netkit lab

PEC

<table>
<thead>
<tr>
<th>Version</th>
<th>0.1.4.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>G. Pantanetti</td>
</tr>
<tr>
<td>E-mail</td>
<td><a href="mailto:gpantanetti@yahoo.it">gpantanetti@yahoo.it</a></td>
</tr>
<tr>
<td>Web</td>
<td><a href="http://www.netkit.org/">http://www.netkit.org/</a></td>
</tr>
<tr>
<td>Description</td>
<td>an OpenPEC laboratory to test open source solution for Certified Email</td>
</tr>
</tbody>
</table>
copyright notice

- All the pages/slides in this presentation, including but not limited to, images, photos, animations, videos, sounds, music, and text (hereby referred to as “material”) are protected by copyright.
- This material, with the exception of some multimedia elements licensed by other organizations, is property of the authors and/or organizations appearing in the first slide.
- This material, or its parts, can be reproduced and used for didactical purposes within universities and schools, provided that this happens for non-profit purposes.
- Information contained in this material cannot be used within network design projects or other products of any kind.
- Any other use is prohibited, unless explicitly authorized by the authors on the basis of an explicit agreement.
- The authors assume no responsibility about this material and provide this material “as is”, with no implicit or explicit warranty about the correctness and completeness of its contents, which may be subject to changes.
- This copyright notice must always be redistributed together with the material, or its portions.
overview

- This lab is built over email-lab from official netkit laboratories
- This time users can exchange certified emails using OpenPEC email system
PEC (1)

- An electronic version of common *registered letter*
  - With sender traceability
  - With guaranteed content’s inalterability
  - With acknowledgement of receipt
- With legal value
  - Stated since “Decreto Ministeriale” 2005
  - For Public Administrations
  - For private citizens and companies
PEC (2)

- Released by certified providers
  - The list of certified providers is maintained by CNIPA
    - National Center for Informatics in Public Administrations
  - Each provider must pass a compatibility test
- Certified receipts of message’s delivery route
PEC (3)

- Mail are signed with PEC providers’ certificates
- Communications between MUAs and MXs are encrypted
  - TLS, IPSEC (for LDAP access)
- Each mail is checked for viruses
- Sender and recipient need to authenticate themselves
PEC receipts (1)

- A certificate-signed PEC receipt is sent to sender
  - When sender’s mail server accepts to deliver the mail
  - When mail is received on recipient's mailbox
  - Every time an error occurs
PEC receipts (2)

- Each receipt contains informations on:
  - Date and time
  - Email subject
  - Whether mail contains attachments
  - Email message’s content
    - Only on mail delivered receipt
PEC flow (send)
PEC flow (receive)
PEC’s strengths

- Certified receipt of message delivery on recipient’s mailbox
- Archived log of all events and receipts for 30 months
- Traceability of sender mailbox and its owner
- Recognized legal value
- Strict requirements with required interoperability test
PEC’s notes

- Doesn’t provide download/read proof
- Not applicable on legal field
- Uses “From:” field in a no-standard way
  - From: "Per conto di: mario.bianchi@dominio.it"
    <posta-certificata@gestore.it>
OpenPEC

- OpenPEC is an Open Source project born to realize a PEC system
- OpenPEC is an extension for popular Open Source mail servers
- OpenPEC is developed in Perl with a modular structure
architecture overview

- Two mail-users exchange emails between two different domains
- Two mail-servers with PEC system
- A basic DNS hierarchy tree served by five name-servers
base configuration

- The configurations of the PCs are the same as the mail lab
- The MXs are configured as in mail lab
- The NSs are configured as in dns lab
PEC servers

- PEC services are installed on mail servers
- Each PEC server requires
  - Required PERL modules
  - OpenPEC scripts
  - LDAP server
  - Antivirus deamon
  - A mail server
  - An LMTP server
OpenPEC installation

- Each OpenPEC server has different releases of OpenPEC software
- In PEC servers' startup script you can choose which version to install
- Make utilities packages are installed
- OpenPEC package is unzipped, compiled and installed
OpenPEC installation (2)

- user.group is opec.opec
- workspace is in /home/opec/opec/
- configuration file is /etc/opec.conf
- scripts are in /usr/sbin/
- Perl libraries are in /usr/local/share/perl/
installation of other services and libraries

- LDAP, Antivirus, LMTP services and libraries are installed using debian (unstable) packages during first server startup

- Debian packages are in /install directory
  - OpenLDAP, Clamav, Maidag (from GNU Mailutils), and others...
LDAP

- LDAP server use PEC schema
  - `/etc/ldap/schema/ind_pec.schema`
- The database is populated with PEC providers
  - Each provider is saved with its certificate, specification of managed domains, mail address of PEC referee, ecc.
  - Check objectclass ‘provider’ on LDAP schema
- LDAP server listens to standard 389 TCP port
certificates

- PEC needs two type of certificates
  - one or more certificates for TLS connections (IMAPS, POPS, SMTPS e HTTPS)
  - an x509 certificate (S/MIME) for every PEC domain
- We created self-signed certificates for lab purpose
  - The CA certificate is installed as system certificate on PEC servers
antivirus

- PEC requires an antivirus daemon to scan sent and received mails
- Clamav antivirus is installed as a TCP service on port 3310
LMTP

- An LMTP server is used to deliver local mails to users
- Maidag is configured to listen to local TCP port 24
  - `listen tcp://127.0.0.1:24;`
OpenPEC architecture
Lab startup

- Lab startup is nearly straightforward
- PEC servers need to install a lot of packages
  - You have to choose a password for LDAP admin
lab startup (2)

- PEC servers will compile and install OpenPEC services
- All virtual machine will be prepared by startup scripts
  - All scripts (except those for PEC servers) belong to email lab
PEC servers startup

- As stated before, these servers need to install plenty of packages
  - For LDAP, Clamav, PERL libraries, make tool, LMTP server
- Some directories need to be created and permissions granted
- In startup script are all commands necessary to configure, compile and install PEC services
test PEC server

- To quickly test PEC environment login on pc1 virtual machine
- Become *guest* user, go to test directory and launch test script

```
root@pc1:~# su guest
guest@pc1:/root$ cd
guest@pc1:/root$ cd test
guest@pc1:/~$ ./test.sh
```
test PEC server (2)

- Test script will contact mailserver and send a mail
- You can check your mail has been sent using pine
- You should receive two mails for any test you executed
  - One mail is your accepted for delivery receipt
  - The other one is the delivery notification receipt
test screenshot
sender mailbox in pine
Test PEC server (3)

- On pc2 you can check your mailbox for certified email
- Become guest and use pine to read your mail
recipient mailbox in pine
to be done

- Install POP3 and IMAP on TLS
- Test OpenPEC different releases
- Correct buffer overflow error of OpenPEC latest release due to Perl Crypt::SMimeEngine library
- Uniform LDAP PEC schema with latest schema from CNIPA