DT149G — Administration of UNIX-like systems
Nuntio servitium

Lennart Franked*

October 25, 2024

Contents

1 Introduction

In this laboratory assignment you will install and configure an email server and related mechanisms. Before starting this assignment, you must have finished lab assignment 4 — DNS

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 Nemeth et al., 2017, chapter 18 During this laboratory assignment you should also consult the following sites and documents: Postfix, 2024b, Postfix, 2024a, Dovecot, 2024a, Dovecot, 2024b, Ubuntu, 2014, Ubuntu, 2013, Melnikov and Zeilenga, 2006.

4 Tasks

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

4.1 IPTables

Before setting up an email server, you must update your firewall so that the ports for the services you will configure are open.

Hence update your firewall policy with the following:

- Allow all incoming packets using transport protocol TCP and port 25 (SMTP).
- (If applicable) Allow all incoming packets using transport protocol TCP 465 (Secure SMTP).
- Allow all incoming packets using transport protocol TCP and port 110 (POP).
- (If applicable) Allow all incoming packets using transport protocol TCP and port 995 (Secure POP3).
- Allow all incoming packets using transport protocol TCP and port 143.
- (If applicable) Allow all incoming packets using transport protocol TCP and port 993 (secure IMAP).

To answer in you report For this task, present the following in your report:

- Include a screenshot showing your new IPTable rules.

4.2 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 Postfix, 2024a. See Postfix, 2024b 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.

4. Add TLS authentication to your Postfix installation, see Postfix, 2024a for detailed information about how to achieve this.

To answer in your report For this task, answer the following questions in your report:

- Explain each step taken to install the MTA-server and the purpose of it
- Include a screenshot showing that you can telnet to your MTA-server.
- What did you have to do, to ensure that your MTA will only relay emails from your local network?
- Discuss why it is important to restrict relaying emails, when it is not suitable to have this restriction.

4.3 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 the DNS-server that is responsible for mcduckcorp.duckburg.cali.

2. 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 Ubuntu, 2013, 2014 for the necessary steps to achieve this.

3. You will in a later lab run this email-server in a container. Therefore make sure that Postfix and DKIM communicates through a local UNIX-socket.

4. 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.

5. Restart Bind to ensure that it includes the new MX, DKIM and SPF-records

[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.

6. Using Telnet, send an email from your current account to any of the other accounts you created in previous labs. Then confirm that the email have gotten an DKIM-signature.

To answer in your report For this task, answer the following questions in your report:

- Include a screenshot showing your MX, DKIM and SPF-records.
- Include a screenshot showing the full header of the email that you sent, to show that DKIM works properly.

4.4 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 Dovecot, 2024a, 2024b for instructions on how to install and configure Dovecot on your system. *An alternative to installing Dovecot manually, is to download a docker container for Dovecot.*

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)`, `mutt(1)` or `Thunderbird (1)`
3. Make sure that your user name and password is not sent in plain text, by ensuring Dovecot is using TLS based authentication instead of plain-text authentication.
4. Make sure that your Dovecot-server is now using TLS to encrypt your password, for example by analyzing the traffic using Wireshark, or connect to it using *openssl s_client*

To answer in your report For this task, answer the following questions in your report:

- Include a screenshot showing that your AA is working properly.
- Include a screenshot showing that TLS is working as it should.

5 Examination

Hand in a report containing all your solutions to the questions in Section 4 *Remember that you must include references to the given reading instructions, alternatively to the laboratory work you have done*

References

Dovecot. (2024a). *Dovecot*. Retrieved October 25, 2024, from https://documentation.ubuntu.com/server/how-to/mail-services/install-dovecot/

Dovecot. (2024b). *Dovecot official documentation*. Retrieved October 25, 2024, from https://doc.dovecot.org/2.3/

Melnikov, A., & Zeilenga, K. (2006). *Simple Authentication and Security Layer (SASL)* (rfc No. 4422). IETF. http://tools.ietf.org/rfc/rfc4422.txt

Nemeth, E., Snyder, G., Hein, T. R., Whaley, B., & Mackin, D. (2017). *Unix and linux system administration handbook* (Fifth edition.). Addison-Wesley/Pearson.

Postfix. (2024a). *Postfix*. Retrieved October 25, 2025, from https://documentation.ubuntu.com/server/how-to/mail-services/install-postfix/

Postfix. (2024b). *Postfix official documentation*. Retrieved October 25, 2024, from http://www.postfix.org/documentation.html

Ubuntu. (2013). *Postfix/spf*. Retrieved October 25, 2024, from https://help.ubuntu.com/community/Postfix/SPF

Ubuntu. (2014). *Postfix/dkim*. Retrieved October 25, 2024, from https://help.ubuntu.com/community/Postfix/DKIM