Homework #5

Due Time: 2016/5/18 (Wed.) 17:00
Contact TAs: `vegetable@csie.ntu.edu.tw`

Submission

- Compress all your files into a file named **HW5_<studentID>_<version>.tar.gz**, which contains two folders named **<studentID>_SA1** and **<studentID>_SA2** respectively.
- **Folder <studentID>_SA1** should contain a pdf file of all your answers and the command(s) you wrote in *System Administration 1 Part*.
- **Folder <studentID>_SA2** should contain a pdf file of all your answers in *System Administration 2 Part*.
- Submit your tar file to **sftp://intern.csie.ntu.edu.tw:7000** with your workstation account and password.

Instructions and Announcements

- Discussions with others are encouraged. However, you should write down your solutions `in your own words`. In addition, for each problem you have to specify the references (the Internet URL you consulted with or the people you discussed with) on the first page of your solution to that problem.
- Problems below would be related to the material taught in the class and might be far beyond that. Try to search for additional information on the Internet and give a reasonable answer.
- Some problem below might not have standard solutions. We would give you the point if your answer is followed by reasonable explanations.
- **NO LATE SUBMISSION IS ALLOWED.**

System Administration 1

Debian Package Manager

In problem 1-2, write down your answer. In problem 3-9, write down your commands. You may use `apt-*`, `aptitude`, `dpkg/dpkg-*` commands to answer the question. Replace the key id with `$keyid` in the answer.

1. What is the difference between `apt-get update`, `apt-get upgrade` and `apt-get dist-upgrade` commands?
2. What is the difference between `apt-get remove`, `apt-get autoremove` and `apt-get purge` commands?
3. List all packages with name containing `perl`.
4. Find out the package containing file `/usr/bin/ncat`.
5. In our in-class lab, we installed a meta package `nasa-meta`, which depends on `gcc`. In this situation, we call `nasa-meta` is installed as explicit and `gcc` is installed as dependencies. What is the command to determine whether `gcc` is installed as explicit or dependencies?
6. Change `gcc` from installed as dependencies to installed as explicit.
7. Generate a gpg key and sign the `nasa-meta` package.
8. Add the key generated above to the list of trusted keys used by apt.
9. (Bonus) Create a local repository in `/srv/repo` and add it to `sources.list`. Add the signed `nasa-meta` package into the repository. You need to prepare `Packages`, `InRelease`, `Release` and `Release.gpg` files.

After doing 7-9, we can `apt-get install nasa-meta` without warnings! Write down your answer/commands to `<your student ID>`.pdf.

System Administration 2

1 System Log

System logging facility varies between operating systems and distributions, so please write down the name and the version of the GNU/Linux distribution you use in this section. If you use more than one GNU/Linux distribution, please write down the name and the version again whenever you change the distribution.

There is no portability requirement on commands or scripts written in this section. Just write down what work on your system.

1.1 The standard system logging facility

`syslog` is the standard API and protocol to write logs on Unix-like systems. It is usually implemented by running a service accepting socket connections from any process. The service may store messages in text files, binary files, databases, depending on the configuration. Many implementations also support forwarding messages to another server.

1. Most systems use a socket file at `/dev/log` to receive messages from local applications. Which process on your system listens on it? Which package does it belong to? Write down how you find the answer.

2. Most systems store logs in `/var/log` directory. Use `logger` command to send a message to the system. Please find out where your message get written. Is it stored in a text file or a binary file? If it is a text file, write down the line or the entry containing your message. If it is a binary file, write down which tool is used to read the log file.

3. Run the following 3 `logger` commands with different messages:

   a. `logger -p mail.err -t sendmail <msg1>`

   b. `logger -p auth.info -t sshd[8352] <msg2>`

   c. `logger -p user.emerg -t ta217 <msg2>`

   Does these 3 messages get stored in the same file? Is there a reliable way to distinguish between messages produced by users and system services? If the answer is yes, describe the difference between them. If the answer is no, can you find a way to make your log system more trusted?

1.2 Systemd journal service

`systemd` is an init system and a service manager made for GNU/Linux. It also contains a login manager, a logging service and many other services. Its logging service is called journal, or `systemd-journald`. It uses its own binary format to store messages. Each message has many useful and trusted metadata fields automatically recorded by the journal service.

`journalctl` is the tool used to access the systemd journal. It supports several different output formats and it can filter messages with simple matches. All questions here can be answered with single command without using pipe, `grep`, `sed`, `awk` or other text processing tools.

1. Which systemd version you are using? Please remember to answer this question so we can know your environment.

2. Is your systemd journal persistent across reboots? If it is currently volatile, you have to make it persistent now because the next question requires it. Write down the command you use to make it persistent.
3. Print all messages sent to `dmesg` of previous boot.
4. Print all messages generated by the SSH server. Run `logger -t sshd <msg>` with random messages several times and make sure these bad messages don't show in the output.
5. Print all messages produced by both `dbus` user and your own user account.
6. Print all messages generated by `/usr/bin/sudo` executable.

2 Network Log

As an NTU CSIE workstation administrator, you sometimes get messages from NTU C&INC that machines you manage have tried to attack other machines on the Internet or downloaded too many papers in a short time. To resolve this kind of issue, you must be able to find the user who did the network connection that triggered the detection system.

Please set up Linux netfilter to log required information, so you can find the user with IP addresses, TCP/UDP ports and time.

> **Note** To use Linux netfilter, you can use `nftables` or `iptables` to add packet filtering rules. `nftables` is a new framework and using Linux >= 3.18 is recommended. `iptables` is an older framework and it is fully supported on all stable and longterm Linux releases.