket-en keresztük kommunikálnak. Ezt a clamd.conf-ban és az amavisd.conf-ban fontos, hogy ugyan arra állítsuk, és mind két démon tudja írni ezt a fájlt.

/etc/clamad.conf

```
...
LocalSocket /var/run/clamav/clamd.sock
...
User clam
...
AllowSupplementaryGroups yes
...
```

Indítsuk el a clamd-t.

```
# service clamd start
# chkconfig clamd on
```

Ekkor létrejön a clamd.sock socket fájl.

Nézzük meg, hogy kinek a tulajdonában van

```
# ls -l /var/run/clamav/clamd.sock
srw-rw-rw-. 1 clam clam 0 Jan 31 17:06 /var/run/clamav/clamd.sock
```

Láthatjuk, hogy a clam user és csoport tulajdonában van, és a csoport írhatja és olvashatja a fájlt. Ezért fontos, hogy az amaivis user is benne legyen a clam csoportba, hogy tudja írni a socektet ? is.

```
# usermod -G amavis clam
# cat /etc/group | grep clam
clam:x:489:
amavis:x:488:clam
```

Ezen felül, meg kell engedni, hogy a /var/spool/amavisd mappát a csoport is tudja írni. Ez ahhoz kell, hogy a clamd is bele tudjon írni a mappába.

```
# chmod g+rx /var/spool/amavisd/tmp

/etc/amavisd/amavisd.conf
 ['ClamAV-clamd',
    \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.sock"],
    qr/\bOK$/m, qr/\bFOUND$/m,
    qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
```

Az amaivis az amaivis user és gourp nevében fut. Ami nagyon fontos, hogy a ClamAV-clamd szekcióban a socket fájl ugyan az legyen mint ami clamd.conf-ban meg van adva. Ezt ellen?rizzük.

Spam sz?rés - spamd

Ahhoz hogy az amaivs át tudja adni a leveleket, a clmad-hez hasonló démont kell elindítani, a spamd démont. Indítsuk el:

```
# service spamassassin start
# chkconfig spamassassin on
```

Az amavis-nak nem kell megmondani, hogy hol van a spamd, mert alapértelmezés szerint azt akarja használni. Amúgy így kéne megadni az amavis.conf-ban:

```
@spam_scanners = ( ['SpamAssassin', 'Amavis::SpamControl::SpamAssassin'] );
```

Posfix integráció

A postfix-ben be kell állítani, hogy minden emailt adjon át kézbesítés el?tt az Amavis-nak az 10024-es portra, és fogadja azokat, mikor az amavis visszaküldi az 10025-ös porton.

Ehhez két új szolgáltatást kell beállítani a /etc/postfix/maser.cf-ben.

```
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
amavisfeed unix    -       -       n        -      2     lmtp
    -o lmtp_data_done_timeout=1200
    -o lmtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
    -o max_use=20

# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
127.0.0.1:10025 inet n    -       n       -       -     smtpd
    -o content_filter=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_data_restrictions=reject_unauth_pipelining
    -o smtpd_end_of_data_restrictions=
    -o smtpd_restriction_classes=
    -o mynetworks=127.0.0.0/8
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_milters,no_address_mappings
    -o local_header_rewrite_clients=
    -o smtpd_milters=
    -o local_recipient_maps=
    -o relay_recipient_maps=
```

Az els? azon szolgáltatás, ami átadja a leveleket az Amavis-nak. A neve fontos, mert majd ezzel kell rá hivatkozni a main.cf-ben. A második szolgáltatás fogadja az Amavis-t?l visszaérkez? leveleket. Az itt felsorolt paraméterek mind felülírják a main.cf-ben felsorolt értékeket.

A main.cf végére pedig be kell állítani, hogy a leveleket adja

```
############################
# AMAVIS
############################
content_filter = amavisfeed:[127.0.0.1]:10024
```

Üzenet hozzárakása a kimen? levelekhez (disclaimer)

Vagy a kimen? vagy a bejöv? levelekhez hozzá lehet csapni egy üzenetet, amennyiben a levelet tisztának találta az Amavis. Egyszerre mind két irányban nekem nem sikerült. Az alábbi a kimen? levelekhez csapja hozzá az üzenetet. Ezt az altermime program segítségével tesszük meg, ami az emailek manipulálását teszi lehet?vé. Ehhez els?ként meg kell mondani az amaivis-nak hogy hol van az altermime, majd meg kell adni a két üzenet fájlt. Egy sima szöveges és egy html-es változatot. Az amavis a sima szöveges levelekhez a txt-s fájlt fogja hozzácsapni, míg a html üzenetekhez a html fájlt. A karakter kódolást nem tudom hogy lehet állítani, ezért ékezetek nélkül írtam.

```
$altermime = '/usr/bin/altermime';

@altermime_args_disclaimer =
  qw(--verbose  --disclaimer=/var/spool/amavisd/disclaimer.txt \
     --disclaimer-html=/var/spool/amavisd/disclaimer.html);
$defang_maps_by_ccat{+CC_CLEAN} = [ 'disclaimer' ];

$allow_disclaimers = 1;
```

Ezen felül az összes policy_bank belsejébe kapcsoljuk be disclaimer küldést.

```
$policy_bank{....} = {
   ...
  allow_disclaimers => 1,
  ...
}
```

Értesítések lokalizációja

Ha az email vírusos volt, vagy tiltott csatolmányt tartalmazott, akkor az amaivs a küld?nek és a címzettnek értesítést küld. Alapértelmezés szerint ehhez hard kódolt emial templétet használ. Ezeket felül lehet definiálni. Hozzunk létre egy mappát a /etc/amaivsd/ alatt hu_HU néven. Ebben kötelez?en el kell helyezni az alábbi fájlokat:

- /etc/amavisd/hu_HU/charset
- /etc/amavisd/hu_HU/template-dsn.txt
- /etc/amavisd/hu_HU/template-spam-admin.txt
- /etc/amavisd/hu_HU/template-spam-sender.txt
- /etc/amavisd/hu_HU/template-virus-admin.txt
- /etc/amavisd/hu_HU/template-virus-recipient.txt
- /etc/amavisd/hu_HU/template-virus-sender.txt

Ezek letölthet?k angolul több változatban is, bár nem túl egyszer? megtalálni ?ket. A legfontosabb a charset fájl. Itt meg kell mondani, hogy milyen karakter kódolású fájlokat használunk:

```
/etc/amavisd/hu_HU/charset
utf-8
ignored lines after first one
```

Az amavisd.conf végére, az 1-es elé írjuk oda:

```
read_l10n_templates('/etc/amavisd/hu_HU');


1;  # insure a defined return value
```

A templét fájlokból két fontos van számunkra, csak ezeket kell lefordítani:

- /etc/amavisd/hu_HU/template-virus-recipient.txt
- /etc/amavisd/hu_HU/template-virus-sender.txt

A nevükkel ellentétben, ezeket nem csak vírusos üzenetek esetében használja. Ugyan ezt a templétet használja a szabálytalan header, a tiltott csatolmány, a spam és a vírusos üzenetek küld?jének és címzettjének értesítésére. Az Amaivs-2.9-es verziója már nem tud értesítést küldeni a vírus feladójának, a **$ warnvirussender = 1** paramétert nem viszi már figyelembe.

Tesztelés

Ha már m?ködik az alap rendszer, teszteljük le a rendszert.

Spam sz?rés tesztelése

Küldeni fogunk a parancssorból egy SPAM üzenetet a szervernek, és meg fogjuk nézni, hogyan fogja feldolgozni.

Töltsük le a spam-eket tartalmazó email-eket innen: File:Spam teszt levelek.tar

Mindig kell címzett. Vagy implicit megadjuk:

```
# sendmail adam@berki2.org < spam1.eml
```

vagy megmondjuk, hogy szedje ki a levélb?l.

```
# sendmail -t < spam1.eml
```

Nézzük meg a /var/log/maillog-ban az üzenet feldolgozását:

```
Sep 26 20:56:28 centostest amavis[1505]: (01505-02) Blocked SPAM {RejectedInternal,Quarantined}, ORIGINATING LOCAL [127.0.0.1] [59.99.75.77]
```

A rendszerünk úgy van beállítva, hogy a spam üzeneteket ne a karantén mappába másolja, hanem küldje el a system user-nek. Most vizsgáljuk meg az email header-jét:

```
X-Quarantine-ID: <WlQeNLMXlflo>
X-Spam-Flag: YES
X-Spam-Score: 29.093
X-Spam-Level: *****************************
X-Spam-Status: Yes, score=29.093 tag=2 tag2=6.2 kill=6.9
        tests=[DATE_IN_FUTURE_03_06=2.426, DIGEST_MULTIPLE=0.001,
        FREEMAIL_FROM=0.001, HTML_MESSAGE=0.001, PYZOR_CHECK=1.985,
        RAZOR2_CF_RANGE_51_100=0.365, RAZOR2_CF_RANGE_E8_51_100=2.43,
        RAZOR2_CHECK=1.729, RCVD_IN_BRBL_LASTEXT=1.644, RCVD_IN_PBL=3.558,
        RCVD_IN_PSBL=2.7, RCVD_IN_SBL_CSS=3.558, RCVD_IN_XBL=0.724,
        RDNS_NONE=1.274, URIBL_ABUSE_SURBL=1.948, URI_WP_DIRINDEX=2.996,
        URI_WP_HACKED_2=1.753] autolearn=unavailable
```

Ezeket a mez?ket az email kliensek tudják értelmezni.