SMTP Relay Authentication - Postfix
Author - Nic Maurel

Intro
The reason for this paper is that more and more people are employing a security feature on their mail servers called *smtp authentication*. Now I can totally understand why. SPAM. While I know smtp is clear text, and the password can be sniffed. But the principle goes, if Server A has authentication and Server B doesn't, script kiddies will go for Server B. It just raises the bar a little. Now it is quite simple and is only a few steps, and I am going to show you how to do it on a Linux Postfix server.

Howto
Bear in mind we are not setting up authentication for our mail server, we are only telling our mail server that the remote server for a specific domain requires authentication. So how do we do this for specific domains? Simple we create a file with the root user as follows:

```
Vi /etc/postfix/sasl_passwd

---------------------------------------
#Domain Username:Password
mail.example.com mail01:rght#1
---------------------------------------
```

save and exit. Fairly self explanatory, any mail going to mail.example.com will need the specified username and password.

```
chmod -Rf 600 /etc/postfix/sasl_passwd
chown -Rf root:root /etc/postfix/sasl_passwd
```

Ahh! But now you ask how will postfix read the file if it is only uses the postfix user. The answer is postfix does not only use the postfix user, it starts up as root to read configuration files, and then changes to the postfix user. Nifty to know.

```
/usr/sbin/postmap /etc/postfix/sasl_passwd
```

This will create a sasl_passwd.db file with the same permissions
Take note: every time you make changes to this file you will need to postmap it again, and reload postfix to reread the db file. Lastly edit you main.cf

```
vi /etc/postfix/main.cf

--Add these three lines:

-------------------------------------------------
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options =
-------------------------------------------------
```

Save and exit.

- The first line just enables the authentication.
- The second line just points to the password file.
- The third line is for additional security options but since we are doing a basic setup we do not require additional settings.

Do a "*/etc/init.d/postfix reload*". This will reread the new changes and Voila! You will be able to send to that specific server or domain with authentication.

Take note: If you need to relay through a server that requires authentication then you need to add this additional line in your /etc/postfix/main.cf.

```
-------------------------------------------------------
relayhost = mail.example.com
-------------------------------------------------------
```

This will send all your mail through mail.example.com

Conclusion
SMTP Authentication, can be a useful security mechanism, but do not think it is fool proof. As I have mentioned smtp is a clear text protocol, which allows the username and password to be viewed. Consider this just an additional step to ensure that you are sending to the correct server or servers.
I hope you have found this useful, and always remember you won't learn things unless you try them.