Mittuniversitetet
MID SWEDEN UNIVERSITY

DT149G Administration of UNIX-like systems

Laboratory Assignment: Email anatomy

Lennart Franked*

lab_assgn5.tex 2071 2014-11-05 10:14:51Z lenfra

Contents

1 Introduction

In this laboratory assignment you will install and configure an email server and related mechanisms.

2 Aim

After completion of this assignment you will:

- Have the knowledge to set up an SMTP server process.
- Be able to set up the necessary security measures so that an email sent from your SMTP server will not be regarded as spam and cannot easily be used by spammers.
- Know how to correctly set up your DNS to handle email and related mechanisms.

*E-post: `lennart.franked@miun.se`.

- Be able to install and configure software for delivering emails using either POP3 or IMAP.

3 Reading instructions

Before starting this assignment you should have read chapter 20 and chapter 17 – "SPF records" and "DKIM and ADSP records", respectively, in Nemeth et al. [9]. During this laboratory assignment you should also consult the following sites and documents: [6], [4], [3], [1], [2], [5], [7], [8].

4 Tasks

Perform the following tasks and document all the steps taken to complete them.

4.1 MTA/MDA

As you have read in the course literature, there are numerous types of components involved in an email system. We are going to start by setting up the mail transfer agent (MTA). Which MTA you choose to use is up to you, the book covers Sendmail, Exim and Postfix. The instructions will be based on Postfix.

Since Postfix more or less works out of the box, there are only a few configurations that must be made in order to make your SMTP server work.

1. Install and configure a basic Postfix server, you can easily follow the instructions given in [4]. Make sure to explain each step taken and the purpose of it in your report See [6] for detailed information about the configuration steps.

2. Test your email server using `telnet(1)` to connect and send an email from your user to Mickey at localhost.

3. Check your Postfix access restrictions and ensure that it will only relay emails that originate from your local network. In your report, make sure to motivate why this is important and when it is not suitable to have this restriction.

4. If you were to send an email from your email server to a Gmail-account[1], your email would be marked as spam and maybe even discarded before reaching the recipient. To ensure that this will not be the case we must setup DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF). See [5; 7] for the necessary steps to achieve this.

5. (Optional) Add SSL authentication to your Postfix installation, see [3] for detailed information about how to achieve this.

[1] Since you are installing your email server locally and your ISP probably will not allow SMTP-traffic, you will not be able to actually send any emails from this email server to an outside domain.

4.2 DNS

Now that you have a working email server up and running, you must add an MX record to your domain zone-file so that messages sent to *youruser@yourdomain* will find its way to the comfort of your local mailbox.

1. Add the appropriate MX record to your DNS-server.
2. Since you have configured your Postfix-server to check the SPF records before accepting an incoming email, you should also add your own SPF-records in your zone configuration-file. Since not all email servers support the SPF resource record, you should add your SPF entries using both SPF RR and TXT RR.

4.3 Access Agents

Your server is now able to send and receive email, however, in order for you to be able to access your emails from another PC you need to set up an Access Agent that runs POP3 or IMAP. The instructions will be based upon Dovecot, but as always, your are free to choose any software. See [1; 2] for instructions on how to install and configure Dovecot on your system.

1. Install and configure basic Dovecot with both POP3 and IMAP support.
2. Once installed, test and make sure that your AA-server is working properly, use for example `telnet(1)` or set up a user agent, e.g `mail(1)` or `Thunderbird(1)`
3. Since your user name and password will be sent in plain text you must now configure Dovecot to use SSL based authentication instead of plain-text authentication. Dovecot use the Simple Authentication and Security Layer (SASL) to enable SSL-based authentication, see [8] for how this protocol layer works[2]. See [1; 2] for instructions on setting up SSL-based authentication in Dovecot.
4. Make sure that your Dovecot-server is now using SSL to encrypt your password, for example by analyzing the traffic using Wireshark.

5 Examination

Hand in a report containing all your solutions to the questions in section 4

References

[1] Dovecot, 2012. URL `https://help.ubuntu.com/community/Dovecot`.

[2] Dovecot official documentation, 2012. URL `http://wiki2.dovecot.org/`.

[2] You do not have to read the entire document, just get yourself an understanding of the protocol.

[3] Postfix, 2012. URL https://help.ubuntu.com/community/Postfix.

[4] Postfix basic setup howto, 2012. URL https://help.ubuntu.com/community/PostfixBasicSetupHowto.

[5] Postfix/dkim, 2012. URL https://help.ubuntu.com/community/Postfix/DKIM.

[6] Postfix official documentation, 2012. URL http://www.postfix.org/documentation.html.

[7] Postfix/spf, 2012. URL https://help.ubuntu.com/community/Postfix/SPF.

[8] A. Melnikov and K. Zeilenga. Simple Authentication and Security Layer (SASL). RFC 4422 (Proposed Standard), June 2006. URL http://www.ietf.org/rfc/rfc4422.txt.

[9] Evi Nemeth, Garth Snyder, Trent R. Hein, and Ben Whaley. *UNIX and Linux system administration handbook*. Prentice Hall, Upper Saddle River, NJ, 4th ed. edition, 2011. ISBN 978-0-13-148005-6 (pbk. : alk. paper).