Network Administration/System Administration Homework #5

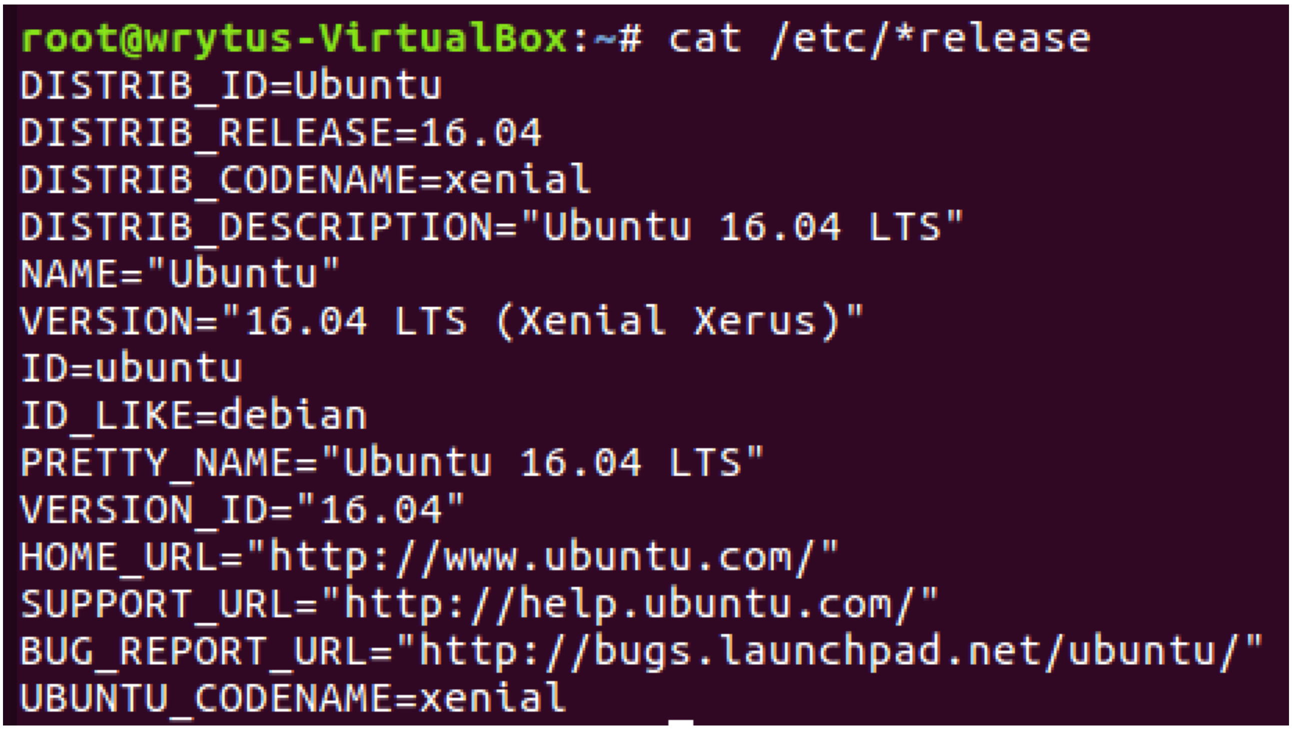
System Administration 2

Professor: Hsin-Mu Tsai

b03502040 劉君猷

1 System Log

Name="Ubuntu" , Version="16.04 LTS"



```
root@wrytus-VirtualBox:~# cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04 LTS"
NAME="Ubuntu"
VERSION="16.04 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
UBUNTU_CODENAME=xenial
```

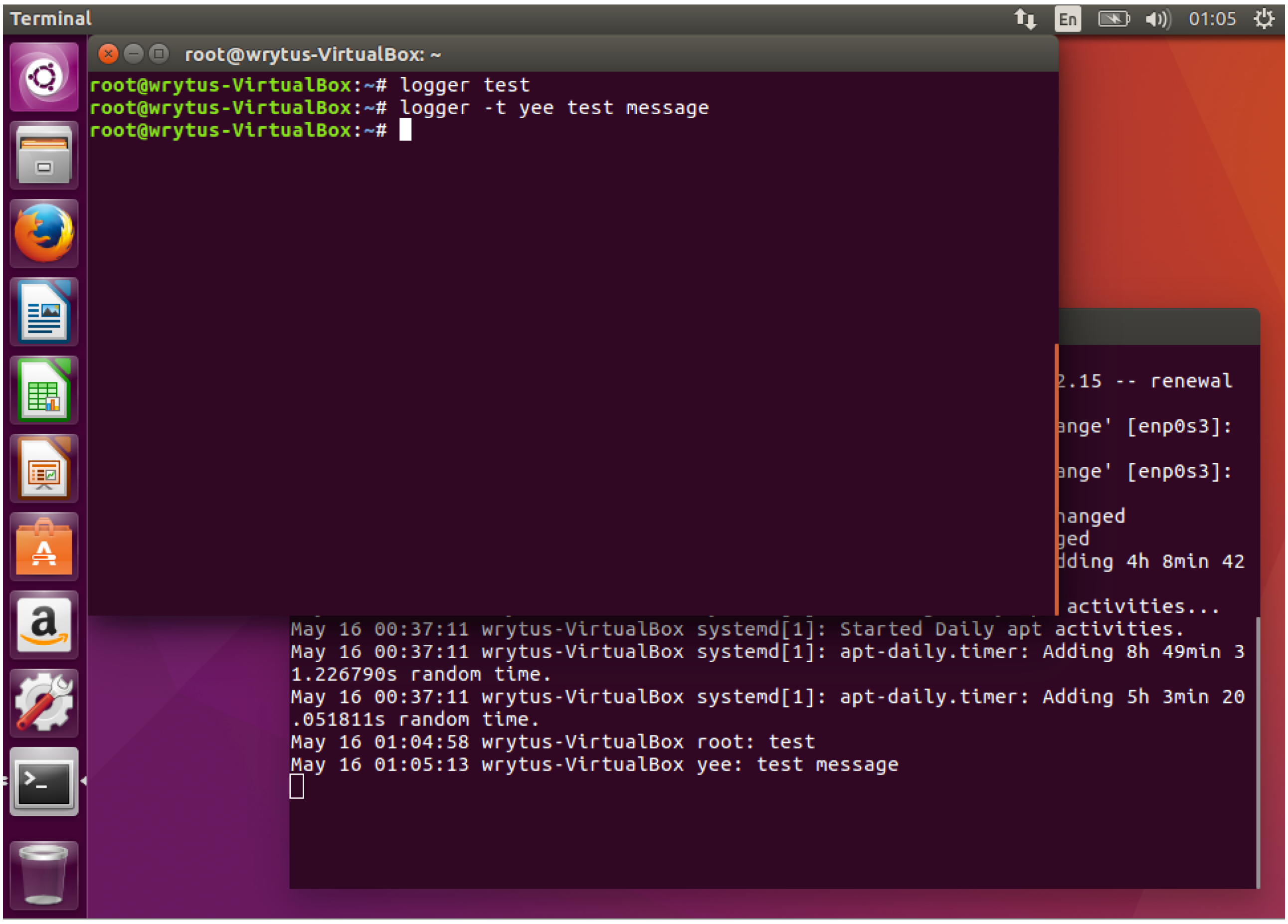
REFERENCE:
(1) [http://whatsmyos.com]

1.1

1.
The process is called "rsyslogd". It belongs to the package named "rsyslog". I find this answer from the reference below (the official ubuntu website) as well as trying it on my distribution using `apt-cache search`.

REFERENCE:
(1) [http://www.gnu.org/software/libc/manual/html_node/Overview-of-Syslog.html]
(2) [http://manpages.ubuntu.com/manpages/xenial/man8/syslogd.8.html]
(3) [http://manpages.ubuntu.com/manpages/xenial/man8/rsyslogd.8.html]
(4) [http://man7.org/linux/man-pages/man8/rsyslogd.8.html]

2.
I use `logger (-t [tag]) [message]` to write system log into "/var/log/syslog", which is a text file. Simultaneously, I run `tail -f /var/log/syslog` to see what I wrote in it, which displayed as "[date] [time] [host] [tag]: [message]"



```
root@wrytus-VirtualBox:~# logger test
root@wrytus-VirtualBox:~# logger -t yee test message
root@wrytus-VirtualBox:~# 
```

```
2.15 -- renewal
ange' [enp0s3]:
ange' [enp0s3]:
hanged
ged
dding 4h 8min 42
 activities...
May 16 00:37:11 wrytus-VirtualBox systemd[1]: Started Daily apt activities.
May 16 00:37:11 wrytus-VirtualBox systemd[1]: apt-daily.timer: Adding 8h 49min 3
1.226790s random time.
May 16 00:37:11 wrytus-VirtualBox systemd[1]: apt-daily.timer: Adding 5h 3min 20
.051811s random time.
May 16 01:04:58 wrytus-VirtualBox root: test
May 16 01:05:13 wrytus-VirtualBox yee: test message
```

REFERENCE:
(1) [http://man7.org/linux/man-pages/man1/logger.1.html]
(2) [https://blog.longwin.com.tw/2011/11/linux-data-syslog-logger-2011/]

3.
No. `logger -p mail.err -t sendmail msg1` and `logger -p user.emerg -t ta217 msg2` store in "/var/log/syslog" with their own tag, which follows -t option. Whereas `logger -p auth.info -t sshd[8352] msg2` store in "/var/log/auth.log".

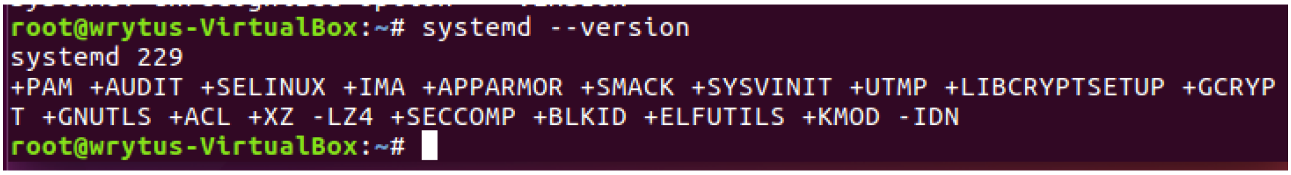
No. We cannot discriminate whether a log is written by a user or system. But we can config the file "/etc/rsyslog.conf"and add some rules in it to make log system more trusted.

REFERENCE:

(1) [http://man7.org/linux/man-pages/man5/rsyslog.conf.5.html]

1.2

1.



```
root@wrytus-VirtualBox:~# systemd --version
systemd 229
+PAM +AUDIT +SELINUX +IMA +APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYP
T +GNUTLS +ACL +XZ -LZ4 +SECCOMP +BLKID +ELFUTILS +KMOD -IDN
root@wrytus-VirtualBox:~# 
```

REFERENCE:

(1) [https://www.freedesktop.org/software/systemd/man/systemd.html]

2.

Not persistent across reboot, which is volatile now.

`mkdir -p /var/log/journal`

`systemd-tmpfiles --create --prefix /var/log/journal`

`systemctl restart systemd-journald`

REFERENCE:

(1) [http://unix.stackexchange.com/questions/191313/why-is-my-systemd-journal-not-persistent-across-reboots]

(2) [https://www.freedesktop.org/software/systemd/man/systemd-journald.service.html]

(3) [http://unix.stackexchange.com/questions/159221/how-display-log-messages-from-previous-boots-under-centos-7]

3.

`journalctl -k -b -1`

REFERENCE:

(1) [http://unix.stackexchange.com/questions/159221/how-display-log-messages-from-previous-boots-under-centos-7]

(2) [https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs]

(3) [https://doc.opensuse.org/documentation/leap/reference/html/book.opensuse.reference/cha.journalctl.html]

4.

`journalctl _COMM=sshd`

REFERENCE:

(1) [http://serverfault.com/questions/465833/where-is-the-sshd-log-file-on-red-hat-linux-stored]

5.

`journalctl _UID=$(id -u dbus) _UID=$(id -u $(whoami))`

REFERENCE:

(1) [https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs]

(2) [http://askubuntu.com/questions/468236/how-can-i-find-my-user-id-uid-from-terminal]

(3) [http://askubuntu.com/questions/333718/how-can-i-find-out-my-user-name]

6.

`journalctl _EXE=/usr/bin/sudo`

REFERENCE:

(1) [https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs]

(2) [https://www.freedesktop.org/software/systemd/man/journalctl.html]

2 Network Log

Add these two rules in the OUTPUT chain of filter table.
`iptables -I OUTPUT -p tcp -j LOG --log-prefix "IPTABLES: "`
`iptables -I OUTPUT -p udp -j LOG --log-prefix "IPTABLES: "`

Then we can use the command below to get all the traffic with tcp/udp protocol routed outward by the CSIE server.
`cat /var/log/syslog | grep "IPTABLES: "`

According to the log format of "DST", "SRC", "DPT" and "SPT", we can always overlook the destination ip, source ip, destination port as well as source port respectively. Moreover, by reported from C&INC with the victim ip, we can find the exact user who attacked other machines on the Internet or downloaded too many papers.

REFERENCE:

(1) [https://gigenchang.wordpress.com/2014/04/19/10分鐘學會iptables/]

(2) [http://linux.vbird.org/linux_server/0250simple_firewall.php#netfilter]

(3) [https://en.wikibooks.org/wiki/Communication_Networks/IP_Tables]

(4) [http://www.thegeekstuff.com/2012/08/iptables-log-packets/]

(5) [http://www.linuxquestions.org/questions/linux-networking-3/netfilter-iptables-log-file-format-553556/]