



System Administration Practice

Homework2 - File System Server

lctseng / yench / chchang2222

FTP (1)

- ❑ Install a FTP server for FreeBSD
 - Pure-FTPd: `/usr/ports/ftp/pure-ftpd`
- ❑ Compile it with “upload script” support (from port)

```
pure-ftpd-1.0.42
-(-)
[ ] ANONRENAME Allow anonymous user to rename files
[ ] ANONRESUME Allow anonymous user to resume file upload
[x] DOCS Build and/or install documentation
[x] EXAMPLES Build and/or install examples
[ ] LARGEFILE 2GB+ file download
[ ] LDAP User accounts in LDAP directories
[ ] MYSQL User accounts in MySQL database
[x] PAM PAM authentication
[ ] PERUSERLIMITS Per-user concurrency limits
[ ] PGSQL User accounts in PostgreSQL database
[x] PRIVSEP Privilege separation (recommended)
[x] SCRYPT Hash passwords in PureDB with scrypt
[x] SENDFILE Sendfile syscall
[ ] THROTTLING Bandwidth throttling
[x] TLS Secure network connection support via TLS
[x] UPLOADSCRIPT Uploadscript daemon support
[x] UTF8 UTF-8 filenames
-.(+)
94%
process and fork it in background.
< OK > <Cancel>
```

FTP (2)

❑ Settings (total 25%)

1. Anonymous Login

- ❑ Can **download** from */home/ftp/for_all*
- ❑ Can **upload & mkdir** from */home/ftp/anonymous*
- ❑ Can't **delete** from */home/ftp/anonymous*
- ❑ *Can only download the files which owner isn't "ftp"*
- ❑ Hidden directory */home/ftp/private*
 - There is a directory called "flag" inside
 - Client can't list in */home/ftp/private/* but can in *private/flags*

FTP (3)

- ❑ Settings (cont'd)
 2. Create a virtual user “ftp-god”
 - ❑ Chrooted (*/home/ftp* is your root directory)
 - ❑ Password is your student-id
 - ❑ Full access to */home/ftp*
 - ❑ Read/write to *ftp root directory/private/for_all/anonymous*
 - ❑ Private directory is visible to ftp-god
 3. Create a system user “sysgod”
 - ❑ Could login by **ssh**
 - ❑ Password is your student id
 - ❑ Permission is same as ftp-god
 4. Your ftp server should support **FTP over TLS**
 5. All accounts are **chrooted** (*/home/ftp* is the root directory)

FTP (4)

❑ Grading

- Anonymous login (total 10%, 2% for each)
 - Download from “for_all”
 - Upload to “anonymous”
 - Can’t delete from “anonymous”
 - Can only download the files which owner isn’t “ftp”
 - Hidden directory “private” problem: enter without listing
- ftp-god (total 5%)
 - (3%) Full access for “/home/ftp”, “for_all”, “anonymous”
 - (2%) Full access for “private” (read, write)
- Sysgod (total 5%)
 - (3%) Login from ssh
 - (1%) Full access for “/home/ftp”, “for_all”, “anonymous”
 - (1%) Full access for “private” (read, write)
- TLS connection (ftpes) (5%)

FTP – Hints (1)

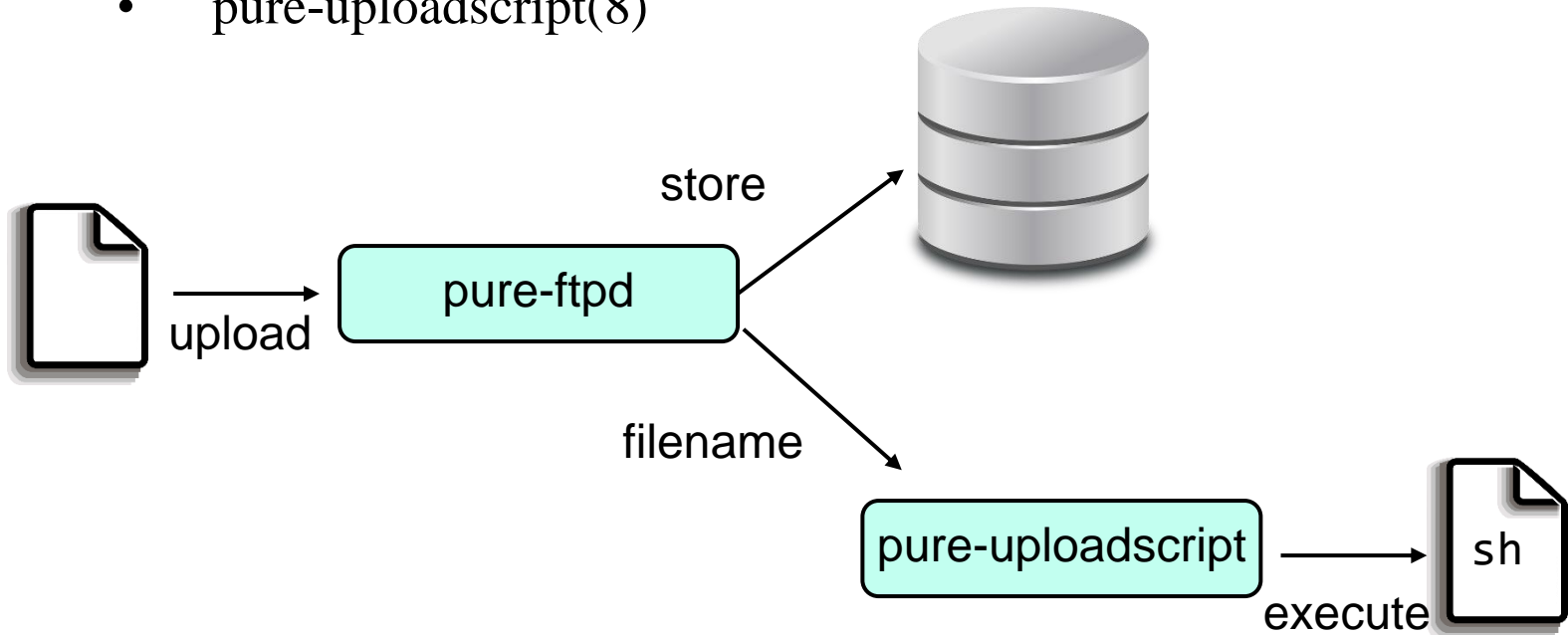
- ❑ Lots of README
 - `/usr/local/share/doc/pure-ftpd/*`
- ❑ Accounts related:
 - `pure-pw(8)`
 - `pure-pwconvert(8)`
 - `README.Virtual-Users`

FTP – Hints (2)

- ❑ How to setup demo environment
- ❑ Within VM, using notebook/remote desktop
 - Don't need to open GUI for VM (console)
 - Just need putty and Filezilla
 - Use host-only network interface, connect from host OS
 - host-only network interface: create connection between host and VM
- ❑ Within VM, no remote desktop
 - Using public IP
 - Active mode from npbsd0~4 (`ftp -A -P 8021 140.113.X.Y`)
 - Port forwarding for your VM (related to your firewall)
- ❑ Real Machine
 - Using public IP
- ❑ If you have public IP, use bridge mode is better for VM

RC (1)

- ❑ Write some rc scripts to start daemons when booting
- ❑ Upload script for pure-ftpd
 - A program executed when files are uploaded
 - pure-uploadsript(8)



RC (2)

❑ Record uploaded filenames

```
9:54pm lctseng@lctseng(10.0.2.15)[~]
] > tail -f /var/log/sa_ftp_log
upload:/usr/home/ftp/easing function.rb
upload:/usr/home/ftp/test.rb
upload:/usr/home/ftp/desktop.ini
upload:/usr/home/ftp/desktop.ini
```

❑ Your task

- Write a rc script called “sa_upload” under /usr/local/etc/rc.d

```
22:29 root@lctseng(10.0.2.15)[/usr/local/etc/rc.d]
[^^] # ll | grep sa_upload
-rwxr-xr-x  1 root  wheel   530  10  14  21:59 sa_upload*
```

RC (3)

- ❑ RC script can be used to start the pure-uploadsript program
 - Instead of executing that program manually

```

7:22pm lctseng@lctseng(10.0.2.15)[/etc]
[W5]g> sudo service sa_upload start
Password: bz2
Starting sa_upload.
10:32pm lctseng@lctseng(10.0.2.15)[/etc]
[W5]g> ps auxww | grep pure-uploadsript
rootg.5.bz2 8582  0.0ai0.2.25576 4624 - sslog 10:32下午 0:00.00 /usr/local/sbin/pure-uploa

```

- ❑ This rc script requires “sa_upload_enabled="YES"” in /etc/rc.conf
 - Just like a daemon start-up script

RC (4)

- ❑ Kill pure-uploadsript using rc script

```
10:35pm lctseng@lctseng(10.0.2.15)[/etc]
[W5] > sudo service sa_upload stop
Kill:8582
```

- ❑ This requires a pid file to indicate which process to stop

```
10:37pm lctseng@lctseng(10.0.2.15)[~]
[W5] > cat /var/run/pure-uploadsript.pid
8626
```

- You need this to write the stopping function

RC (5)

❑ Prepare for upload script

- Enable upload script under pure-ftpd.conf
 - CallUploadScript yes
- Create a simple upload script and rename it to /root/sa_upload_process
 - Don't forget to `chmod a+x sa_upload_process`

```
10:48pm lctseng@lctseng(10.0.2.15)[/root]
[W4] > ll sa_upload_process
-rwxr-xr-x 1 root wheel 51 10 14 21:35 sa_upload_process*
```

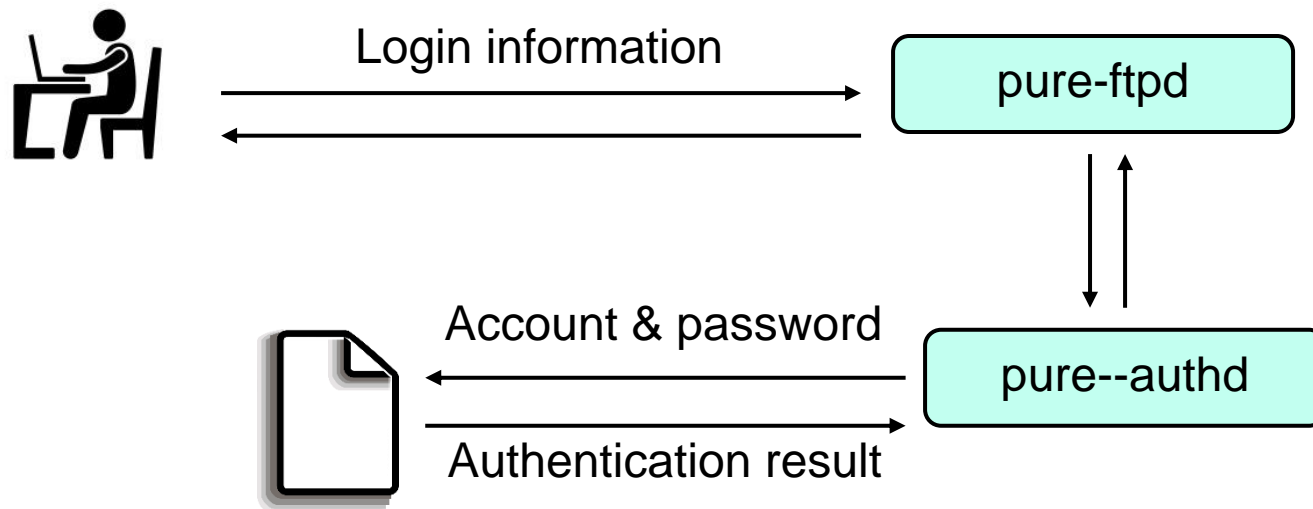
- Script content is provided below: (copy info file and rename it)

```
#!/bin/sh
echo "upload:$1" >> /var/log/sa_ftp_log
```

- After starting **pure-ftpd**, you need to start **sa_upload** so that you can upload files

RC (6)

- ❑ External authenticate for pure-ftpd
 - You can write your own program to check password
 - pure-authd(8)
 - README.Authentication-Modules



External program

RC (7)

- ❑ In this homework, there is special account ‘alibaba’
 - Not a system nor a virtual user account
 - Login with password “opensesame”
 - Go into /tmp
 - Other password
 - Go into /home/ftp



RC (8)

- ❑ Same as previous, you need to write a rc script under `/usr/local/etc/rc.d`

```
23:50 root@lctseng(10.0.2.15)[/usr/local/etc/rc.d]
[^_^] # ll | grep sa_auth
-rwxr-xr-x 1 root wheel 504 10 14 23:44 sa_auth*
```

- ❑ Enabled by `sa_auth_enabled="YES"` in `/etc/rc.conf`
- ❑ Controlled by service `sa_auth` start/stop
- ❑ The authentication script is placed in `/root/ftp-auth-handler`

RC (9)

❑ Prepare for external authentication

- Enable upload script under pure-ftpd.conf
 - ExtAuth `/var/run/ftpd.sock`
- Create a simple upload script and rename it to `/root/ftp-auth-handler`
 - Don't forget to `chmod a+x ftp-auth-handler`
 - Script content is provided below: (copy info file and rename it)

```
#!/bin/sh
if [ "$AUTHD_ACCOUNT" = "alibaba" ]; then
    echo 'auth_ok:1'
    echo 'uid:65534'
    echo 'gid:65534'
    if [ "$AUTHD_PASSWORD" = "opensesame" ]; then
        echo 'dir:/tmp'
    else
        echo 'dir:/home/ftp'
    fi
else
    echo 'auth_ok:0'
fi
echo 'end'
```


RC (10)

❑ Requirement

- Control the upload script daemon with service sa_upload start/stop
- Control the external auth daemon with service sa_auth start/stop
- Can record filenames into /var/log/sa_ftp_log
- Special user 'alibaba' can login with password 'opensesame', see different directory(/tmp), otherwise see /home/ftp
- pure-ftpd, pure-uploadsript and pure-authd should start automatically when booting

RC (11)

❑ Grading

- sa_upload (5%)
 - (2%) Upload record functionality (can demo **without rc script**)
 - rc script
 - (2%) Controlled by service(8)
 - (1%) Startup automatically
- Sa_auth (5%)
 - (2%) External authentication functionality (can demo **without rc script**)
 - rc script
 - (2%) Controlled by service(8)
 - (1%) Startup automatically

RC – Hints (1)

- ❑ For pure-uploadsript, you can manually start the daemon by following commands

```
pure-uploadscrip -B -r /root/sa_upload_process
```

- ❑ For pure-authd

```
pure-authd -s /var/run/ftpd.sock -r /root/ftp-auth-handler -B
```

- ❑ Before you write rc scripts, you can use these commands to check that whether you enable the upload-script/external-auth services

RC – Hints (2)

- ❑ How to write a rc start-up script:
 - <https://www.freebsd.org/doc/en/articles/rc-scripting/>
- ❑ You needs some shell script technique
 - <https://www.twbsd.org/cht/book/ch24.htm>
- ❑ README.Virtual-Users
 - <http://download.pureftpd.org/pub/pure-ftpdoc/doc/README.Virtual-Users>
- ❑ README.Authentication-Modules
 - <http://download.pureftpd.org/pub/pure-ftpdoc/doc/README.Authentication-Modules>

Samba

Install Samba

- `/usr/ports/net/samba4`

Location

- Samba share `/home/ftp/for_all` to Windows (10%)
- Mount Windows directory at `/home/ftp/windows`(5%)

You should create at least 4 accounts

Admin (total 5%)

- Full access (read, download, delete, rename, mkdir, upload) to all files and directories

Guest (total 5%)

- Can only list the files and directories (2%)
- Can't perform (read, download, delete, rename, mkdir, upload) to all files and directories (3%)

Samba

❑ Common User (total 10%)

❑ Test1

- Can (read, rename, delete, download) to Test1's files (3%)
- Can mkdir (1%)
- Can upload files to Test1's directory and root directory */home/ftp/for_all* (1%)
- Can't do (read, rename, delete, download) to other files and directories (5%)

❑ Test2

- Can (read, download, delete, rename) to Test2's files
- Can mkdir
- Can upload files to Test2's directory and root directory */home/ftp/for_all*
- Can't do (read, download, delete, rename) to other files and directories

ZFS on /home/ftp

- Create a zfs file system with mirror (5%)
- Set compression (5%)
- Do zfs snapshot (5%)
- Do zfs rollback (5%)
- Automatic snapshot script (10%)
 - Write a script such that whenever the script is invoked, it will take a snapshot for the dataset; in addition, it will only preserve the most recent 7 snapshots took by this script.
- Automatic backup (5% bonus)
 - Periodically backup a zfs dataset to google drive

Reminder

- ❑ Demo with root is **not allowed**
- ❑ Please use **sudo**
 - */usr/ports/security/sudo*
- ❑ File/directory permissions are important
 - Owner, group, other
 - Read, write, execute
 - Set UID, set GID, sticky bit
- ❑ Setting **port forwarding** to allow your services to be accessible over the Internet

Deadline

- Demo sheet will be available next week
- Demo week: **10/26~10/30**
- More details about demo will be announced soon

Help!

- ❑ Newsgroup cs.course.sysadm
- ❑ BS2 board CS-SysAdmin
- ❑ CSCC (EC building 3F)
- ❑ ta@nasa.cs.nctu.edu.tw (For complex problems)
- ❑ IRC channel #nctuNASA (Recommend)
 - passwd: ILoveCSCC
 - Use screen or tmux to stay online, so TAs can tag you to answer your questions.
- ❑ Before you ask a question...
 - 提問的智慧: How To Ask Questions The Smart Way
 - <http://mis.ndhu.edu.tw/docu/question.htm>