Relazione esercitazione 4 Laboratorio di reti
Server Mail con Postfix e Dovecot

Franco Masotti Danny Lessio

April 26, 2015

Contents

Part I
Configurazione ed installazione del server mail

1 Scopo dell'esercitazione

L'obbiettivo di questa esercitazione é quello di realizzare un server mail completo sia dal punto di vista delle funzionalitá sia da quello della sicurezza.

2 Componenti

Tutti gli strumenti necessari sono presenti sia nei repository ufficiali sia in quelli non ufficiali. Di seguito sono elencati componenti e scopo:

- Server SMTP
  - Il server SMTP ha lo scopo di inviare la posta.
  - Per questo componente abbiamo utilizzato `Postfix`[1] .
- Server IMAP
  - Questo server ha lo scopo di ricevere la posta grazie alle notifiche del server SMTP.
  - Il componente che abbiamo usato é `Dovecot`[2]
- Autenticazione degli utenti
  - Abbiamo effettuato l'autenticazione degli utenti LDAP con `PAM`[3], in particolare con il pacchetto `nss-pam-ldapd`[4] . Questo tipo di autenticazione vale sia per Dovecot sia per Postfix (che sfrutta proprio Dovecot per questo).
- Sicurezza
  - Per controllare le mail abbiamo usato `ClamAv`[5] e `Spamassassin`[6]. Il primo serve a verficare la presenza di virus mentre il secondo per avvertire il destinatario che si tratta di spam.
  - Per mettere in comunicazione questi due programmi con Postfix abbaimo usato `Amavis`[7]
- Mail aliases

[1]http://www.postfix.org/
[2]http://dovecot.org/
[3]http://linux-pam.org
[4]https://www.archlinux.org/packages/community/x86_64/nss-pam-ldapd/
[5]http://www.clamav.net/
[6]http://spamassassin.apache.org
[7]http://www.ijs.si/software/amavisd/

  - Per effettuare il mail aliasing, cioé la traduzione da un nome mail alternativo al nome reale abbiamo utilizzato Postfix che va ad attingere direttamente al database LDAP.

- SSL/TLS
  - Tutte le comunicazioni sia in entrata, sia in uscita, sono protette con SSL/TLS sfruttando i certificati di OpenLDAP. Questo lo si puó vedere nei file di configurazione di Postfix e Dovecot.
  - Inoltre non é possibile utilizzare comunicazioni *non* protette.

3 Postfix

Nel file `main.cf` si trovano le impostazioni di base valide per tutti i socket in ascolto, mentre in `master.cf` é possibile definire nuovi socket e fare l'override delle impostrazioni (anche aggiungendone di nuove).

main.cf:

- Abbiamo configurato Postfix in modo che utilizzi le directory di tipo `Maildir`. In questo modo viene creata tale directory nella home di ogni utente nella quale viene recapitata la posta.
- Abbiamo configurato dominio ed hostname del server SMTP rispettivamente con `gruppo2.labreti.it` e `mail.gruppo2.labreti.it`
- Grazie alla direttiva `alias_maps` é possibile utilizzare gli alias mail salvati nell'albero LDAP. Abbiamo creato un file chiamato `ldap-aliases.cf` in cui é definito come recuperare il nome originario.
- Per fare in modo che l'utente venga notificato dell'arrivo di nuova posta (grazie a Dovecot) bisogna esplicitare il valore di `mailbox_command`
- Abbiamo anche abilitato esplicitamente l'ascolto in IPv4 ed IPv6.

master.cf:

- All'interno di questo file abbiamo definito la porta 587 (vedi RFC 2476[8]) come porta in ascolto sicura. Infatti SSL/TLS é abilitato di default. Se non fosse cosí basterebbe fare sniffing del traffico per intercettare le password di autenticazione oltre che per leggere la posta. Tutto questo é stato possibile anche grazie ai certificati precedentemente generati per OpenLDAP.
- Per mettere in comunicazione anti-virus e anti-spam abbiamo aperto la porta 10024 (socket di tipo unix) e la porta 10025 (socket di tipo inet). La prima é utlizzata da Postfix per mandare ad Amavis le email da scansionare mentre la seconda da Amavis per mandare indietro a Postfix le email valide.
- Per autenticare gli utenti, in modo che solo chi é registrato con username e password possa inviare email, piuttosto che dover installare e configurare un nuovo pacchetto abbiamo utilizzato l'autenticazione con `SASL` di Dovecot per tutti gli utenti (sia rete interna, sia rete esterne). Questo lo si vede con la direttiva `-o smtpd_sasl_type=dovecot` .

[8] http://www.ietf.org/rfc/rfc2476.txt

ldap-aliases.cf:

- Nell'albero LDAP abbiamo creato un'organizational unit chiamata `ALIAS`. Ogni utente é definito attraverso il campo `rfc822MailMember` che corrisponde al campo `uid` nell' organizational unit `PEOPLE`. Il campo `cn` rappresenta l'alias.
- La ricerca viene quindi fatta sul sottoalbero `ALIAS` con `query_filter = (&(cn=%s)(objectClass=nisMailAlias))` cioé viene cercato l'alias con il cn corrispondente, e che faccia parte della classe `nisMailAlias` (usata solo dagli alias). Il valore ritornato é di tipo `rfc822MailMember` (vedi lda direttiva: `result_attribute = rfc822MailMember`) .

4 Dovecot

Dovecot contiene molti fie di configurazione ma per semplicitá abbiamo raggruppato tutto in `dovecot.conf` dopo aver eliminato tutti i commenti.

dovecot.conf

- Per leggere la posta utilizziamo esclusivamente il protocollo `IMAP` che permette agli utenti la mobilitá. Le mail (ed il loro stato) sono salvate sul server. Con il protocollo `POP` al conrario si impone di scaricare la mail dal server per poi cancellarle da questo e comunque non fornisce sincronizzazione. POP non é adatto alla gestione delle mail tra piú dispositivi e per questo motivo sta cadendo in disuso.
- Anche per Dovecot va definito il tipo di mailbox, che deve essere dello stesso tipo di Postfix (vedi la direttiva: `mail_location = maildir: /Maildir`) .
- Anche in questo caso abbiamo utilzzato le chiavi pubbliche e private di OpenLDAP per l'SSL/TLS di Dovecot con le direttive `ssl_cert` ed `ssl_key`.
- NSS permette di mappare gli utenti LDAP e di simularli come se fossero appartenenti al sistema[9], PAM invece ne permette solo l'autenticazione. Se un utente si logga per la prima volta allora viene creata la sua home directory (dove verranno salvate le mail). La creazione automatica delle home é garantita dalla direttiva `args = session=yes dovecot` e dal modulo `pam_mkhomedir.so` presente nel file `dovecot` di PAM .
- Come accennato precedentemente, Dovecot si occupa anche dell'autenticazione SMTP attraverso SASL. Avermmo potuto utilizzare l'implementazione di SASL provvista nella libreria `cyrus-sasl`[10] ma abbiamo notato che Dovecot possiede giá la propria implementazione di SASL, quindi abbiamo utilizzato tale sistema senza installare altri pacchetti (vedi la direttiva `service_auth`).

5 Amavis

Amavis é un'interfaccia fra il mail server SMTP (Postfix) e i mail filters (ClamAV e Spamassassin). Abbiamo installato prima ClamAV (un anti-virus libero), poi abbiamo aggiornato i suoi database con il comando `freshclam`. Successivamente lo abbiamo testato con il test virus `EICAR`[11] . Infine abbiamo modificato amavis.conf in modo da abilitare la scansione dei virus.

[9] si puó verificare con `getnent passwd`

[10] https://www.archlinux.org/packages/extra/x86_64/cyrus-sasl/

[11] http://www.eicar.org/86-0-Intended-use.html

Amavis é in grado di gestire la configurazine di Spamassassin (da installare separatamente poiché non é fornita un'implementazione). Infatti all'interno di amavis.conf si possono modificare alcuni parametri di Spamassassin tra cui anche l'efettiva attivazione del servizio.

Amavis é comunque in grado di gestire un'ampia varietá di antivirus quindi non é limitato a ClamAV.

Part II
Test

6 Verifica delle funzionalitá

Per testare gradualmente le nostre configurazioni abbiamo usato telnet, OpenSSL e Sylpheed[12] (un client di posta grafico). Abbiamo effettuato tre tipi di test finali:

- Mail normale:

```
apr 23 18:00:50 antergos amavis[2455]: (02455-01) Passed CLEAN {RelayedInternal},
MYNETS LOCAL [192.168.2.1]:44188
<dannylessio@mail.gruppo2.labreti.it> -> <jacktripper@mail.gruppo2.labreti.it>,
Queue-ID: 9E0DB24270A, Message-ID:
<20150423180030.8d49490ef0555c080a0b2e8c@mail.gruppo2.labreti.it>, mail_id:
65zA1DuN5P5h, Hits: -1.01, size: 799, queued_as: E88A72426C3, 10260 ms
```

- Mail spam:

```
apr 23 18:01:34 antergos amavis[2456]: (02456-01) Passed SPAMMY
{RelayedTaggedInternal}, MYNETS LOCAL [192.168.2.1]:44193
<jacktripper@mail.gruppo2.labreti.it> -> <dannylessio@mail.gruppo2.labreti.it>,
Queue-ID: 51A7124270C, Message-ID:
<20150423180124.6329dd42269b72556e2fb340@mail.gruppo2.labreti.it>, mail_id:
FUf99b9scvM4, Hits: 3.453, size: 813, queued_as: 8DE512426E5, 10217 ms
```

- Mail contenente virus di prova:

```
apr 23 18:02:38 antergos amavis[2455]: (02455-02) Blocked BANNED
(application/x-msdownload,.dat,eicar.com) {DiscardedInternal,Quarantined},
MYNETS LOCAL [192.168.2.1]:44196 <dannylessio@mail.gruppo2.labreti.it> ->
<jacktripper@mail.gruppo2.labreti.it>, quarantine: banned-wKIkH7wpTbg2,
Queue-ID: 8C22A24270D, Message-ID:
<20150423180238.207d7c28e55468544ea4f410@mail.gruppo2.labreti.it>, mail_id:
wKIkH7wpTbg2, Hits: -, size: 1390, 79 ms
```

[12] http://sylpheed.sraoss.jp/en/

Part III
Listati

7 main.cf

/etc/postfix/main.cf
File di configurazione principale di Postfix.

```
#
# main.cf
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
    masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
    modify
# it under the terms of the GNU General Public License as
    published by
# the Free Software Foundation, either version 3 of the License,
    or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
    License
# along with networks-lab.  If not, see <http://www.gnu.org/
    licenses/>.
#


alias_database = $alias_maps
alias_maps = hash:/etc/postfix/aliases, ldap:/etc/postfix/ldap-
    aliases.cf
command_directory = /usr/bin
compatibility_level = 2
daemon_directory = /usr/lib/postfix/bin
data_directory = /var/lib/postfix
debug_peer_level = 2
debugger_command = PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/
    bin ddd $daemon_directory/$process_name $process_id & sleep 5
home_mailbox = Maildir/
```

```
html_directory = no
inet_interfaces = all
inet_protocols = ipv4, ipv6
mail_owner = postfix
mailbox_command = /usr/lib/dovecot/dovecot-lda -f "$SENDER" -a "
   $RECIPIENT"
mailq_path = /usr/bin/mailq
manpage_directory = /usr/share/man
meta_directory = /etc/postfix
mydestination = $myhostname
mydomain = gruppo2.labreti.it
myhostname = mail.gruppo2.labreti.it
mynetworks = 127.0.0.0/8
mynetworks_style = host
myorigin = $myhostname
newaliases_path = /usr/bin/newaliases
queue_directory = /var/spool/postfix
readme_directory = /usr/share/doc/postfix
sample_directory = /etc/postfix
sendmail_path = /usr/bin/sendmail
setgid_group = postdrop
shlib_directory = /usr/lib/postfix
unknown_local_recipient_reject_code = 550
```

8 master.cf

/etc/postfix/master.cf

File di configurazione dei socket di Postfix. Qui vengono inserite le opzioni di sicurezza e di autenticazione.

```
#
# master.cf
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
   masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
   modify
# it under the terms of the GNU General Public License as
   published by
# the Free Software Foundation, either version 3 of the License,
   or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
   License
# along with networks-lab.  If not, see <http://www.gnu.org/
   licenses/>.
#



#
# Postfix master process configuration file.  For details on the
   format
# of the file, see the master(5) manual page (command: "man 5
   master" or
# on-line: http://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this
   file.
#
#
   ====================================================================

# service type  private unpriv  chroot  wakeup  maxproc command +
   args
```

```
#               (yes)   (yes)   (no)    (never) (100)
#
    ==========================================================================


##########################
#
# antispam & antivirus section
#
amavisfeed      unix  -    -       n       -       2       smtp
 -o smtp_data_done_timeout=1200
 -o smtp_send_xforward_command=yes
 -o disable_dns_lookups=yes
 -o max_use=20
127.0.0.1:10025 inet n  -       y       -       -       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_restrictions_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
 -o local_header_rewrite_clients=
##########################

#smtp      inet  n       -       n       -       -       smtpd
#smtp      inet  n       -       n       -       1
   postscreen
smtpd     pass  -       -       n       -       -       smtpd
#dnsblog   unix  -       -       n       -       0       dnsblog
#tlsproxy  unix  -       -       n       -       0       tlsproxy

##########################
# SSL RFC port 587
submission inet n       -       n       -       -       smtpd
  # SSL
  -o smtpd_use_tls=yes
  -o smtpd_enforce_tls=yes
  -o smtpd_tls_auth_only=yes
```

```
  -o smtpd_tls_wrappermode=yes
  -o smtpd_tls_security_level=encrypt
  -o smtpd_tls_key_file=/etc/openldap/ssl/slapdkey.pem
  -o smtpd_tls_cert_file=/etc/openldap/ssl/slapdcert.pem
  -o smtpd_tls_loglevel=1
  -o smtpd_tls_received_header=yes
  -o smtpd_tls_session_cache_timeout=3600s
  -o tls_random_source=dev:/dev/urandom
  # Amavis
  -o content_filter=amavisfeed:[127.0.0.1]:10024
  # SASL authentication with dovecot
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=private/auth
  -o smtpd_sasl_security_options=noanonymous
  -o smtpd_sasl_local_domain=$myhostname
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,
     reject_unknown_recipient_domain,permit_sasl_authenticated,
     reject

##########################
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING

#  -o content_filter=spamassassin
#  -o receive_override_options=no_address_mappings

#spamassassin   unix   -     n       n      -       -       pipe
#       user=spamd argv=/usr/bin/vendor_perl/spamc -f -e /usr/sbin
   /sendmail -oi -f ${sender} ${recipient}

#smtps     inet  n       -       n       -       -       smtpd
#  -o syslog_name=postfix/smtps
#  -o smtpd_tls_wrappermode=yes
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#628       inet  n       -       n       -       -       qmqpd
```

```
pickup    unix  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      unix  n       -       n       300     1       qmgr
#qmgr     unix  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-
   rewrite
bounce    unix  -       -       n       -       0       bounce
defer     unix  -       -       n       -       0       bounce
trace     unix  -       -       n       -       0       bounce
verify    unix  -       -       n       -       1       verify
flush     unix  n       -       n       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       n       -       -       smtp
relay     unix  -       -       n       -       -       smtp
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
retry     unix  -       -       n       -       -       error
discard   unix  -       -       n       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       n       -       1       anvil
scache    unix  -       -       n       -       1       scache
#
#
   ==========================================================================

# Interfaces to non-Postfix software. Be sure to examine the
   manual
# pages of the non-Postfix software to find out what options it
   wants.
#
# Many of the following services use the Postfix pipe(8) delivery
# agent.  See the pipe(8) man page for information about ${
   recipient}
# and other message envelope options.
#
   ==========================================================================

#
# maildrop. See the Postfix MAILDROP_README file for details.
# Also specify in main.cf: maildrop_destination_recipient_limit=1
#
#maildrop  unix  -       n       n       -       -       pipe
#  flags=DRhu user=vmail argv=/usr/local/bin/maildrop -d ${
   recipient}
```

```
#
#
    ==========================================================================

#
# Recent Cyrus versions can use the existing "lmtp" master.cf
    entry.
#
# Specify in cyrus.conf:
#   lmtp    cmd="lmtpd -a" listen="localhost:lmtp" proto=tcp4
#
# Specify in main.cf one or more of the following:
#  mailbox_transport = lmtp:inet:localhost
#  virtual_transport = lmtp:inet:localhost
#
#
    ==========================================================================

#
# Cyrus 2.1.5 (Amos Gouaux)
# Also specify in main.cf: cyrus_destination_recipient_limit=1
#
#cyrus     unix  -       n       n       -       -       pipe
#  user=cyrus argv=/cyrus/bin/deliver -e -r ${sender} -m ${
    extension} ${user}
#
#
    ==========================================================================

#
# Old example of delivery via Cyrus.
#
#old-cyrus unix  -       n       n       -       -       pipe
#  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} $
    {user}
#
#
    ==========================================================================

#
# See the Postfix UUCP_README file for configuration details.
#
#uucp      unix  -       n       n       -       -       pipe
#  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!
    rmail ($recipient)
#
#
    ==========================================================================
```

```
#
# Other external delivery methods.
#
#ifmail    unix  -       n       n       -       -       pipe
#  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop (
   $recipient)
#
#bsmtp     unix  -       n       n       -       -       pipe
#  flags=Fq. user=bsmtp argv=/usr/local/sbin/bsmtp -f $sender
   $nexthop $recipient
#
#scalemail-backend unix -       n       n       -       2
   pipe
#  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-
   store
#  ${nexthop} ${user} ${extension}
#
#mailman   unix  -       n       n       -       -       pipe
#  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman
   .py
#  ${nexthop} ${user}
```

9 ldap-aliases.cf

/etc/postfix/ldap-aliases.cf

File di configurazione per il recupero del nome originario (con LDAP) a partire dall'alias.

```
#
# ldap-aliases.cf
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
    masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
    modify
# it under the terms of the GNU General Public License as
    published by
# the Free Software Foundation, either version 3 of the License,
    or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
    License
# along with networks-lab.  If not, see <http://www.gnu.org/
    licenses/>.
#


server_host = ldap://192.168.2.1
search_base = ou=ALIAS,dc=gruppo2,dc=labreti,dc=it
query_filter = (&(cn=%s)(objectClass=nisMailAlias))
result_attribute = rfc822MailMember
bind = no
scope = sub
version = 3
```

10 File ldif con gli alias degli utenti

gruppo2.labreti.it.aliases.ldif

Il file contiene gli alias degli utenti oltre che l'ou ALIAS ed il record MX (*Mail eXchange server*) che indica semplicemente qual é il server mail del dominio.

```
#
# gruppo2.labreti.it.aliases.ldif
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
    masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
    modify
# it under the terms of the GNU General Public License as
    published by
# the Free Software Foundation, either version 3 of the License,
    or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
    License
# along with networks-lab.  If not, see <http://www.gnu.org/
    licenses/>.
#


# Name server.
dn: relativeDomainName=mail,zoneName=gruppo2.labreti.it,ou=HOST,dc
    =gruppo2,dc=labreti,dc=it
objectClass: dNSZone
relativeDomainName: mail
zoneName: gruppo2.labreti.it
dNSTTL: 86400
dNSClass: MX
aRecord: 192.168.2.10
aAAARecord: 2002:0000:0000:0000:0000:0000:0000:000a

# Reverse mx entries.

# ALIAS, gruppo2.labreti.it
dn: ou=ALIAS,dc=gruppo2,dc=labreti,dc=it
```

```
ou: ALIAS
objectClass: organizationalUnit

# Mail aliases.
dn: cn=franco.masotti,ou=ALIAS,dc=gruppo2,dc=labreti,dc=it
objectClass: top
objectClass: nisMailAlias
cn: franco.masotti
rfc822MailMember: francomasotti

dn: cn=danny.lessio,ou=ALIAS,dc=gruppo2,dc=labreti,dc=it
objectClass: top
objectClass: nisMailAlias
cn: danny.lessio
rfc822MailMember: dannylessio

dn: cn=jack.tripper,ou=ALIAS,dc=gruppo2,dc=labreti,dc=it
objectClass: top
objectClass: nisMailAlias
cn: jack.tripper
rfc822MailMember: jacktripper

dn: cn=janet.wood,ou=ALIAS,dc=gruppo2,dc=labreti,dc=it
objectClass: top
objectClass: nisMailAlias
cn: janet.wood
rfc822MailMember: janetwood
```

11 dovecot.conf

/etc/dovecot/dovecot.conf
File di configurazione di Dovecot.

```
#
# dovecot.conf
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
    masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
    modify
# it under the terms of the GNU General Public License as
    published by
# the Free Software Foundation, either version 3 of the License,
    or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
    License
# along with networks-lab.  If not, see <http://www.gnu.org/
    licenses/>.
#


# 2.2.16: /etc/dovecot/dovecot.conf
auth_debug = yes
auth_debug_passwords = yes
auth_mechanisms = plain login
base_dir = /var/run/dovecot/
mail_location = maildir:~/Maildir
namespace inbox {
  inbox = yes
  location =
  mailbox Drafts {
    special_use = \Drafts
  }
  mailbox Junk {
    special_use = \Junk
  }
  mailbox Sent {
```

```
    special_use = \Sent
  }
  mailbox "Sent Messages" {
    special_use = \Sent
  }
  mailbox Trash {
    special_use = \Trash
  }
  prefix =
}
passdb {
  args = session=yes dovecot
  driver = pam
}
postmaster_address = manjaro@mail.gruppo2.labreti.it
protocols = imap
service auth {
  unix_listener /var/spool/postfix/private/auth {
    group = postfix
    mode = 0660
    user = postfix
  }
  user = root
}
ssl_cert = </etc/openldap/ssl/slapdcert.pem
ssl_key = </etc/openldap/ssl/slapdkey.pem
userdb {
  driver = passwd
}
```

12 File di autenticazione di PAM per Dovecot

`/etc/pam.d/dovecot`

File di configurazione per l'autenticazione degli utenti di sistema ed LDAP. Da notare i moduli `pam_mkhomedir.so` per la creazione automatica delle cartelle home e il modulo `pam_ldap.so` per il collegamento al database LDAP.

```
#
# dovecot
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
    masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
    modify
# it under the terms of the GNU General Public License as
    published by
# the Free Software Foundation, either version 3 of the License,
    or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
    License
# along with networks-lab.  If not, see <http://www.gnu.org/
    licenses/>.
#


auth    sufficient      pam_ldap.so
auth    required        pam_unix.so     nullok
account sufficient      pam_ldap.so
account required        pam_unix.so
session required        pam_mkhomedir.so skel=/etc/skel umask=0022
session sufficient      pam_ldap.so
```

13 nslcd.conf

/etc/nslcd.conf

File di configurazione di nslcd (local LDAP name service daemon). Questo demone é utilizzato per ottentere le informazioni degli utenti dell'ou PEOPLE

```
#
# nslcd.conf
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
    masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
    modify
# it under the terms of the GNU General Public License as
    published by
# the Free Software Foundation, either version 3 of the License,
    or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
    License
# along with networks-lab.  If not, see <http://www.gnu.org/
    licenses/>.
#


# This is the configuration file for the LDAP nameservice
# switch library's nslcd daemon. It configures the mapping
# between NSS names (see /etc/nsswitch.conf) and LDAP
# information in the directory.
# See the manual page nslcd.conf(5) for more information.

# The user and group nslcd should run as.
uid nslcd
gid nslcd

# The uri pointing to the LDAP server to use for name lookups.
# Multiple entries may be specified. The address that is used
# here should be resolvable without using LDAP (obviously).
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
```

```
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator
uri ldap://192.168.2.1/

# The LDAP version to use (defaults to 3
# if supported by client library)
#ldap_version 3

# The distinguished name of the search base.
base ou=PEOPLE,dc=gruppo2,dc=labreti,dc=it

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#binddn "cn=root,dc=gruppo2,dc=labreti,dc=it"

# The credentials to bind with.
# Optional: default is no credentials.
# Note that if you set a bindpw you should check the permissions
   of this file.
#bindpw gruppo2

# The distinguished name to perform password modifications by root
    by.
#rootpwmoddn cn=admin,dc=example,dc=com

# The default search scope.
#scope sub
#scope one
#scope base

# Customize certain database lookups.
#base   group  ou=Groups,dc=example,dc=com
#base   passwd ou=People,dc=example,dc=com
#base   shadow ou=People,dc=example,dc=com
#scope  group  onelevel
#scope  hosts  sub

# Bind/connect timelimit.
#bind_timelimit 30

# Search timelimit.
#timelimit 30

# Idle timelimit. nslcd will close connections if the
# server has not been contacted for the number of seconds.
#idle_timelimit 3600

# Use StartTLS without verifying the server certificate.
#ssl start_tls
```

```
#tls_reqcert never

# CA certificates for server certificate verification
#tls_cacertdir /etc/ssl/certs
#tls_cacertfile /etc/ssl/ca.cert

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Mappings for Services for UNIX 3.5
#filter passwd (objectClass=User)
#map    passwd uid              msSFU30Name
#map    passwd userPassword     msSFU30Password
#map    passwd homeDirectory    msSFU30HomeDirectory
#map    passwd homeDirectory    msSFUHomeDirectory
#filter shadow (objectClass=User)
#map    shadow uid              msSFU30Name
#map    shadow userPassword     msSFU30Password
#filter group  (objectClass=Group)
#map    group  member           msSFU30PosixMember

# Mappings for Services for UNIX 2.0
#filter passwd (objectClass=User)
#map    passwd uid              msSFUName
#map    passwd userPassword     msSFUPassword
#map    passwd homeDirectory    msSFUHomeDirectory
#map    passwd gecos            msSFUName
#filter shadow (objectClass=User)
#map    shadow uid              msSFUName
#map    shadow userPassword     msSFUPassword
#map    shadow shadowLastChange pwdLastSet
#filter group  (objectClass=Group)
#map    group  member           posixMember

# Mappings for Active Directory
#pagesize 1000
#referrals off
#idle_timelimit 800
#filter passwd (&(objectClass=user)(!(objectClass=computer))(
   uidNumber=*)(unixHomeDirectory=*))
```

```
#map    passwd uid              sAMAccountName
#map    passwd homeDirectory    unixHomeDirectory
#map    passwd gecos            displayName
#filter shadow (&(objectClass=user)(!(objectClass=computer))(
   uidNumber=*)(unixHomeDirectory=*))
#map    shadow uid              sAMAccountName
#map    shadow shadowLastChange pwdLastSet
#filter group  (objectClass=group)

# Alternative mappings for Active Directory
# (replace the SIDs in the objectSid mappings with the value for
   your domain)
#pagesize 1000
#referrals off
#idle_timelimit 800
#filter passwd (&(objectClass=user)(objectClass=person)(!(
   objectClass=computer)))
#map    passwd uid           cn
#map    passwd uidNumber     objectSid:S
   -1-5-21-3623811015-3361044348-30300820
#map    passwd gidNumber     objectSid:S
   -1-5-21-3623811015-3361044348-30300820
#map    passwd homeDirectory "/home/$cn"
#map    passwd gecos         displayName
#map    passwd loginShell    "/bin/bash"
#filter group (|(objectClass=group)(objectClass=person))
#map    group gidNumber      objectSid:S
   -1-5-21-3623811015-3361044348-30300820

# Mappings for AIX SecureWay
#filter passwd (objectClass=aixAccount)
#map    passwd uid              userName
#map    passwd userPassword     passwordChar
#map    passwd uidNumber        uid
#map    passwd gidNumber        gid
#filter group  (objectClass=aixAccessGroup)
#map    group  cn               groupName
#map    group  gidNumber        gid
```

14 nsswitch.conf

/etc/postfix/nsswitch.conf

File di configurazione di NSS (Name Service Switch) utilizzato dal sistema per definire dove si trovano i database di amministrazione. Da notare le direttive passwd, group, shadow che contengono la stringa ldap.

```
#
# nsswitch.conf
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
    masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
    modify
# it under the terms of the GNU General Public License as
    published by
# the Free Software Foundation, either version 3 of the License,
    or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
    License
# along with networks-lab.  If not, see <http://www.gnu.org/
    licenses/>.
#


# Begin /etc/nsswitch.conf

passwd: files ldap
group: files ldap
shadow: files ldap

publickey: files

hosts: files dns myhostname
networks: files

protocols: files
services: files
ethers: files
```

```
rpc: files

netgroup: files

# End /etc/nsswitch.conf
```

15 amavisd.conf

/etc/amavisd/amavisd.conf
File di configurazione di Amavis.

```
#
# amavisd.conf
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
   masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
   modify
# it under the terms of the GNU General Public License as
   published by
# the Free Software Foundation, either version 3 of the License,
   or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
   License
# along with networks-lab.  If not, see <http://www.gnu.org/
   licenses/>.
#


use strict;
# @bypass_virus_checks_maps = (1);
# @bypass_spam_checks_maps = (1);
$max_servers = 2;
$daemon_user  = 'amavis';
$daemon_group = 'amavis';
$mydomain = 'gruppo2.labreti.it';
$MYHOME = '/var/spool/amavis';
$TEMPBASE = "$MYHOME/tmp";
$ENV{TMPDIR} = $TEMPBASE;
$QUARANTINEDIR = "$MYHOME/virus";
$helpers_home = "$MYHOME/var";
$lock_file = "/run/amavis/lock";
$pid_file = "/run/amavis/pid";
$log_level = 0;
$log_recip_templ = undef;
```

```
$do_syslog = 1;
$syslog_facility = 'mail';

$enable_db = 1;
$nanny_details_level = 2;
$enable_dkim_verification = 1;
$enable_dkim_signing = 1;
@local_domains_maps = ( [".$mydomain"] );
@mynetworks = qw( 127.0.0.0/8 [::1] [FE80::]/10 [FEC0::]/10
                  10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 );
$unix_socketname = "/run/amavis/sock";

$inet_socket_port = 10024;
$policy_bank{'MYNETS'} = {
  originating => 1,
  os_fingerprint_method => undef,
};
$interface_policy{'10026'} = 'ORIGINATING';
$policy_bank{'ORIGINATING'} = {
  originating => 1,
  allow_disclaimers => 1,

  virus_admin_maps => ["virusalert\@$mydomain"],
  spam_admin_maps  => ["virusalert\@$mydomain"],
  warnbadhsender   => 1,

  forward_method => 'smtp:[127.0.0.1]:10027',

  smtpd_discard_ehlo_keywords => ['8BITMIME'],
  bypass_banned_checks_maps => [1],
  terminate_dsn_on_notify_success => 0,
};

$interface_policy{'SOCK'} = 'AM.PDP-SOCK';
$policy_bank{'AM.PDP-SOCK'} = {
  protocol => 'AM.PDP',
  auth_required_release => 0,
};

$sa_tag_level_deflt  = 1.0;
$sa_tag2_level_deflt = 1.0;
$sa_kill_level_deflt = 5.0;
$sa_dsn_cutoff_level = 8;
$sa_crediblefrom_dsn_cutoff_level = 10;
$penpals_bonus_score = 8;
$penpals_threshold_high = $sa_kill_level_deflt;
$bounce_killer_score = 100;
$sa_mail_body_size_limit = 400*1024;
$sa_local_tests_only = 0;
```

```
@addr_extension_virus_maps      = ('virus');
@addr_extension_banned_maps     = ('banned');
@addr_extension_spam_maps       = ('spam');
@addr_extension_bad_header_maps = ('badh');
$path = '/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/
   bin';
$MAXLEVELS = 14;
$MAXFILES = 3000;
$MIN_EXPANSION_QUOTA =      100*1024;
$MAX_EXPANSION_QUOTA = 500*1024*1024;
$sa_spam_subject_tag = '***Spam*** ';
$defang_virus  = 1;
$defang_banned = 1;
$defang_by_ccat{CC_BADH.",3"} = 1;
$defang_by_ccat{CC_BADH.",5"} = 1;
$defang_by_ccat{CC_BADH.",6"} = 1;
$myhostname = 'mail.gruppo2.labreti.it';
$notify_method  = 'smtp:[127.0.0.1]:10025';
$forward_method = 'smtp:[127.0.0.1]:10025';
@keep_decoded_original_maps = (new_RE(
  qr'^MAIL$',
  qr'^MAIL-UNDECIPHERABLE$',
  qr'^(ASCII(?! cpio)|text|uuencoded|xxencoded|binhex)'i,
));

$banned_filename_re = new_RE(
  qr'^\.(exe-ms|dll)$',
  [ qr'^\.(rpm|cpio|tar)$'       => 0 ],
  qr'.\.(pif|scr)$'i,
  qr'^application/x-msdownload$'i,
  qr'^application/x-msdos-program$'i,
  qr'^application/hta$'i,

  qr'^(?!cid:).*\.[^./]*[A-Za-z][^./]*\.\s*(exe|vbs|pif|scr|bat|
     cmd|com|cpl|dll)[.\s]*$'i,
  qr'.\.(exe|vbs|pif|scr|cpl)$'i,
);

@score_sender_maps = ({
  '.' => [
   new_RE(
    [qr'^(bulkmail|offers|cheapbenefits|earnmoney|foryou)@'i
                => 5.0],
    [qr'^(greatcasino|investments|lose_weight_today|market\.alert)
       @'i=> 5.0],
    [qr'^(money2you|MyGreenCard|new\.tld\.registry|opt-out|opt-in)
       @'i=> 5.0],
    [qr'^(optin|saveonlsmoking2002k|specialoffer|specialoffers)@'i
          => 5.0],
```

```
    [qr'^(stockalert|stopsnoring|wantsome|workathome|yesitsfree)@'
       i  => 5.0],
    [qr'^(your_friend|greatoffers)@'i
                                      => 5.0],
    [qr'^(inkjetplanet|marketopt|MakeMoney)\d*@'i
                          => 5.0],
  ),
  {
    'nobody@cert.org'                           => -3.0,
    'cert-advisory@us-cert.gov'                 => -3.0,
    'owner-alert@iss.net'                       => -3.0,
    'slashdot@slashdot.org'                     => -3.0,
    'securityfocus.com'                         => -3.0,
    'ntbugtraq@listserv.ntbugtraq.com'          => -3.0,
    'security-alerts@linuxsecurity.com'         => -3.0,
    'mailman-announce-admin@python.org'         => -3.0,
    'amavis-user-admin@lists.sourceforge.net'=> -3.0,
    'amavis-user-bounces@lists.sourceforge.net' => -3.0,
    'spamassassin.apache.org'                   => -3.0,
    'notification-return@lists.sophos.com'      => -3.0,
    'owner-postfix-users@postfix.org'           => -3.0,
    'owner-postfix-announce@postfix.org'        => -3.0,
    'owner-sendmail-announce@lists.sendmail.org'   => -3.0,
    'sendmail-announce-request@lists.sendmail.org' => -3.0,
    'donotreply@sendmail.org'                   => -3.0,
    'ca+envelope@sendmail.org'                  => -3.0,
    'noreply@freshmeat.net'                     => -3.0,
    'owner-technews@postel.acm.org'             => -3.0,
    'ietf-123-owner@loki.ietf.org'              => -3.0,
    'cvs-commits-list-admin@gnome.org'          => -3.0,
    'rt-users-admin@lists.fsck.com'             => -3.0,
    'clp-request@comp.nus.edu.sg'               => -3.0,
    'surveys-errors@lists.nua.ie'               => -3.0,
    'emailnews@genomeweb.com'                   => -5.0,
    'yahoo-dev-null@yahoo-inc.com'              => -3.0,
    'returns.groups.yahoo.com'                  => -3.0,
    'clusternews@linuxnetworx.com'              => -3.0,
    lc('lvs-users-admin@LinuxVirtualServer.org')    => -3.0,
    lc('owner-textbreakingnews@CNNIMAIL12.CNN.COM') => -5.0,

    'sender@example.net'                        =>  3.0,
    '.example.net'                              =>  1.0,
  },
 ],
});

@decoders = (
  ['mail', \&do_mime_decode],
  ['F',    \&do_uncompress, ['unfreeze', 'freeze -d', 'melt', '
```

```
    fcat'] ],
  ['Z',    \&do_uncompress, ['uncompress', 'gzip -d', 'zcat'] ],
  ['gz',   \&do_uncompress, 'gzip -d'],
  ['gz',   \&do_gunzip],
  ['bz2',  \&do_uncompress, 'bzip2 -d'],
  ['xz',   \&do_uncompress,
           ['xzdec', 'xz -dc', 'unxz -c', 'xzcat'] ],
  ['lzma', \&do_uncompress,
           ['lzmadec', 'xz -dc --format=lzma',
            'lzma -dc', 'unlzma -c', 'lzcat', 'lzmadec'] ],
  ['lrz',  \&do_uncompress,
           ['lrzip -q -k -d -o -', 'lrzcat -q -k'] ],
  ['lzo',  \&do_uncompress, 'lzop -d'],
  ['lz4',  \&do_uncompress, ['lz4c -d'] ],
  ['rpm',  \&do_uncompress, ['rpm2cpio.pl', 'rpm2cpio'] ],
  [['cpio','tar'], \&do_pax_cpio, ['pax', 'gcpio', 'cpio'] ],

  ['deb',  \&do_ar, 'ar'],
  ['rar',  \&do_unrar, ['unrar', 'rar'] ],
  ['arj',  \&do_unarj, ['unarj', 'arj'] ],
  ['arc',  \&do_arc,   ['nomarch', 'arc'] ],
  ['zoo',  \&do_zoo,   ['zoo', 'unzoo'] ],
  ['doc',  \&do_ole,   'ripole'],
  ['cab',  \&do_cabextract, 'cabextract'],
  ['tnef', \&do_tnef_ext, 'tnef'],
  ['tnef', \&do_tnef],
  [['zip','kmz'], \&do_7zip,  ['7za', '7z'] ],
  [['zip','kmz'], \&do_unzip],
  ['7z',   \&do_7zip,  ['7zr', '7za', '7z'] ],
  [[qw(gz bz2 Z tar)],
           \&do_7zip,  ['7za', '7z'] ],
  [[qw(xz lzma jar cpio arj rar swf lha iso cab deb rpm)],
           \&do_7zip,  '7z' ],
  ['exe',  \&do_executable, ['unrar','rar'], 'lha', ['unarj','arj
     '] ],
);

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

  ['KasperskyLab AVP - aveclient',
    ['/usr/local/kav/bin/aveclient','/usr/local/share/kav/bin/
       aveclient',
     '/opt/kav/5.5/kav4mailservers/bin/aveclient','aveclient'],
    '-p /var/run/aveserver -s {}/*',
    [0,3,6,8], qr/\b(INFECTED|SUSPICION|SUSPICIOUS)\b/m,
```

```
  qr/(?:INFECTED|WARNING|SUSPICION|SUSPICIOUS) (.+)/m,
],

['KasperskyLab AntiViral Toolkit Pro (AVP)', ['avp'],
  '-* -P -B -Y -O- {}', [0,3,6,8], [2,4],
  qr/infected: (.+)/m,
  sub {chdir('/opt/AVP') or die "Can't chdir to AVP: $!"},
  sub {chdir($TEMPBASE) or die "Can't chdir back to $TEMPBASE $
     !"},
],

['KasperskyLab AVPDaemonClient',
  [ '/opt/AVP/kavdaemon',       'kavdaemon',
    '/opt/AVP/AvpDaemonClient', 'AvpDaemonClient',
    '/opt/AVP/AvpTeamDream',    'AvpTeamDream',
    '/opt/AVP/avpdc', 'avpdc' ],
  "-f=$TEMPBASE {}", [0,8], [3,4,5,6], qr/infected: ([^\r\n]+)/m
      ],

['CentralCommand Vexira (new) vascan',
  ['vascan','/usr/lib/Vexira/vascan'],
  "-a s --timeout=60 --temp=$TEMPBASE -y $QUARANTINEDIR ".
  "--log=/var/log/vascan.log {}",
  [0,3], [1,2,5],
  qr/(?x)^\s* (?:virus|iworm|macro|mutant|sequence|trojan)\
     found:\ ( [^\]\s']+ )\ \.\.\.\ /m ],

['Avira AntiVir', ['antivir','vexira'],
  '--allfiles -noboot -nombr -rs -s -z {}', [0], qr/ALERT:|VIRUS
     :/m,
  qr/(?x)^\s* (?: ALERT: \s* (?: \[ | [^']* ' ) |
       (?i) VIRUS:\ .*?\ virus\ '?) ( [^\]\s']+ )/m ],

['Avira AntiVir', ['avscan'],
 '-s --batch --alert-action=none {}', [0,4], qr/(?:ALERT|FUND):/
    m,
 qr/(?:ALERT|FUND): (?:.* <<< )?(.+?)(?: ; |$)/m ],

['Command AntiVirus for Linux', 'csav',
  '-all -archive -packed {}', [50], [51,52,53],
  qr/Infection: (.+)/m ],

['Symantec CarrierScan via Symantec CommandLineScanner',
  'cscmdline', '-a scan -i 1 -v -s 127.0.0.1:7777 {}',
  qr/^Files Infected:\s+0$/m, qr/^Infected\b/m,
  qr/^(?:Info|Virus Name):\s+(.+)/m ],

['Symantec AntiVirus Scan Engine',
  'savsecls', '-server 127.0.0.1:7777 -mode scanrepair -details
```

```
    -verbose {}',
  [0], qr/^Infected\b/m,
  qr/^(?:Info|Virus Name):\s+(.+)/m ],

 ['F-Secure Linux Security',
  ['/opt/f-secure/fsav/bin/fsav', 'fsav'],
  '--virus-action1=report --archive=yes --auto=yes '.
  '--list=no --nomimeerr {}', [0], [3,4,6,8],
  qr/(?:infection|Infected|Suspected|Riskware): (.+)/m ],

['CAI InoculateIT', 'inocucmd',
  '-sec -nex {}', [0], [100],
  qr/was infected by virus (.+)/m ],

['CAI eTrust Antivirus', 'etrust-wrapper',
  '-arc -nex -spm h {}', [0], [101],
  qr/is infected by virus: (.+)/m ],

['MkS_Vir for Linux (beta)', ['mks32','mks'],
  '-s {}/*', [0], [1,2],
  qr/--[ \t]*(.+)/m ],

['MkS_Vir daemon', 'mksscan',
  '-s -q {}', [0], [1..7],
  qr/^... (\S+)/m ],

['ESET Software ESETS Command Line Interface',
  ['/usr/bin/esets_cli', 'esets_cli'],
  '--subdir {}', [0], [1,2,3],
  qr/:\s*action="(?!accepted)[^"]*"\n.*:\s*virus="([^"]*)"/m ],

['ESET NOD32 for Linux File servers',
  ['/opt/eset/nod32/sbin/nod32','nod32'],
  '--files -z --mail --sfx --rtp --adware --unsafe --pattern --
     heur '.
  '-w -a --action=1 -b {}',
  [0], [1,10], qr/^object=.*, virus="(.*?)",/m ],

['Norman Virus Control v5 / Linux', 'nvcc',
  '-c -l:0 -s -u -temp:$TEMPBASE {}', [0,10,11], [1,2,14],
  qr/(?i).* virus in .* -> \'(.+)\'/m ],

['Panda CommandLineSecure 9 for Linux',
  ['/opt/pavcl/usr/bin/pavcl','pavcl'],
  '-auto -aex -heu -cmp -nbr -nor -nos -eng -nob {}',
  qr/Number of files infected[ .]*: 0+(?!\d)/m,
  qr/Number of files infected[ .]*: 0*[1-9]/m,
  qr/Found virus :\s*(\S+)/m ],
```

```
  ['NAI McAfee AntiVirus (uvscan)', 'uvscan',
    '--secure -rv --mime --summary --noboot - {}', [0], [13],
    qr/(?x) Found (?:
        \ the\ (.+)\ (?:virus|trojan)  |
        \ (?:virus|trojan)\ or\ variant\ ([^ ]+)  |
        :\ (.+)\ NOT\ a\ virus)/m,
  ],

  ['VirusBuster', ['vbuster', 'vbengcl'],
    "{} -ss -i '*' -log=$MYHOME/vbuster.log", [0], [1],
    qr/: '(.*)' - Virus/m ],

  ['CyberSoft VFind', 'vfind',
    '--vexit {}/*', [0], [23], qr/

  ],

  ['avast! Antivirus', ['/usr/bin/avastcmd','avastcmd'],
    '-a -i -n -t=A {}', [0], [1], qr/\binfected by:\s+([^ \t\n
       \[\]]+)/m ],

  ['Ikarus AntiVirus for Linux', 'ikarus',
    '{}', [0], [40], qr/Signature (.+) found/m ],

  ['BitDefender', 'bdscan',
    '--action=ignore --no-list {}', qr/^Infected files\s*:\s
       *0+(?!\d)/m,
    qr/^(?:Infected files|Identified viruses|Suspect files)\s*:\s
       *0*[1-9]/m,
    qr/(?:suspected|infected)\s*:\s*(.*)(?:\033|$)/m ],

  ['BitDefender', 'bdc',
    '--arc --mail {}', qr/^Infected files *:0+(?!\d)/m,
    qr/^(?:Infected files|Identified viruses|Suspect files)
       *:0*[1-9]/m,
    qr/(?:suspected|infected): (.*)(?:\033|$)/m ],

  ['ArcaVir for Linux', ['arcacmd','arcacmd.static'],
    '-v 1 -summary 0 -s {}', [0], [1,2],
    qr/(?:VIR|WIR):[ \t]*(.+)/m ],
);

@av_scanners_backup = (

  ['ClamAV-clamscan', 'clamscan',
    "--stdout --no-summary -r --tempdir=$TEMPBASE {}",
    [0], qr/:.*\sFOUND$/m, qr/^.*?: (?!Infected Archive)(.*)
       FOUND$/m ],
```

```
  ['F-PROT Antivirus for UNIX', ['fpscan'],
    '--report --mount --adware {}',
    [0,8,64],  [1,2,3, 4+1,4+2,4+3, 8+1,8+2,8+3, 12+1,12+2,12+3],
    qr/^\[Found\s+[^\]]*\]\s+<([^ \t(>]*)/m ],

  ['FRISK F-Prot Antivirus', ['f-prot','f-prot.sh'],
    '-dumb -archive -packed {}', [0,8], [3,6],
    qr/(?:Infection:|security risk named) (.+)|\s+contains\s+(.+)$
       /m ],

  ['Trend Micro FileScanner', ['/etc/iscan/vscan','vscan'],
    '-za -a {}', [0], qr/Found virus/m, qr/Found virus (.+) in/m
       ],

  ['drweb - DrWeb Antivirus',
    ['/usr/local/drweb/drweb', '/opt/drweb/drweb', 'drweb'],
    '-path={} -al -go -ot -cn -upn -ok-',
    [0,32], [1,9,33], qr' infected (?:with|by)(?: virus)? (.*)$'m
       ],

   ['Kaspersky Antivirus v5.5',
     ['/opt/kaspersky/kav4fs/bin/kav4fs-kavscanner',
      '/opt/kav/5.5/kav4unix/bin/kavscanner',
      '/opt/kav/5.5/kav4mailservers/bin/kavscanner', 'kavscanner
         '],
     '-i0 -xn -xp -mn -R -ePASBME {}/*', [0,10,15], [5,20,21,25],
     qr/(?:INFECTED|WARNING|SUSPICION|SUSPICIOUS) (.*)/m,
   ],

  ['Sophos Anti Virus (savscan)',
    ['/opt/sophos-av/bin/savscan', 'savscan'],
    '-nb -f -all -rec -ss -sc -archive -cab -mime -oe -tnef '.
    '--no-reset-atime {}',
    [0,2], qr/Virus .*? found/m,
    qr/^>>> Virus(?: fragment)? '?(.*?)'? found/m,
  ],
);
1;
```

16 clamd.conf

/etc/clamav/clamd.conf
File di configurazione principale dell'antivirus ClamAV.

```
#
# clamd.conf
#
# Copyright (C) 2016 frnmst (Franco Masotti) <franco.
   masotti@student.unife.it>
#                    dannylessio (Danny Lessio)
#
# This file is part of networks-lab.
#
# networks-lab is free software: you can redistribute it and/or
   modify
# it under the terms of the GNU General Public License as
   published by
# the Free Software Foundation, either version 3 of the License,
   or
# (at your option) any later version.
#
# networks-lab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public
   License
# along with networks-lab.  If not, see <http://www.gnu.org/
   licenses/>.
#


LogFile /var/log/clamav/clamd.log
LogTime yes
PidFile /run/clamav/clamd.pid
TemporaryDirectory /tmp
LocalSocket /var/lib/clamav/clamd.sock
User clamav
# Added:
AllowSupplementaryGroups true
#ScanMail yes
```