GNU/Linux Administration - Feature #611

Configure Postfix and Dovecot To Use Forward Secrecy

05/02/2015 05:24 PM - Daniel Curtis

Status:	Closed	**Start date:**	05/02/2015
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Mail Server	**Estimated time:**	1.50 hour
Target version:	Debian	**Spent time:**	2.00 hours

Description

This is a guide for setting up forward secrecy with Postfix and Dovecot mail services.

Prepare the Environment

- Make sure the system is up to date:

```
apt-get upadte && apt-get upgrade
```

Harden Postfix

- Generate DH params, we don't go with 2048-bit EDH as not all clients might support this

```
openssl gendh -out /etc/postfix/dh_512.pem -2 512
openssl gendh -out /etc/postfix/dh_1024.pem -2 1024
```

- Edit the main postfix config file:

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

  - And add/modify the following parameters:

```
#the dh params
smtpd_tls_dh1024_param_file = /etc/postfix/dh_1024.pem
smtpd_tls_dh512_param_file = /etc/postfix/dh_512.pem

#enable ECDH
smtpd_tls_eecdh_grade = strong

#enabled SSL protocols, don't allow SSLv2 and SSLv3
smtpd_tls_protocols= !SSLv2, !SSLv3
smtpd_tls_mandatory_protocols= !SSLv2, !SSLv3

#allowed ciphers for smtpd_tls_security_level=encrypt
smtpd_tls_mandatory_ciphers = high

#allowed ciphers for smtpd_tls_security_level=may
#smtpd_tls_ciphers = high

#enforce the server cipher preference
tls_preempt_cipherlist = yes

#disable following ciphers for smtpd_tls_security_level=encrypt
```

```
smtpd_tls_mandatory_exclude_ciphers = aNULL, MD5 , DES, ADH, RC4, PSD, SRP, 3DES, eNULL

#disable following ciphers for smtpd_tls_security_level=may
#smtpd_tls_exclude_ciphers = aNULL, MD5 , DES, ADH, RC4, PSD, SRP, 3DES, eNULL

#enable TLS logging to see the ciphers for inbound connections
smtpd_tls_loglevel = 1

#enable TLS logging to see the ciphers for outbound connections
smtp_tls_loglevel = 1
```

- Restart postfix

```
service postfix restart
```

Harden Dovecot

Dovecot tries to use Perfect Forward Secrecy by default, so besides the enabled SSL almost no actions are required.

- Edit the Dovecot config file:

```
nano /etc/dovecot/dovecot.conf
```

  - And add/modify the following:

```
# specify the cipher list to use
ssl_cipher_list = EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA2
56:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:EECDH:EDH+aRSA:!aNULL:!eNULL:!LOW:!3
DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4

#only for dovecot >=2.2.6, enforce the server cipher preference
ssl_prefer_server_ciphers = yes

#disable SSLv2 and SSLv3
ssl_protocols = !SSLv2 !SSLv3
```

- Restart Dovecot:

```
service dovecot restart
```

Testing

- Try SSLv2 which shouldn't work and just hang

```
openssl s_client -connect mail.example.com:143 -ssl2
^C
```

- Test smtp with starttls

```
openssl s_client -starttls smtp -connect mail.example.com:25
quit
```

- *Truncated output*:

```
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
```

- Test imap with starttls

```
openssl s_client -starttls imap -connect mail.example.com:143
logout
```

- *Truncated output*:

```
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
```

h2. Resources

- https://www.2realities.com/blog/2014/02/13/secure-ssl-configuration-for-apache-postfix-dovecot/

History

#1 - 05/02/2015 05:44 PM - Daniel Curtis

- Description updated

- Status changed from New to In Progress

#2 - 05/02/2015 06:27 PM - Daniel Curtis

- Tracker changed from Support to Feature

#3 - 05/02/2015 06:28 PM - Daniel Curtis

- Subject changed from Configure Postfix and Dovecot Use Forward Secrecy to Configure Postfix and Dovecot To Use Forward Secrecy

#4 - 05/02/2015 07:43 PM - Daniel Curtis

- Description updated

- Status changed from In Progress to Resolved

#5 - 05/02/2015 07:44 PM - Daniel Curtis

- % Done changed from 0 to 100

#6 - 05/10/2015 09:21 AM - Daniel Curtis

- Status changed from Resolved to Closed