SMTP (PORT 25) Penetration Testing

✓ Lab Setup

- Target machine ubuntu : `192.168.1.12` (IP Address)
- Attacking machine kali : `192.168.1.42` (IP Address)

✓ Host Name Configuration

```
sudo nano /etc/hosts
```

Here change with the domain name on not .com or .in anything

```
mail.kiran.com kiran
```

```
cat /etc/hosts
```

```
 GNU nano 7.2                                                /etc/hosts
127.0.0.1       localhost.localdomain   localhost
127.0.0.1       mail.kiran.com  kiran

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

To check :

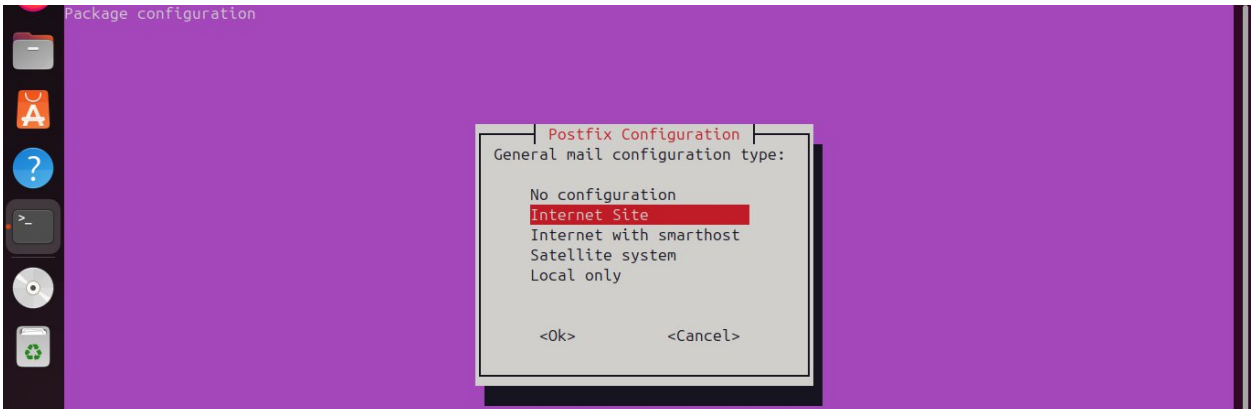
- `hostname`
- `hostname -f`

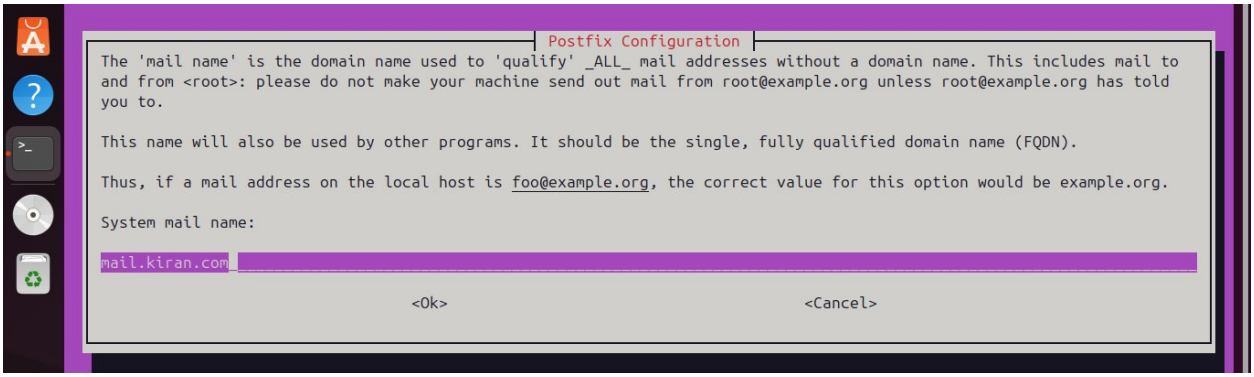
```
root@kiran:~# cat /etc/hostname
kiran
root@kiran:~# hostname -f
mail.kiran.com
root@kiran:~#
```

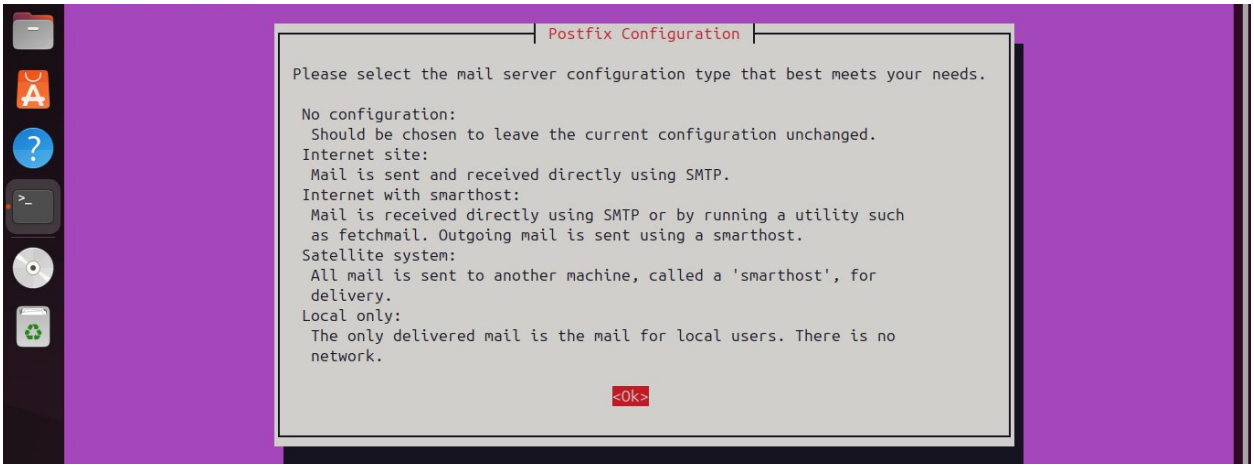
✓ Postfix Installation

cmd:- sudo apt-get install postfix

```
root@kiran:~# apt-get install postfix
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm19
Use 'apt autoremove' to remove it.
The following additional packages will be installed:
  libnsl2
Suggested packages:
  mail-reader postfix-cdb postfix-doc postfix-ldap postfix-lmdb postfix-mta-sts-resolver postfix-mysql postfix-pcre
  postfix-pgsql postfix-sqlite procmail sasl2-bin | dovecot-common
The following NEW packages will be installed:
  libnsl2 postfix
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,296 kB of archives.
After this operation, 4,321 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu noble/main amd64 libnsl2 amd64 1.3.0-3build3 [41.4 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/main amd64 postfix amd64 3.8.6-1build2 [1,254 kB]
Fetched 1,296 kB in 50s (26.2 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libnsl2:amd64.
(Reading database ... 162786 files and directories currently installed.)
Preparing to unpack .../libnsl2_1.3.0-3build3_amd64.deb ...
Unpacking libnsl2:amd64 (1.3.0-3build3) ...
```







- sudo nano /etc/postfix/main.cf

```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.kiran.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, mail.kiran.com, localhost.kiran.com, , localhost
relayhost =
mynetworks = 127.0.0.0/8 192.168.1.0/24
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

```
myorigin = /etc/mailname
mydestination = $myhostname, mail.kiran.com, localhost.kiran.com, , localhost
relayhost =
mynetworks = 127.0.0.0/8 192.168.1.0/24
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4
home_mailbox = maildir/
```

- service postfix restart
- netstat -tnl or -ntnl

```
root@kiran:~# service postfix restart
root@kiran:~# netstat -tnl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 :::993                  :::*                    LISTEN
tcp6       0      0 :::995                  :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::110                  :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::143                  :::*                    LISTEN
root@kiran:~#
```

✓ Installation of Dovecot

- Its agent POP3 and IMAP

```
sudo apt-get install dovecot-imapd dovecot-pop3d
```

```
root@kiran:~# sudo apt-get install dovecot-imapd dovecot-pop3d
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm19
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  dovecot-core libexttextcat-2.0-0 libexttextcat-data
Suggested packages:
  dovecot-gssapi dovecot-ldap dovecot-lmtpd dovecot-managesieved dovecot-mysql dovecot-pgsql dovecot-sieve dovecot-solr
  dovecot-sqlite dovecot-submissiond ntp
The following NEW packages will be installed:
  dovecot-core dovecot-imapd dovecot-pop3d libexttextcat-2.0-0 libexttextcat-data
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,785 kB of archives.
After this operation, 12.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu noble/main amd64 libexttextcat-data all 3.4.7-1build1 [193 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/main amd64 libexttextcat-2.0-0 amd64 3.4.7-1build1 [13.3 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 dovecot-core amd64 1:2.3.21+dfsg1-2ubuntu6.1 [3,351 kB]
```

- `cd /etc/dovecot/conf.d`
- `sudo nano 10-auth.conf`
- Change to diasble_plaintext_auth = yes

```
# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
# See also ssl=required setting.
disable_plaintext_auth = yes

# Authentication cache size (e.g. 10M). 0 means it's disabled. Note that
# bsdauth and PAM require cache_key to be set for caching to be used.
#auth_cache_size = 0
```

- Chage auth_mechenisms = plain login

```
# Space separated list of wanted authentication mechanisms:
#   plain login digest-md5 cram-md5 ntlm rpa apop anonymous gssapi otp
#   gss-spnego
# NOTE: See also disable_plaintext_auth setting.
auth_mechanisms = plain login

##
## Password and user databases
##

#
# Password database is used to verify user's password (and nothing more).
# You can have multiple passdbs and userdbs. This is useful if you want to
# allow both system users (/etc/passwd) and virtual users to login without
```

- `sudo nano 10-mail.conf`
- Change mail_location = maildir:/home/%u/Maildir

```
# <doc/wiki/MailLocation.txt>
#
mail_location = maildir:/home/%u/Maildir

# If you need to set multiple mailbox locations or want to change default
# namespace settings, you can do it by defining namespace sections.
```

- `sudo nano 10-master.conf`
    - Remove # -> port = 143

```
service imap-login {
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    #port = 993
    #ssl = yes
  }
```

- Remove # -> port = 110

```
service pop3-login {
  inet_listener pop3 {
    port = 110
  }
  inet_listener pop3s {
    #port = 995
    #ssl = yes
  }
}
```

- Add user & group = postfix

```
  # To give the caller full permissions to lookup all users, set the mode to
  # something else than 0666 and Dovecot lets the kernel enforce the
  # permissions (e.g. 0777 allows everyone full permissions).
  unix_listener auth-userdb {
    #mode = 0666
    #user = postfix
    #group = postfix
  }

  # Postfix smtp-auth
  #unix_listener /var/spool/postfix/private/auth {
```

- `Service dovecot restart`
- `Netstart -ntnl or -tnl`

```
root@kiran:~# service dovecot restart
root@kiran:~# netstat -ntnl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 :::993                  :::*                    LISTEN
tcp6       0      0 :::995                  :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::110                  :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::143                  :::*                    LISTEN
root@kiran:~#
```

✓ Installing Rain Loop

sudo apt install apache2 php php-curl php-json php-iconv php-xml php-dom php-mysql php-pdo libapache2-mod-php

```
root@kiran:~# sudo apt install apache2 php php-curl php-json php-iconv php-xml php-dom php-mysql php-pdo  libapache2-mod-php
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'php8.3-common' instead of 'php-iconv'
Note, selecting 'php8.3-xml' instead of 'php-dom'
Note, selecting 'php8.3-common' instead of 'php-pdo'
apache2 is already the newest version (2.4.58-1ubuntu8.8).
php is already the newest version (2:8.3+93ubuntu2).
php-curl is already the newest version (2:8.3+93ubuntu2).
php-curl set to manually installed.
php8.3-common is already the newest version (8.3.6-0ubuntu0.24.04.5).
php8.3-common set to manually installed.
php-xml is already the newest version (2:8.3+93ubuntu2).
php-xml set to manually installed.
php8.3-xml is already the newest version (8.3.6-0ubuntu0.24.04.5).
php8.3-xml set to manually installed.
php-mysql is already the newest version (2:8.3+93ubuntu2).
php-mysql set to manually installed.
The following package was automatically installed and is no longer required:
  libllvm19
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  libapache2-mod-php php-json
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
```

sudo apt install curl

```
root@kiran:~# apt install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (8.5.0-2ubuntu10.6).
The following package was automatically installed and is no longer required:
  libllvm19
Use 'apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

- cd /var/www/html
- rm *

```
root@kiran:~# cd /var/www/html
root@kiran:/var/www/html# ls
index.html
root@kiran:/var/www/html# rm *
```

Curl -s https://repository.rainloop.net/installer.php |sudo php

```
root@kiran:/var/www/html# curl -s https://repository.rainloop.net/installer.php | sudo php


      [RainLoop Webmail Installer]


 * Connecting to repository ...
 * Downloading package ...
 * Complete downloading!
 * Installing package ...
 * Complete installing!

 * [Success] Installation is finished!

root@kiran:/var/www/html#
```

http://localhost/?admin