Antispam Test Dökümanı

Antispam sisteminin çalışabilmesi için öncelikle çalışan bir mail sunucuya ihtiyaç vardır. Mail sunucu kurulumu projenin kapsamı dışında olmakla beraber aşağıdaki adımlar mail sunucu kurulumu için yol gösterecektir.

Değişkenler

```
export DOMAIN="ahtapot.org"
export AVAS_HOSTNAME="avas"
export MAIL_HOSTNAME="mail"
export AVAS_IPv4="169.254.2.254"
export MAIL_IPv4="169.254.2.252"
export BIND9_Ipv4="169.254.2.252"
```

Hosts dosyası ayarları

```
sed -i "/127.0.0.1/ s/127.0.0.1.*/127.0.0.1\t${MAIL_HOSTNAME}.${DOMAIN}\t$
{MAIL_HOSTNAME}/" /etc/hosts
hostnamectl set-hostname ${MAIL_HOSTNAME}.${DOMAIN}
```

DNS Server Kurulumu

```
apt install bind9 dnsutils
```

DNS Server Ayarları

```
cat > /etc/bind/db.${DOMAIN} << EOF
; ${DOMAIN} Dumped Thu Jul 12 06:45:03 2018
;
${DOMAIN}. 86400   IN      SOA     ${DOMAIN}. root.${DOMAIN}. (
                                     2017092801      ;serial
                                     10800           ;refresh
                                     1800            ;retry
                                     604800          ;expire
                                     86400   )       ;minimum
${DOMAIN}. 300     IN      A       ${MAIL_IPv4}
${DOMAIN}. 86400   IN      NS      ns1.${DOMAIN}.
${DOMAIN}. 300     IN      MX      10 ${MAIL_HOSTNAME}.${DOMAIN}.
ns1.${DOMAIN}.     300     IN      A       ${BIND9_IPv4}
${MAIL_HOSTNAME}.${DOMAIN}.    300     IN      A       ${MAIL_IPv4}
${AVAS_HOSTNAME}.${DOMAIN}.    300     IN      A       ${AVAS_IPv4}

EOF

cat >> /etc/bind/named.conf << EOF

zone "${DOMAIN}" {
        type master;
        file "/etc/bind/db.${DOMAIN}";
};

EOF

cat > /etc/host.conf << EOF
order hosts,bind
multi on
EOF
```

```
cat > /etc/resolv.conf << EOF
domain ${DOMAIN}
search ${DOMAIN}
nameserver 127.0.0.1
EOF

systemctl restart bind9
```

Postfix Mail Server Kurulumu

```
DEBIAN_FRONTEND=noninteractive apt install -y -q postfix
```

Sertifika oluşturma

```
mkdir /etc/postfix/ssl
cd /etc/postfix/ssl/
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 2048

chmod 600 smtpd.key
openssl req -new -key smtpd.key -out smtpd.csr

openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt

openssl rsa -in smtpd.key -out smtpd.key.unencrypted

mv -f smtpd.key.unencrypted smtpd.key
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days
3650
chmod 600 cakey.pem
```

Postfix Mail Server Ayarları

```
postconf -e "smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt"
postconf -e "smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key"
postconf -e "smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem"
postconf -e "myhostname = ${MAIL_HOSTNAME}.${DOMAIN}"
postconf -e "mydomain = ${DOMAIN}"
postconf -e 'myorigin = $myhostname'
postconf -e 'home_mailbox = Maildir/'
postconf -e 'mailbox_command ='
postconf -e 'smtpd_banner = $myhostname ESMTP $mail_name'
#ipv4, ipv6, all
postconf -e 'inet_protocols = ipv4'

sed -i '/^mydestination/ s/$myhostname/$myhostname\, $mydomain/'
/etc/postfix/main.cf

systemctl reload posfix
```

Test için kullanıcı ekleme

```
adduser user1
adduser user2
```

Telnet ile mail gönderim testi

```
telnet 127.0.0.1 25
ehlo ahtapot.org
mail from: user1@ahtapot.org
rcpt to: user2@ahtapot.org
data
Subject: Test maili 1
Test mailidir.

.
quit
```

Maili kontrol etmek için alıcının aşağıdaki dizinine bakılır.

```
/home/user1/Maildir/new/*
```

Log dosyaları

```
tail -f /var/log/mail.*
```

Mail sunucusu bu şekilde kurulup mail başarılı bir şekilde göderildikten sonra oluşturulan sertifika dosyaları kullanım kılavuzunda belirtildiği şekilde antispam sistemine kopyalanır. Ardından antispam sistemi kullanım kılavuzunda açıklandığı şekilde parametreleri ayarlanarak kurulum gerçekleştirilir. Kurulumun ardından spam, virus ve spf testleri için aşağıdaki örnek test e-postaları gönderilir.

Telnet ile mail gönderim testi yapılır ve mail sunucuda ilgili kullanıcıya mailin gittiği görülür.

```
telnet 127.0.0.1 25
ehlo ahtapot.org
mail from: user1@ahtapot.org
rcpt to: user2@ahtapot.org
data
Subject: Test maili 1
Test mailidir.

.
quit
```

SPAM Test Loglardan izlenir.

```
telnet 127.0.0.1 25
ehlo ahtapot.org
mail from: user1@ahtapot.org
rcpt to: user2@ahtapot.org
data
Subject: Spam Test Maili
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

.
quit
```

Virüs Test

```
telnet 127.0.0.1 25
ehlo ahtapot.org
mail from: user1@ahtapot.org
rcpt to: user2@ahtapot.org
data
Subject: Virus Test Maili
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

.
quit
```

SPF Test

```
telnet mail.server.com 25
ehlo gmail.com
mail from: a@gmail.com
rcpt to: user1@ahtapot.org
data
test maili

.
quit
```

SKS Test Dökümanı

Sks playbook'u kullanım kılavuzunda belirtildiği şekilde kurulur. Ardından aşağıdaki şekilde test edilir.

Test için lokal bilgisayarınızda pgp tool'u kullanılarak aşağıdaki işlemler yapılabilir.
#Key Generate ederken system de event oluşturmak için

```
apt install rng-tools
rngd -r /dev/urandom
```

#Create Key

```
gpg --full-gengenerate-key
```

#List Keys

```
gpg --list-keys
/root/.gnupg/pubring.kbx
------------------------
pub   rsa2048 2018-07-10 [SC] [expires: 2020-07-09]
      08A23480C071AAF8AE2CE2EA85BD51A206EEC532
uid           [ultimate] Fatih USTA <fatihusta@labrisnetworks.com>
sub   rsa2048 2018-07-10 [E] [expires: 2020-07-09]

pub   rsa2048 2018-07-10 [SC] [expires: 2018-07-30]
      EE58FA26A7C6DB43A90900EC7D0E85D4BE63AFD3
uid           [ultimate] Fatih USTA (Fatih USTA GMAIL Account)
<fatihusta86@gmail.com>
sub   rsa2048 2018-07-10 [E] [expires: 2018-07-30]
```

#Server'a public key'in komut satırından gönderilmesi.

```
gpg --keyserver 169.254.2.254 --send-key 85BD51A206EEC532 # Son 16 karakter
```

#Web üzerinde Key import etmek için aşağıdaki gibi key export edilir.
#ASCII-armored OpenPGP Public Key

```
gpg --armor --export fusta@fusta.com
veya
gpg --armor --export 34EBACE1B5BAE8A1
```