Unix Fundamentals – System

Marek Kozłowski
Faculty of Mathematics and Information Sciences
Warsaw University of Technology

Never use copy&paste for the following exercises. Retype all commands manually!
Don't just read those exercises and examples. Do them, please!

1. **System init – theory**
   (a) Read about OpenRC: https://wiki.gentoo.org/wiki/Handbook:AMD64/Working/Initscripts .
   (b) The syntax of '`/etc/inittab`' is quite simple: https://manpages.debian.org/stretch/sysvinit-core/inittab.5.en.html
   (c) Read about BSD daemon management: https://www.freebsd.org/cgi/man.cgi?query=rc&apropos=0&sektion=8&manpath=FreeBSD+12.0-RELEASE+and+Ports&arch=default&format=html .
   (d) ..and the BSD '`/etc/rc.conf`' file: https://www.freebsd.org/cgi/man.cgi?query=rc.conf&sektion=5&apropos=0&manpath=FreeBSD+12.0-RELEASE+and+Ports .
   (e) What the *Init Freedeom* initiative aims at? Read: https://www.devuan.org/os/init-freedom.html .
   (f) Try to find other init systems for Linux/Unix systems.
   (g) If unsure why systemd is evil visit: https://nosystemd.org/ and https://suckless.org/sucks/systemd/ .

2. **System init – practice**
   (a) Presentations provided by the lecturer for the following systems:
      i. CentOS 6 (sysvinit),
      ii. Gentoo Linux (openrc),
      iii. Arch Linux (systemd),
      iv. FreeBSD.

3. **Systemd**
   (a) List unit files:
   `$ ls /usr/lib/systemd/system`
   (b) Display a service file for the sshd daemon:
   `$ cat /usr/lib/systemd/system/sshd.service`
   Is it running?
   `$ systemctl status sshd`
   (c) List a unit file status list:
   `$ systemctl list-unit-files -all`
   (d) Display `journald` log:
   `$ journalctl`
   Well, honestly, `journald` puts all entries unfiltered to a single, binary, local file. Yes, it must be a large single file; inefficient parsing – who cares? Yes, it may contain sensitive data and is readable by all users. Yes, all entries are stored only locally and in case of successful attack can be easily wiped out. Yes, its size is limited but we cannot decide

which entries are very frequent but unimportant and should not be stored. Yes, there is no policy for storing critical entries longer than other ones. A backup copy of old important entries – what for? Yes, binary files may easily get corrupted/unreadable during system crash. Yes, it requires a dedicated tool for reading. No, we have to use it. Yes, it is typical systemd design example! ;-)

4. **Cron daemon**

   (a) Display the crontab files:
   `$ cat /etc/cron.d/*`

   (b) Take a look at cron-related documentation:
   `$ man cron`
   `$ man 5 crontab`
   `$ man 1 crontab`

   (c) Are there any tasks scheduled to be run hourly, daily or weekly? How about the '`ssh`' server?

5. **Syslog-ng**

   (a) Examine your syslog configuration:
   `$ less /etc/syslog-ng/syslog-ng.conf`

   (b) Send a message to syslog:
   `$ logger "some message"`
   You syslog daemon is configured for displaying all log messages on `tty12` so check it by pressing `<Ctrl><Alt><F12>`.

6. **Linux kernel and modules**

   (a) Display kernel buffer ring:
   `$ dmesg | less`

   (b) List all available kernel modules:
   `$ find /lib/modules/`uname -r`/kernel/ -name "*.ko.zst"`

   (c) List all loaded kernel modules:
   `$ lsmod`

   (d) What parameters can be set for the '`thinkpad_acpi`' module?
   `$ modinfo thinkpad_acpi`

7. **Homework**

   (a) Install Unix or Linux. Before proceeding it is highly recommended that you disable *UEFI* or at least *UEFI Secure Boot*. The following systems/distros may be worth trying:

      i. **Gentoo**. Great documentation. You'll learn the most about Unix, Linux and BSD during system installation. OpenRC subsystem. A rolling release with BSD-like organized software (*portage*). Every task can be completed manually (the documentation is really perfect!) – even compiling the kernel. Although extremely flexible this distro installation and upgrades are very time-consuming. For this reason it is not recommended for lightweight workstations.

      ii. **CentOS 6** (6! not 7!). Pure SysV enterprise LAMP (Linux+Apache+MySQL+PHP) platform. Fast, easy installation. The system and most critical services work out-of-the-box. Default configuration is relatively functional, stable and secure. Rather heavy distro suitable for server use, not recommended for workstations. Use documentation for RedHat Entrerprise Linux (it perfectly suits). Nice distro for getting familiar with AT&T commercial, enterprice Unices at no cost.

      iii. **Devuan**. Systemd-free Debian clone. A solid and extremely stable, secure and standard-compliant distro. Although stable and secure the software may be a little bit obsolete.

iv. **Ubuntu**. A Debian clone intended for workstation use. Simple and fast installation. It works out-of-the-box and looks nice. A systemd, slightly automagical distro for those who need Linux workstation and are not interested how and why it works. Numerous clones with other default desktops do exist.

v. **Arch Linux**. Lightweight, KISS, rolling-release distro intended for workstation use. Although requires some knowledge and more time spent on installation and configuration than Ubuntu it offers much more flexibility and explicitness. It uses systemd but there are numerous systemd-free clones including Artix, Hyperbola or Parabola.

vi. **Void Linux**. Minimalistic, extremely lightweight and simple rolling-release distro. Services managed by *runit*. Some administrators find it a tempting alternative to (getting more and more complex) Arch Linux. Due to limited documentation Arch Linux wiki may be useful in many cases.

vii. **Alpine Linux**. Minimalistic, lightweight distro with security in mind. It uses *musl* instead of *glibc*. Services managed by OpenRC. Frequently used in docker containers due to simplicity, security and really small size (image size approx. 5MB).

viii. **FreeBSD**. The most popular and general-purpose among all open BSD Unices. It provides Linux binary emulation mode. BSDs are really simply but well... a little bit strange at first glance. Some experience with Gentoo Linux may help switching to BSDs. Note that BSD community don't like lamers! Never ask questions before reading the documentation!