**Lab on Email Services with sendmail**

- MUA (Mail User Agent): Examples->kmail, mozilla thunderbird, ms outlook express etc.
- MTA (Mail Transport Agent): Examples Sendmail, postfix, qmail etc.
- MDA (Mail Delivery Agent): Example-> procmail, sendmail)

Sender->MUA->MTA->MDA->Receiver

- Mails are stored in /var/spool/mail/<username>

**1. Configuring the MTA to Receive Mail**

```
#cd /etc/mail
#vi sendmail.mv
dnl DAEMON_OPTIONS (Port=smtp,addr=127.0.0.1,NAME=MTA)
#m4 sendmail.mc > sendmail.cf
```

Note:

- dnl is to comment the line so that mail can be received form anywhere. The above line will make the machine to accept mail from local host only.
- **sendmail.cf** is the main configuration file

```
#vi /etc/mail/local-host-names
     cba.com
     example.com

#service sendmail restart
```

**2. To allow host to relay message**

```
#vi /etc/mail/access
     172.16.0  RELAY
     shiba.com RELAY
     hacker.net     REJECT
     spammer.org    DISCARD
     badguy@cba.com ERROR:550 “BAD guys not allowd”
     shiba@cba.com  RELAY
     cba.com RELAY
```

**3. To create alises**

To send mail to all the members of group staff

```
#vi /etc/aliases
     staff: staff1, staff2, staffN
```

4. Virtual user and domains mapping

```
#vi /etc/mail/virtusertable
```

**Secure Dovecot**

```
#cd /usr/share/ssl/certs
#rm dovcot.pem
#make dovecot.pem
```

```
#rm /usr/share/ssl/private/dovecot.pem
cp /usr/share/certs/dovecot.pem /usr/share/ssl/private
```

**Secutiry**
**Lab on PAM Authentication**

**1. Restricting root user from logging through insecured terminals (blocking tty1)**

```
#vi /etc/securetty
     #tty1
```

**Note # is used to comment, just comment the line for restring loging to ttyN**

```
#vi /etc/pam.d/login
Or,
#vi /etc/pam.d/system-auth
     auth required pam_securetty.so
```

It will detect the setting of /etc/securetty

**2. To restrict normal users to login**

```
#touch /etc/nologin

#vi /etc/pam.d/login
     auth required pam_nologin.so
```

**3. Restricting particular user to login**

```
#vi /etc/security/access.conf
     -:user1 user2:ALL
```

Note:

```
syntax: permission:users:location
```

**4. Time based Restriction**

```
#vi /etc/security/time.conf
     login;*;S1|S2|S3;A109000-1700
```

```
Syntax: Application;location;user;time
Example
login;*;s1|s2;Mo0900-2400|TuWeTH0000-24000|Fr0000-1700
```

```
#vi /etc/pam.d/login
     account required pam_time.so
```

**5. Specifying Resources**

```
#vi /etc/security/limits.conf
     user hard nproc     100
#vi /etc/pam.d/login
     session required pam_limits.so
```

```
Note: we can write the account information in
/etc/pam.d/system-auth in place of login
```

**Lab on System Monitor**

**Locating for valnerable files:**
Locate SUID and SGID files and stories named in /root/ stickyfiles:

```
#find / -tpe f -perm +6000 2>/dev/null >/root/sticyfiles
```

**Locate world-writable files and store their named in root/world.writable.files:**

```
find / type f -perm -2 2>/dev/null>/root/world.writable.files
```

**Controlling access to files**

1. create a user named shiba
2. create two files in shiba's home directory
3. prevent the payroll file from being deleted
   #chattr +i /home/shiba/payroll
4. verity that the attributes have been changed
   #lsattr /home/shiba/*
5. Try to remove the file
   #rm /home/shiba/payroll

**Monitoring processes**

#top

Key Letters
M-sort by memory usage
L-load average display on/off
P – processor Usage
T – Time based sort
u – user based sort
k – likk process
r – to renice sort
s – to update time

**Display login and reboot history**

#last

**To display last reboot time**

#last reboot

**To display all running progress**

#ps -ax
(for detail see man page)

**To kill process use kill command (for detail see man)**

#kill -9 <process_id>

**Display the average lode of CPU and time duration of system running**

#uptime

**Lab on TCP wrapper**

**Using hosts.allow and hosts.deny to restrict user to user service**

Syntax in file:
domain:client_list:option

**1. To deny ftp access from cba.com domain**

#vi /etc/hosts.deny
vsftpd:.cba.com

**2. To allow telnet from 172.16.0.14 only**

#vi /etc/hosts.allow
in.telnetd:172.16.0.14
#vi /etc/hosts.deny
in.telnetd:All:ALL

**3. To allow ssh from all host of .cba.com except** station1.cba.com and all to localhost

#vi /etc/hosts.allow
sshd: .cba.com EXCEPT station1.cba.com EXCEPT LOCAL

**4. To allow ssh from only one interface among two (assuming ip is assigned to 1 interface we are using)**

#vi /etc/hosts.allow
sshd@172.16.0.1:ALL

**5. To allow ssh to all except cracker.org. But allowing trusted.cracker.org to access.**

#vi /etc/hosts.allow
sshd: ALL EXCEPT .cracker.org EXCEPT trusted.cracker.org

**Lab on Data Security**

**Secure https**

see in lab on http

**Secure dovecote**

see in lab on mail

**Lab on SSH**

#service sshd start
#ssh cba@172.16.0.1

**Using secure copy**

#scp cba@172.16.0.1:/etc/passwd /home/shiba

**Using SSH for Encrypted communications by avoiding issue of password**

User1
1. create a key
#ssh-keygen -t dsa
2. copy ~.ssh/id_dsa.pub to user2's computer in user2's ~/.ssh as authorized keys
#scp ~/.ssh/id_dsa.pub user2@172.16.0.1:/home/user2/.ssh/authorized_key
3. change the permission of !/.ssh to 700 and ~/.ssh/authorized_keys to 600

```
     #chmod 700 ~/.ssh
     #chmod 600 ~/.ssh/authorized_keys
4.ssh user2@172.16.0.1
```

**SSH server (Do find yourself)**

configuration file /etc/ssh/sshd_config

**To deny root from login using ssh**

```
     #vi /etc/ssh/sshd_config
          PermitRootLogin no
```

**To change port to 2008**

```
     #vi /etc/ssh/sshd_config
          Port 2008
```