Project 4 - Sending Email for the Hesk Web App

Goal:

The goal of this project is to configure a Linux system to forward emails to an SMTP (Simple Mail Transfer Protocol) relay server. An SMTP relay server accepts outbound email from a system and then sends, or relays, the email to the final destination.

Background:

In the real world you will most likely never configure your Linux systems to send email directly to recipients. Unless you were specifically hired into an email administration role, you will probably never have to worry about the details of email configuration and delivery. Your role will be to ensure email originating from your systems gets forwarded to a designated SMTP relay server.

Just like Linux system administration is a specialized skill, so is email administration. Email administration is beyond the scope of this course and could warrant an entire course on its own.

It's becoming increasingly common for IT departments to completely outsource email. Some popular options include Google's Gmail service and Microsoft's Exchange Online. Even if the entire email solution is not outsourced, it's still common to outsource transactional email services to a third party provider such as SendGrid or Amazon Web Service's Simple Email Service. (A transactional email is an email that is triggered by a user action such as a user creating an account or submitting a help desk ticket.)

SMTP Relay Options

If you work for a large organization it probably already has an email infrastructure. In that case you would configure your Linux servers to forward mail to your company's existing SMTP relay host. If your organization has outsourced email, then you will forward email to that outsourced service's SMTP relay host.

If you work for a small organization that doesn't have an existing email infrastructure or you are working on personal projects, your best option is to use a transactional email provider such as SendGrid.

For testing purposes or for extremely low email volumes, you can *sometimes* use the SMTP server of your own email provider. If the email provider has instructions for setting up an email client, then you could potentially use that information to configure your Linux server to send email through your provider.

Disclaimers:

We have several things going against our favor in terms of email deliverability. Because of this I am not able to provide support for ultimate email deliverability. I will guide you through configuring your Linux system to send to an SMTP relay, but what the SMTP relay does with the email is beyond my control.

Here are just some issues:

1. Many of us are working on this course from home and most ISPs block access to common SMTP ports in an effort to fight spam.
2. Some of us might be working on this course at work or school. Those networks may also be configured to block outgoing email that doesn't originate from their IT infrastructure.
3. We are working on a local lab environment. In the real world, your system will be part of a company network or accessible from the public internet.
4. We are not using real domain names that we control. Again, in the real world your system will be part of a larger company infrastructure or be part of a domain you control.
5. Even if we use a transactional email service, they may only allow you to send emails with a from address that you can prove that you own. For example, they will send a verification link to an email address that you plan to send from. If you don't click the link, they will not allow email to be sent from that email address. Also, they may only allow you to send emails from domains that you can verify. For example, they may ask you to add a DNS record for your domain to prove you have control of that domain. Finally, they will typically not deliver email unless it is a valid routable email address. They typically will not deliver emails from "root@localhost.localdomain" or similar.
6. If we use the SMTP server from our email provider, they may silently refuse to deliver emails for a variety of reasons including their default security settings that disallow SMTP relaying, the number of emails sent, the timeframe in which they were sent, and the from address not matching the address on the account.
7. Even if email gets delivered, it could be sent to a spam folder and never seen by the recipient.

Instructions:

Start the Hesk Virtual Machine

For this project you are going to use the hesk virtual machine that you created in a previous project. First, start a command line session. Change into your `linuxclass` folder and then change into the `hesk` directory.

```
cd linuxclass
cd hesk
```

Next, start the virtual machine using the `vagrant up` command. If the virtual machine is already running, vagrant will let you know that it's ready to use. If it's stopped or paused, vagrant will start the virtual machine.

Start the virtual machine and connect to it.

```
vagrant up
vagrant ssh
```

Choose an SMTP Relay Service

Since this server isn't directly connected to the Internet or to a company network with an email infrastructure, you'll need to use a third-party mail delivery system.

One such system is SendGrid (http://www.sendgrid.com). As of this writing, it's free to use. Once you create an account, you'll have to verify your email address. Consult SendGrid's documentation for details on how to verify your email address. (NOTE: you will only be able to send emails from addresses that you have verified.)

Another option is ReachMail's Easy-SMTP transactional email service located at https://reachmail.com/solutions/transactional/. They also have a free plan that will allow you to send up to several thousand emails a month. You will need to verify a domain, so this is only a viable option if you own your own domain.

Yet another option is to use the SMTP server from your email provider. I do NOT recommend using Gmail because they have made it extremely difficult to use their SMTP server as a relay server. I would use a less popular email service such as GMX. You can create a free email account at https://www.gmx.com. Typically, you have to enable a setting to send emails through the service. In the settings of your email provider, enable access to your account via anything that is labeled POP3, IMAP, or SMTP.

Regardless of which SMTP relay method you choose, make a note of the SMTP connection details provided by the service. You will need this information soon.

Configure From Email Addresses for the Linux Server

By default, when an email is generated by a web application, it is given a from address of the Linux user running the web server. The domain portion of the from email address is set to the Linux host name and domain. Because Apache (the httpd process) runs as the "apache" user, emails will be given a from address of "apache@hesk.localdomain". This can be overridden by the web application, but many times it is not.

That email address is a non-routable email address. A non-routable email address is simply an email address without a valid domain name. For example, root@hesk.localdomain is a non-routable email address because "hesk.localdomain" is not a real domain name. Other non-routable email address examples include "vagrant@hesk.localdomain", "apache@localhost", and "admin@local".

As you already know, most SMTP relays will reject invalid or non-routable email addresses, be they TO email addresses or FROM email addresses. This means we have to configure our Linux system to send emails from a real, routable email address.

Postfix is the MTA (mail transfer agent) that you will use to forward emails to the SMTP Relay host. You are going to edit the Postfix configuration. First, make a backup of the Postfix configuration file located at `/etc/postfix/main.cf.`

```
sudo cp /etc/postfix/main.cf /etc/postfix/main.cf.orig
```

Now you're ready to add some configuration to the end of the file.

```
sudo nano /etc/postfix/main.cf
```

Add the following line to the bottom of the `/etc/postfix/main.cf` file.

```
sender_canonical_maps = hash:/etc/postfix/sender_canonical
```

Save your changes. If you are using nano, type "Ctrl-X" followed by "Y", and finally hit <ENTER> to save your changes.

Create the `/etc/postfix/sender_canonical` file by editing it.

```
sudo nano /etc/postfix/sender_canonical
```

Add this line to the file. Be sure to **use your real email address.**

```
@hesk.localdomain YOU@YOUR_DOMAIN
```

For example, if your email address is jason@gmx.com, the line would look like this:

```
@hesk.localdomain jason@gmx.com
```

This configuration tells Postfix to use your email address as the from address for any emails with a from address that ends in "@hesk.localdomain". This means that your server will send emails from your email address instead of "apache@hesk.localdomain".

Now we have to convert the file into a format that Postfix can use by using the `postmap` command:

```
sudo postmap hash:/etc/postfix/sender_canonical
```

This command will create a `/etc/postfix/sender_canonical.db` file. Confirm that it exists.

```
ls -l /etc/postfix/sender_canonical.db
```

Restart the postfix service to make sure the configure is accepted. If you get an error message, fix your mistakes and restart the service again.

```
sudo systemctl restart postfix
```

Configure the System to Forward Emails to an SMTP Relay Host

Now that you have configured the from email address, it's time to configure Postfix to send emails to the SMTP relay host. Edit the Postfix configuration file.

```
sudo nano /etc/postfix/main.cf
```

Add the following to the bottom of the `/etc/postfix/main.cf` file. Be sure to use the SMTP host name and port of the provider you're using. Save the file when you're done.

```
relayhost = [YOUR_PROVIDERS_SMTP_HOST_NAME]:YOUR_PROVIDERS_SMTP_PORT
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
header_size_limit = 4096000
```

Here is an example using SendGrid:

```
relayhost = [smtp.sendgrid.net]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
header_size_limit = 4096000
```

Here is an example using GMX:

```
relayhost = [mail.gmx.com]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
header_size_limit = 4096000
```

Save your changes.

Next, create the `/etc/postfix/sasl_passwd` file by editing it.

```
sudo nano /etc/postfix/sasl_passwd
```

Create one line in the file that follows this format:

```
SMTP_RELAY_HOST YOUR_USERNAME:YOUR_PASSWORD
```

Be sure to use the SMTP host name of the provider *you* are using, *your* username, and *your* password. Save the file when you're done.

Here is an example using SendGrid:

```
smtp.sendgrid.net jason:jasonsPassword
```

Here is an example using GMX:

```
mail.gmx.com jason@gmx.com:jasonsPassword
```

Now we have to convert the file into a format that Postfix can use by using the `postmap` command:

```
sudo postmap hash:/etc/postfix/sasl_passwd
```

This command will create a `/etc/postfix/sasl_passwd.db` file. Confirm that it exists.

```
ls -l /etc/postfix/sasl_passwd.db
```

NOTE: If you need to edit the `/etc/postfix/sasl_passwd` file in the future, you will also need to run the `postmap` command again.

Finally, restart the postfix service so it can load this new configuration.

```
sudo systemctl restart postfix
```

Configure From Email Addresses in the Web Application

Web applications can specify a from address different from the default, but not all do. Sometimes it is configurable and sometimes it is hard coded. Fortunately, HESK provides a way to configure email addresses.

To change the email addresses used by HESK, edit the `/var/www/html/hesk_settings.inc.php` file.

```
sudo nano /var/www/html/hesk_settings.inc.php
```

Change the "webmaster_email" address and "noreply_email" from support@example.com to **your email address.** If you are using a transactional email service such as SendGrid, make sure to use the email address that you verified with the service.

Here are the two lines that need to change:

```
$hesk_settings['webmaster_mail']='support@example.com';
$hesk_settings['noreply_mail']='support@example.com';
```

For example, if your email address is jason@gmx.com, you would change those two lines to this:

```
$hesk_settings['webmaster_mail']='jason@gmx.com';
$hesk_settings['noreply_mail']='jason@gmx.com';
```

Save your changes.

You can verify your setting changes by visiting http://10.23.45.20/admin/admin_settings_general.php in your web browser.

Update the Email Address in Your Profile

Make sure to use your email address in the HESK admin user profile. You can update your email address by editing the profile here: http://10.23.45.20/admin/profile.php

Send an Email

Visit the HESK web application located at http://10.23.45.20/ in your browser. Click "Submit a ticket". Fill out the form. Be sure to **use your real email address**. Click "Submit Ticket".

Check the email log file from the command line:

```
sudo cat /var/log/maillog
```

Look for a line that has "relay=" in it. If you see one, then **consider this project a success!**

The best case scenario is that the status is "sent". However, as noted in the disclaimer above, the status may very will be rejected, deferred, or something else. Again, the goal of this project is to configure your Linux server to send its messages to an SMTP relay server. What that SMTP relay server does with that message is beyond the scope of this lesson and course.

Troubleshooting Tips:

When troubleshooting email, the easiest thing to do is check the spam folder for the message. If you find the message in spam folder, you may want to whitelist the sending email address so that messages from it never get routed to the spam folder.

On the server side, the best place to start is with the mail log:

```
sudo cat /var/log/maillog
```

Make sure the from email address is a valid and routable email address.

```
grep from= /var/log/maillog
```

Make sure the to email address is a valid and routable email address.

```
grep to= /var/log/maillog
```

Completely read any messages. Many times the SMTP relay host will provide an error code in addition to a brief text message explaining the error.

```
grep said /var/log/maillog
```

Here is an example message you may see: "host smtp.sendgrid.net[1.1.1.1] said: 403-You are not authorized to send from that email address"

Perhaps the credentials you supplied for the SMTP relay host are invalid. In that case, you will get an authentication error.

```
grep -i auth /var/log/maillog
```

Here is an example message you may see: "host smtp.sendgrid.net[1.1.1.1] said: 535 Authentication credentials invalid"

Edit the `/etc/postfix/sasl_passwd` file and set the proper username and password. Then, recreate the postfix lookup table:

```
sudo nano /etc/postfix/sasl_passwd
sudo postmap hash:/etc/postfix/sasl_passwd
sudo systemctl restart postfix
```

If you haven't determined the issue at this point, look at the information and/or logs provided by your SMTP relay host. For example, if you are using SendGrid look at the "activity feed" and all the reports under "suppressions".

Some SMTP relay host providers have a troubleshooting document. Find the troubleshooting document for your provider and follow the instructions.

Finally, if email is still not being delivered, contact your SMTP relay host provider.