

Week 03

Deadline: Saturday, March 4th 2017

Preparation before lab

Before doing our lab session, **please update osteam's public key**, because the old one found in week02 is going to be expired soon. To do that, follow these simple steps.

1. Login to your badak account
2. Make work03 folder in your work directory change your present working directory to work03

```
$ cd work  
$ mkdir work03  
$ cd work03
```

3. You must copy a file for this week's task (you can download it on SCELE week03 forum) and put it in "work03" folder

- a) 01-public-osteam.txt

This is osteam's public key, Save it into a file named "01-public-osteam.txt"

Remember to use **tunnels** which was used in previous week's task

4. Check whether the files copied safely by using ls-al command.

```
$ ls -al
```

5. Import osteam's public key using command "gpg --import <key_file>"

```
$ gpg --import 01-public-osteam.txt
```

6. Go back to your badak home

```
$ cd ~/
```

Get to know what boot is all about

1. Create a new text file named "what-is-boot.txt" on your badak home

```
$ vi what-is-boot.txt
```

2. Write the following text on "what-is-boot.txt"

```
Hello, this is explanation about linux booting!
```

When you're done, save your file

```
Esc  
:wq
```

3. Create a new script file named `".profile"`

```
$ vi .profile
```

4. Add commands to echo your name and print the contents of `"what-is-boot.txt"` in `".profile"` script

```
echo <<your-name>>  
cat what-is-boot.txt
```

When you're done, save your file

```
Esc  
:wq
```

5. Run the `".profile"` script to check your work

```
$ bash ".profile"
```

6. Exit from badak

```
$ exit
```

7. Login with your badak account again to see the work showing on start-up

```
$ ssh your\_username@badak.cs.ui.ac.id
```

Example:

```
Last login: Sat Feb 25 08:56:06 2017 from kawung.cs.ui.ac.id  
nama kamu  
contoh jawaban
```

8. Answer the question below on `"what-is-boot.txt"`

Explain the order of events when a linux computer start up!

WARNING: Don't forget to put the source of your answer. Make sure it is your own answer, don't plagiarize!

When you're done, save your file

```
Esc
```

```
:wq
```

9. If you see your name and your answer when you first login, you have succeeded your first subtask!

Example of start up script

10. From badak home, go to `/etc/init.d/`

```
$ cd /etc/init.d/
```

11. Copy `sudo` to your badak home

```
$ cp sudo ~/
```

12. Go back to your badak home

```
$ cd ~/
```

13. Open `sudo` in `vi` and try to understand the script

```
$ vi sudo
```

14. Answer the question below on the script below the code

Explain what happen when the system runs this command

```
$ /etc/init.d/sudo start
```

WARNING: You can't actually run the command because you don't have the privilege

Use comment to answer it. This is how you comment

```
# this is an example of comment,  
# make sure you put the hashtag  
# at the start of every row
```

WARNING: Make sure it is your own answer, don't plagiarize!

15. Save and exit your `sudo` file

```
Esc  
:wq
```

16. Rename your `sudo` into `sudo-explanation.txt`

```
$ mv <<current file name>> <<new file name>>
```

17. Move `.profile`, `what-is-boot.txt`, and `sudo-explanation.txt` from your badak home into `work03` folder

```
$ cd ~/
$ mv <<file name>> <<new file location>>
```

18. Make sure there are 3 files in your `/work/work03`

```
$ ls -al
```

Remember, there are 3 files to be moved into `work03` folder: `.profile`, `what-is-boot.txt`, `sudo-explanation.txt`

19. Congratulations! You have learned about boot and startup script.

Back to Privacy Matters, Encryption and Digital Signature using GnuPG

1. Now let's get back to our encryption session: Sign your works so the others will know that they truly are your work. First we generate hash of all your works. So, instead of signing every file, we just need to sign the hash. We will use *SHA-1 algorithm* for now. (Ask *uncle G* for more information about *hashing* and *SHA-1*). Execute the following commands

```
$ shasum * > SHA1SUM
$ shasum .profile >> SHA1SUM
$ shasum -c SHA1SUM
```

- The first command is for creating SHA1SUM to all files in current directory (**work03**) and save it into a file named "SHA1SUM"
 - The second command is to append .profile because it cannot be added automatically with shasum * > SHA1SUM. **Don't forget to do this!**
 - The third command is for verify the hash of your files. The "OK" output means there is no modification in your current files (try to modify some of your files and then verify it). So, **if you modify your files, you must generate the new hash of it.**
2. To sign a file, use command "gpg --sign --armor --detach <file>". The "--sign --armor --detach" argument means "*create detached signature with ASCII armored (human readable) output*"

```
$ gpg --sign --armor --detach SHA1SUM
```

After this, there should be a file called SHA1SUM.asc, the signature file. This file contains hash and information of the one who signing the file (again, checked by public key)

3. Try to verify your signature. Use command "gpg -verify <signature_file> [<file>]". The "<file>" argument is optional. If not provided, it will try to use <signature_file> without ".asc" suffix (e.g test.asc → test)

```
$ gpg --verify SHA1SUM.asc
```

So, as long as the signature is good, we can ensure that the files in this folder (**work03**) is not being modified from the last time of your works

4. Create a tar ball. Tar is a way to create an archive file. They will be a new file called "work03.tbj". You can ask uncle G for more information.

```
$ cd ..  
$ tar cvfj work03.tbj work03/
```

*Useful info: to untar the .tbj file, you can use command "tar xvfj <file>"

5. Now you can start encrypting your files. To encrypt a file, use command "gpg --encrypt [--recipient <recipient_identifier>] <file>".

The "--recipient <recipient_identifier>" argument define the one who can decrypt the file. You can define n many recipients.

Encrypt the tar file

```
$ gpg --output work03.tbj.gpg --encrypt --recipient OSTEAM --recipient  
your@email.com work03.tbj
```

*Use the same email as your Email input on GnuPG key generator.

**Usefull info: after this, there should be a file called <file>.gpg. That is the encrypted version of your <file> (try to read the content if you can). That file only can be decrypted using recipient's private key (in this case either use osteam's or yours). To decrypt a file, use command "gpg <file>"

```
$ gpg <file>.gpg
```

6. Copy the file to your github account, under the file week03/

```
$ cp work03.tbj.gpg ~/os171/week03/work03.tbj.gpg
```

7. Change your directory to "~/os171/week03/"
8. Remove file named "dummy"
9. Check whether there is a file named work03.tbj.gpg. If you can't find it, do the copy once more from the "work03" directory
10. Push the change to GitHub server. You can see GitHub tutorial in week01 forum
11. Done

Review your Work

Dont forget to check your files/folders. After this lab, your current `os171` folder should looks like:

```
os171
  key
    mypublickey1.txt
  log
    log01.txt
    log02.txt
    log03.txt
  SandBox
    <some_random_name>
  week00
    report.txt
  week01
    lab01.txt
    report.txt
    myExpectation.txt
    what-time-script.sh
  week02
    work02.tbj.gpg
      *work02
        *00-toc.txt
        *01-public-osteam.txt
        *02-ls-al.txt
        *03-list-keys1.txt
        *04-list-keys2.txt
        *hello.c
        *hello
        *status.c
        *status
        *loop.c
        *loop
        *exercise.c
        *exercise
        *SHA1SUM
        *SHA1SUM.asc
  week03
```

```
work03.tbj.gpg
    *work03
        *01-public-osteam.txt
        *.profile
        *sudo-explanation.txt
        *what-is-boot.txt
        *SHA1SUM
        *SHA1SUM.asc
week04
    dummy
week05
    dummy
week06
    dummy
week07
    dummy
week08
    dummy
week09
    dummy
week10
    dummy
xtra
    dummy
```

keep in mind for every files/folders with wrong name, you will get **penalty** point.

***means file that should be inside the archived file.**