Sécurité de la messagerie

Jean-Marc Pouchoulon

Licence Pro MRIT- parcours CYBER

1 Environnement du TP et notation.

1.1 Objectifs du TP :

L'objectif de ce TD/TP est de vous faire travailler sur une architecture proche d'une "prod messagerie" et de mettre en place différents outils antispam et un antivirus. Vous travaillerez par groupe de deux en collaboration avec les autres groupes pour le routage des message.

Un compte rendu succinct (fichiers de configuration , réponses aux questions, logs de messagerie, copies d'écran montrant la réussite de vos tests antispam ...) est demandé. Rendez-le sur Moodle Didex avec un titre contenant vos noms et le sujet du TP mais votre travail sera évalué par l'enseignant à la fin de chaque partie (cf compétences).

Je rappelle que les jeux ne sont pas autorisés dans votre temps de travail ...

2 Mise en place d'une configuration basique de messagerie

Les compétences suivantes seront validées dans cette partie :

1. Mettre en place un serveur SMTP Postfix capable de recevoir des messages pour son domaine et de forwarder les messages pour les autres domaines vers un hub.
2. Savoir expliquer ce que font les options présentées par le "dpkg-reconfigure postfix".
3. Tester le bon fonctionnement d'un MTA depuis bash de plusieurs façons.
4. Tester l'anti-relais sur un serveur depuis le CLI.
5. Configurer Postfix pour le format Mailbox.

2.1 Installation basique de Postfix

Vous serez peut être amené à supprimer exim le MTA par défaut de Postfix :

```
apt-get remove exim4
```

Deux fichiers utiles pour configurer postfix :

— /etc/postfix/main.cf
— /etc/postfix/master.cf

Vous pouvez aussi passer le daemon smtp en mode debug afin de faciliter la résolution des problèmes et désactiver le chroot des daemons Postfix.

```
# ==========================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================
smtp      inet  n       -       n       -       -       smtpd -v
```

Les commandes suivantes peuvent aussi vous être utiles afin de vérifier que les démons de messagerie fonctionnent :

```
lsof -i :110,995,143,993
ss -tunlp # plus moderne que lsof
Vérifier que des processus écoutent bien sur les différents ports.
openssl s_client -connect localhost:465 # Vérifier les connexions ssl pour smtps
```

Vous forwarderez les messages qui ne sont pas à destination de la machine locale vers le serveur MX de l'IUT de Béziers. Votre MTA sera accessible sur le réseau et vous ferez les tests sur l'IP de votre machine. Vous utiliserez comme DNS le 10.255.255.204. qui résout les adresses des postes de la salle et leurs "reverse".

2.2 Vérification du bon fonctionnement du MTA Postfix via le CLI

Envoyez un message à l'utilisateur test de votre machine locale via une commande telnet :

```
[root@localhost ~]# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 localhost.localdomain ESMTP Sendmail 8.13.8/8.13.8; Sun, 21 Aug 2005 11:44:12 +0200
ehlo localhost
250-localhost.localdomain Hello localhost.localdomain [127.0.0.1], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN
250-STARTTLS
250-DELIVERBY
250 HELP
mail from:<test@localhost.localdomain>
250 2.1.0 <test@localhost.localdomain>... Sender ok
rcpt to:<test>
250 2.1.5 <test>... Recipient ok
data
354 Enter mail, end with "." on a line by itself
bla
.
250 2.0.0 j7L9iC9l003327 Message accepted for delivery
quit
221 2.0.0 localhost.localdomain closing connection
Connection closed by foreign host.
```

2.3 Envoi d'un mel avec les commandes mail et sendmail

Utilisez la commande mail afin d'envoyer un mel.

```
echo "test message=body" | mail -s "C'est le sujet" -a "From: test" jean-marc.pouchoulon@iutbeziers.fr
```

ainsi que la commande sendmail :

```
sendmail jean-marc.pouchoulon@iutbeziers.fr
From: test
```

```
Subject: C'est un sujet
test message=body
.
```

Regardez le fichier /var/spool/mail/test pour voir comment sont conservés les messages au format mbox. Que pensez-vous de ce format ?

Configurer Postfix afin d'utiliser le format Mailbox.

3 Routage de la messagerie et acceptation des mails

Les compétences suivantes seront validées dans cette partie :

1. Configurer une route sur Postfix vers un serveur afin de forcer l'envoi de tous les messages vers votre voisin pour un ou plusieurs domaines.
2. Utilisez un outil évolué (Swaks) afin d'envoyer les mels en ligne de commande.
3. Etre capable de décrire les principales variables participant à la configuration de Postfix.

3.1 Routage des messages au travers de la salle, autorisation de relayer les messages

Votre domaine sera le nom de votre poste suivi du domaine .local. (203-1.local)

Chaque groupe va configurer un serveur de messagerie postfix qui va forwarder tous les messages à son voisin direct. (sens horaire). Vous utiliserez le fichier /etc/postfix/transport pour le routage des mels et votre voisin autorisera votre serveur pour le relais.

Le dernier poste de la salle sera chargé de router les messages vers le MX du domaine iutbeziers.fr.

1. Utilisez les variables suivantes dans le fichier de configuration main.cf :

   Modifiez d'abord main.cf pour instancier les variables mydomain, myhostname, mynetworks ainsi que alias_maps et alias_database (qui doivent être positionnées)

   ```
   myhostname = 203-1.local
   mydomain = local
   mynetworks = 10.203.0.0/16, 10.203.0.0/16, 127.0.0.0/8
   alias_maps = hash:/etc/aliases
   alias_database = hash:/etc/aliases
   transport_maps=hash:/etc/postfix/transport
   relay_domains=$transport_maps
   smtp_dns_support_level = enabled
   smtp_host_lookup = dns, native
   ```

2. Expliquez à quoi servent ces variables.
3. Autorisez le routage des messages de votre voisin.
4. Créez une route dans le fichier transport afin de diriger tous les mails du domaine iutbeziers.fr vers l'IP de votre voisin. (Vous désactiverez la résolution DNS inverse à l'aide de crochets entourant l'IP).

   Le premier groupe enverra un message à jean-marc.pouchoulon@iutbeziers.fr et indiquera une route de messagerie afin de forwarder tous les messages à destination de iutbeziers.fr au groupe suivant. Le dernier groupe forwardera son message au serveur smtp MX du domaine iutbezier.fr.

   Swaks `http://www.jetmore.org/john/code/swaks/` vous permettra d'envoyer des mels en ligne de commande. Chaque groupe m'enverra un message ensuite en suivant la chaine.

4 Mise en place de défenses antispam de premier niveau

Les compétences suivantes seront validées dans cette partie :

— Savoir filtrer les messages de SPAMs provenant d'une adresse IP en la blacklistant.

— Limiter le nombre de SPAMs provenant de zombies grâce à un delais sur la connexion ("great banner").
— Limiter le SPAM en utilisant des listes noires.
— Filtrer des messages en s'appuyant sur des filtres d'en-têtes ("header check").
— Imposer une authentification au client SMTP lors de l'envoi d'un mel.
— Tester que l'authentification AUTH LOGIN fonctionne bien via telnet.

4.1 Utilisation de Postscreen comme première ligne de défense antispam

Utilisez postscreen afin d'effectuer des filtrages de bases. Un article sur le sujet est à votre disposition sur l'ENT.

1. Interdisez l'envoi de mel des groupes vous suivant dans la chaine de messagerie et n'autorisez les groupes vous précédant.
2. Utilisez les listes noires pour filtrer les emails.
3. Mettez un temporisateur sur la réponse au ehlo d'un client SMTP.

4.2 Utilisation des regex afin de filtrer en fonction de headers

1. Vérifier que vous êtes capables de filter sur un mot clef (exemple viagra) de votre choix dans le sujet du mel avec /etc/postfix/header_checks.

4.3 Mise en place d'une authentification sécurisée avec Postfix et dovecot.

Dovecot permet à Postfix d'authentifier les utilisateurs connus du système et est un moyen simple de faire de l'authentification avant d'autoriser l'envoi d'un mel.

1. Mettez en place une authentification sécurisée lors de l'envoi des emails (on se s'intéresse pas à POP et IMAP).
   Vous pouvez suivre le tutoriel suivant "un-serveur-mail-debian-avec-postfix-et-dovecot" qui est sur l'ENT.

2. Testez l'authentification avec un telnet sur le port 25 (AUTH LOGIN votre-password-en-base-64).
   Les commandes ci-dessous permettent d'encrypter le mot de passe en base 64.

```
echo -en "pouchou" | openssl enc -base64
LS1lbiBwb3VjaG91Cg==
perl -MMIME::Base64 -e 'print encode_base64("pouchou");'
```

   Vous pouvez tester le bon fonctionnement de l'authentification via Dovecot via :

```
doveadm auth test user pass
```

5 Utilisation d'un milter antispam et antivirus : rspamd

Les compétences suivantes seront validées dans cette partie :

— Utilisez un milter antispam et antivirus : RSPAMD.
— Vérifier le bon fonctionnement de l'antispam avec un fichier gtube.
— Vérifier le bon fonctionnement de l'antivirus avec un fichier eicar.
— Faire un schéma d'un architecture Antispam en dessinant un schéma des inter-relations avec les différentes briques de la solution.

1. Téléchargez le projet de construction d'une image Postfix Antispam et lancez le container :

```
git clone https://registry.iutbeziers.fr:5443/pouchou/docker-postfix
docker build -t registry.iutbeziers.fr/debian:postfix .
docker run --hostname postfix -p 7777:80/tcp -p 2525:25/tcp -p 587:587/tcp  -it \
 registry.iutbeziers.fr/debian:postfix bash
```

Dans le container lancez les daemons nécessaires à l'antispam et à l'antivirus.

```
/root/launch.sh
```

2. Testez l'antispam avec un fichier gtube (voir les logs).
3. Testez l'antivirus avec un enregistrement Eicar (voir les logs).
4. Vérifiez que Dkim fonctionne pour le domaine local.
5. Comment Postfix communique avec rspamd ?
6. Comment Clamav est-il appelé ?
7. Le greylist est-il activé ?
8. Faites un schéma descriptif des relations entre les différentes briques de la solution.
9. Générez une clef et des enregistrements pour un domaine DKIM (votre-poste.iutbeziers.fr).

6 Mise en place d'un serveur LDAP pour filtrer les SPAMS "en brute force"

Les compétences suivantes seront validées dans cette partie :

- Installer d'un backend Openldap pour Postfix.
- Configurer Postfix afin de faire le lien avec OpenLdap.
- Tester avec la commande postmap la validité d'un destinataire de Mail sur son domaine.

Le but est de bloquer l'envoi de mel vers des utilisateurs qui n'existent pas dans votre annuaire ldap. En rejettant au plus prêt de l'expéditeur on économise des ressources.

1. Configurez un container ldap en utilisant l'image et les indications de `https://github.com/osixia/docker-openldap`.

```
docker run --env LDAP_ORGANISATION="asur"
--env LDAP_DOMAIN="asur.LOCAL"
--net mail-network --hostname ldapmail
--env LDAP_ADMIN_PASSWORD="root"
--name ldapmail
--publish 389:389 -p 636:636
--volume /data/slapd/config:/etc/ldap/slapd.d
--detach osixia/openldap:1.3.0
```

2. Créez une entrée dans l'annuaire avec votre nom.
   Adaptez le ldif suivant :

```
dn: uid=pouchou,dc=asur,dc=local
objectClass: inetOrgPerson
objectClass: person
objectClass: organizationalPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
```

```
cn: jean-marc.pouchoulon
sn: pouchoulon
givenName: pouchoulon
uid: pouchou
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/pouchou
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}RWK9BASh/NsGzi0k4XLRm1Xt1DoEceJvtB1h1w==
mail: jean-marc.pouchoulon@iutbeziers.fr
```

Adaptez les commandes suivantes et lancez-les depuis l'hôte.

```
ldapmodify -H ldap://localhost -D "cn=admin,dc=asur,dc=local" -w root -a -f ./monldif.ldif
ldapsearch -vvv -H ldap://10.0.2.15:389 -D "cn=admin,dc=asur,dc=LOCAL" -w root -b "dc=asur,dc=local"
```

3. Installez le paquet postfix-ldap.
4. Créez un fichier /etc/postfix/ldap-aliases.cf en vous inspirant du fichier suivant.

```
server_host = ldap://adr_ip_serveur_ldap:389
search_base = o=gouv,c=fr
query_filter = (|(mail=%s)(mailEquivalentAddress=%s)(mailalternateaddress=%s))
result_attribute = mail
bind = yes
bind_dn = cn=xxxxx,o=gouv,c=fr
bind_pw = xxxxxx
timeout = 10
lookup_wildcards = no
scope = sub
result_filter = OK
```

5. Modifiez /etc/postfix/main.cf.

```
alias_maps = hash:/etc/aliases, ldap:/etc/postfix/ldap-aliases.cf
```

6. Utilisez la commande suivante pour verifiez que Postfix va accepter le mel à destination de cet utilisateur.

```
postmap -q jean-marc.pouchoulon@iutbeziers.fr ldap:/etc/postfix/ldap-aliases.cf
```