LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Configurare minimala server

Fisierul de configurare al serverului ProFTPD este proftpd.conf
Acesta este format din directive si valorile acestora care stabilesc modul in care serverul functioneaza.

Exemplu:

proftpd.conf

```
#serverul asculta pe portul 21 pentru conexiuni de control
Port 21
```

Se recomanda pornirea de la un "schelete" de fisier de configurare care se modifica in functie de necesitati.
O astfel de mostra este /opt/proftpd/etc/proftpd.conf. Aceasta nu contine toate directivele de configurare ci doar pe cele mai importante.

Configurarea minimala a serverului ProFTPD presupune:

1. Crearea unui user si a unui grup sub care sa ruleze serverul.
Fisierul default de configurare cu care vine serverul si anume /opt/proftpd/proftpd.conf in cazul compilarii in directorul /opt/proftpd specifica faptul ca acesta ruleaza ca user nobody si grup nogroup. Acest user si grup sunt folositi in mod default de multe servere ceea ce duce la probleme de securitate.

Exemplu: In cazul in care exista un server Apache si un server Proftpd care ruleaza ca nobody si nogroup, iar serverul Apache este compromis, crackerul va avea acces total si la serverul Proftpd fiindca ruleaza sub acelasi user.

Important

Din punct de vedere al securitatii sistemului este obligatoriu ca fiecare server sa ruleze sub propriul user si group, iar acestea sa nu mai fie folosite in alt scop.

proftpd.conf

```
# Set the user and group under which the server will run.
User                    ftpuser
Group                   ftpgroup
```

2. Stabilirea modului de acces la sistemul de fisiere a unui utilizator odata logat.
Trebuie stabilit daca acesta este blocat (chrooted/jailed) in propriul home directory sau se poate "plimba" in mod liber prin tot sistemul de fisiere.
Directiva DefaultRoot NUME_DIRECTOR stabileste directorul in care un user odata logat este plasat. Pentru respectivul utilizator radacina sistemului de fisiere este NUME_DIRECTOR. Acesta nu poate iesi din director.

proftpd.conf

```
DefaultRoot ~
```

Important

Default directiva DefaultRoot este comentata ceea ce inseamna ca un user conectat prin ftp la server poate iesi din propriul home directory si se muta in orice director din sistemul de fisiere.

3. Activare/dezactivare modul anonymous
Protocolul FTP face referire la un mod special si anume modul anonymous. Acesta se foloseste in momentul in care se doreste logarea userilor fara autentificare.

Exemplu: downloadarea serverului ProFTPD s-a realizat prin FTP. Clientul de FTP s-a conectat la serverul FTP pe care se gaseau sursele logandu-se anonim (fara username sau parola). De multe ori username-ul introdus este anonymous iar parola o adresa de e-mail.

Fisierul sample profptd.conf face referire la sfarsitul sau la modul anonymous. Daca se doreste dezactivarea acestui mod (de recomandat daca nu este un server public) trebuie comentata intreaga sectiune.

Detalii sectiune anonymous din proftpd.conf

- Specifica directorul home al userilor anonimi. Acesta poate fi modificat, dar atentie la permisiunile pentru acel director.

```
<Anonymous /var/ftp>
```

- Specifica userul care se va loga anonim. Acesta este ftp sau anonymous (directiva UserAlias)

```
User                    ftp
Group                   ftp
# We want clients to be able to login with "anonymous" as well as "ftp"
UserAlias               anonymous ftp
```

- Limit the maximum number of anonymous logins

```
MaxClients              10
```

4. Alte configuratii

a) specificarea porturilor pasive pe care le va folosi serverul. Default acesta poate trimite clientului care doreste folosirea modului pasiv orice port mai mare ca 1023 pentru ca acesta sa se conecteze la server la portul trimis. Se recomanda limitarea intervalului de porturi pasive folosite.

```
PassivePorts 49152 65534
```

b) modificare umask si anume pentru stabilirea permisiunilor default cu care se creaza noile fisiere si directoare.

```
Umask                   0022
```

c) modificare umask doar pentru un anumit director.

```
<Directory ~/test>
      umask 0066 0077
</Directory>
```

d) Dezactivare logarii userului root. Se recomanda din considerente de securitate.

```
RootLogin off
```

Exemplu configuratie completa server proftpd:

- server asculta pe portul tcp/21 pentru conexiuni pentru sesiunea de control (default);
- serverul ruleaza sub userul ftpuser si ftpgroup;
- fiecare user conectat si autentificat la server este "jailed" sau izolat in propriul home directory;
- nr. maxim de conexiuni concurente este 10;
- modul anonymous este dezactivat;
- autentificarea userilor are loc pe baza informatiilor din /etc/passwd si /etc/shadow;
- porturile pasive folosite de server sunt doar cele din intervalul 49152-49172;
- login-ul userului root nu este permis;

Exemplu proftpd.conf complet:

```
ServerName              "ProFTPD Default Installation"
ServerType              standalone
DefaultServer           on

# Port 21 is the standard FTP port.
Port                    21

# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
```

```
Umask                   022

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd).
```

Resurse

- Lista completa a directivelor ProFTPD
- ProFTPD FAQ