



EK

Totally not a hacker Email Twitter Github

Linux-Unix-IT Tips and Tricks #3

Different Linux / Unix / IT tips, notes, howto part 3

Other parts

[Part 1](#) [Part 2](#) [Part 3](#)

Speed up MySQL Import

```
mysql -u someuser -p SET AUTOCOMMIT=0; SET UNIQUE_CHECKS=0; SET FOREIGN  
source dump.sql;SET FOREIGN_KEY_CHECKS=1; UNIQUE_CHECKS=1; COMMIT;
```

Coreutils List

```
curl 'http://www.gnu.org/software/coreutils/manual/coreutils.html' 2>/d
```

List all process swap space usage

```
for file in /proc/*/status ; do awk '/VmSwap|Name/{printf $2 " " $3}END
```

CONTENTS

[Other parts](#)[Speed up MySQL Import](#)[Coreutils List](#)[List all process swap space usage](#)[Delete millions files from dir](#)[Nice Diff](#)[Run jobs with parallel](#)[Awk PS SUM](#)[Show ext4 fragmentation %](#)[Statistic of system resource](#)[Tcpdump with SSH stream](#)[Linux Namespaces](#)[Show daemon list need to restart after update](#)[Increases TCPdump buffer](#)[Get Firefox bookmarks](#)

Delete millions files from dir

```
# rm is fucked, this is ok =)
perl -e 'chdir "/tmp/1" or die; opendir D, "."; while ($n = readdir D)
```

Nice Diff

```
diff --side-by-side fileA.txt fileB.txt | pager
```

Run jobs with parallel

```
# apt-get install parallel
ls *.png | parallel -j4 convert {} {}.jpg
```

Awk PS SUM

```
ps alx | tail -n +2 | awk 'BEGIN{rss=0; vsz=0} {rss += $7; vsz+=$8} END
```

Show ext4 fragmentation %

```
# be carefull!!
for D in $( mount | awk '$5~/ext4/ { print $1 }' ); do sudo fsck.ext4 -
```

SSL certs info

Reset root password on
RHEL7\CentOS7

Blacklisting firewire in Linux

Install Ubuntu OpenStack

Vagrant WinXP

Simple Cut Video in linux

How to clean TMP dir on
boot

The port scan attack detector
- PSAD

SNMPTrap using

Remove Postfix Resiver
Header

SSH key login only for one
user

Revert Firefox to init state

Limit MySQL and MongoDB
mem usage with Cgroups

Strace using

Linux System Errors Types

Auditd

```
non-contiguous is a % of fragmentation
```

```
e4defrag /  
e4defrag -c /
```

```
# fragmentation for file  
filefrag -v /PATH/TO/FILE
```

Statistic of system resource

```
# apt-get install dstat  
dstat -c --top-cpu -d --top-bio --top-latency
```

Tcpdump with SSH stream

```
# stream through SSH the tcpdump output and analyze it locally with Wireshark  
mkfifo /tmp/wshark  
ssh root@ip "tcpdump -s 0 -U -n -w - -i eth0 not port 22" > /tmp/wshark  
wireshark -k -i /tmp/wshark
```

Linux Namespaces

Starting from kernel 2.6.24, Linux supports 6 different types of namespaces

CLONE_NEWIPC: IPC Namespaces: SystemV IPC and POSIX Message Queues can
CLONE_NEWPID: PID Namespaces: PIDs are isolated, meaning that a virtual
CLONE_NEWNET: Network Namespaces: Networking (/proc/net, IPs, interface
CLONE_NEWNS: Mount Namespaces. We have the ability to isolate mount poi

MySQL version from an FRM file

Check if a library is installed

FS in File

Encrypt Tar with
OpenSSL\GPG

Split big archive

Installed pkgs size

Compare 2 directory

WGet ALL site

Mount with SSH

Boot in DOS

Remove all tables from
MySQL DB

Resize jpg for web

Postfix redirect outbound
mail

RM: Argument list too long

Rootkits check

Restore deleted files

Flush linux disk cache

```
CLONE_NEWUTS: UTS Namespaces. This namespaces primary purpose is to iso  
CLONE_NEWUSER: User Namespaces. Here, user and group IDs are different
```

Show daemon list need to restart after update

```
sudo lsof / | grep DEL | cut -f1 -d' ' | sort -u
```

Increases TCPdump buffer

```
tcpdump -l -B 10000 host example.com
```

Get Firefox bookmarks

```
sqlite3 ~/.mozilla/firefox/*.[dD]efault/places.sqlite "SELECT strftime(
```

SSL certs info

```
# show expire date of cert  
openssl x509 -enddate -noout -in certnew.cer  
# show all info of cert  
openssl x509 -text -noout -in certnew.cer  
# check that secret key (privkey.pem) is valid  
openssl rsa -noout -text -in privkey.pem
```

Firewall-cmd open http port
80

Auditd

Create dark directory

File attributes Linux-Unix

Iptables to limit connections

Reboot linux with kernel
panic

Reset root password on RHEL7\CentOS7

```
grub linux16 to the end of the line add "rd.break console=tty1"
ctrl+x
switch_root:/# mount -o remount,rw /sysroot
switch_root:/# chroot /sysroot
sh-4.2# passwd root
sh-4.2# touch /.autorelabel
exit
```

Blacklisting firewire in Linux

```
find /lib/modules/`uname -r` -name *firewire*
modinfo snd-firewire-lib
modinfo firewire-core
echo "blacklist firewire-core" > /etc/modprobe.d/blacklist-firewire.conf
modprobe --showconfig | grep blacklist #show blacklist modules
modprobe --showconfig | grep "^install" | grep "/bin"
```

Install Ubuntu OpenStack

```
sudo apt-add-repository -y ppa:cloud-installer/stable
sudo apt-get update
sudo apt-get install -y openstack
sudo openstack-install
```

Vagrant WinXP

```
# https://www.bram.us/2014/09/24/modern-ie-vagrant-boxes/
# http://aka.ms/vagrant-xp-ie6
vagrant box add winxp6 http://aka.ms/vagrant-xp-ie6
vagrant init winxp6
vagrant up
```

Simple Cut Video in linux

```
# cut video from 00:02:52 to 00:03:45
ffmpeg -i original.mp4 -ss 00:02:52 -t 00:03:45 -async 1 -strict -2 cut
```

How to clean TMP dir on boot

```
/etc/default/rcS
#TMPTIME=0
```

The port scan attack detector - PSAD

```
# http://cipherdyne.org/psad/
apt-get install psad

/etc/syslog.conf
kern.info | /var/lib/psad/psadfifo

/etc/init.d/syslogd restart
/etc/init.d/klogd

/etc/psad/psad.conf
```

```
/etc/init.d/psad restart

iptables -A INPUT -j LOG
iptables -A FORWARD -j LOG

view port scan report
psad -S
```

SNMPTrap using

```
/etc/default/snmpd
TRAPDRUN=yes

/etc/snmp/snmptrapd.conf
authCommunity log public

snmptrap -v 1 -c public 127.0.0.1 .1.3.6.1 localhost 6 17 '' .1.3.6.1 s

/var/log/syslog
Jun 23 12:14:47 linux snmptrapd[14221]: 2015-06-23 12:14:47 linux [127.

# tcpdump snmptraps
tcpdump -i eth1 -w test.log "udp and (src port 161 or 162)"
tcpdump -w troubleshoot.pcap -vv -A -T snmp "(dst port 162) or (src port
```

Remove Postfix Resiver Header

```
# add to /etc/postfix/header_checks
/^Received:.*with ESMTP/          IGNORE

# add to /etc/postfix/main.cf
```

```
mime_header_checks = regexp:/etc/postfix/header_checks header_checks =  
postmap /etc/postfix/header_checks  
postfix reload
```

SSH key login only for one user

```
# add to /etc/ssh/sshd_config  
Match user stew  
PasswordAuthentication no  
  
or  
  
Match group dumbusers  
PasswordAuthentication no
```

Revert Firefox to init state

```
open about:support and press <Refresh Firefox>
```

Limit MySQL and MongoDB mem usage with Cgroups

```
cgcreate -g memory:DBLimitedGroup  
echo 16G > /sys/fs/cgroup/memory/DBLimitedGroup/memory.limit_in_bytes  
sync; echo 3 > /proc/sys/vm/drop_caches  
cgclassify -g memory:DBLimitedGroup `pidof mongod`  
cgclassify -g memory:DBLimitedGroup `pidof mysqld_safe`
```

Strace using


```
# file activity common syscalls:
access ()
close (close file handle)
fchmod (change file permissions)
fchown (change file ownership)
fstat (retrieve details)
lseek (move through file)
open (open file for reading/writing)
read (read a piece of data)
statfs (retrieve file system related details)

$ strace php 2>&1 | grep php.ini
$ strace -e open php 2>&1 | grep php.ini
$ strace -e open,access 2>&1 | grep your-filename
$ strace -p PID
# strace -c -p PID

# the network common syscalls:
bind - link the process to a network port
listen - allow to receive incoming connections
socket - open a local or network socket
setsockopt - define options for an active socket

$ strace -e poll,select,connect,recvfrom,sendto nc www.news.com 80
$ strace -e trace=network

# memory common syscalls:
mmap
munmap

$ strace -e trace=memory

# useful options and examples:
-c - See what time is spend and where (combine with -S for sorting)
-f - Track process including forked child processes
-o my-process-trace.txt - Log strace output to a file
-p 1234 - Track a process by PID
```

```
-P /tmp - Track a process when interacting with a path
-T - Display syscall duration in the output

# track by specific syscall group:
-e trace=ipc - Track communication between processes (IPC)
-e trace=memory - Track memory syscalls
-e trace=network - Track network syscalls
-e trace=process - Track process calls (like fork, exec)
-e trace=signal - Track process signal handling (like HUP, exit)
-e trace=file - Track file related syscalls

# trace multiple syscalls:
strace -e open,close
```

Linux System Errors Types

```
cat /usr/include/asm-generic/errno.h |grep "#"
```

Auditd

```
# create rule: open
auditctl -a always,exit -F arch=b64 -F pid=8175 -S open -k cups-open-fi
ausearch -k cups-open-files

# check which process is modifying a certain directory or file
auditctl -w /path/to/directory -p war
ausearch -f /path/to/directory
```

MySQL version from an FRM file

```
# MySQL version 5.5.32
$ hexdump -s 0x33 -n 2 -v -d 55_test.frm
0000033 50532
# MySQL version 5.1.73
$ hexdump -s 0x33 -n 2 -v -d 51_test.frm
0000033 50173
```

Check if a library is installed

```
$ ldconfig -p | grep libjpeg
```

FS in File

```
$ dd if=/dev/zero of=/tmp/disk-image count=20480
$ mkfs -t ext4 -q /tmp/disk-image
$ mkdir /virtual-fs
$ mount -o loop=/dev/loop0 /tmp/disk-image /virtual-fs
# add to /etc/fstab
/tmp/disk-image /virtual-fs ext4 rw,loop 0 0
```

Encrypt Tar with OpenSSL\GPG

```
# encrypt
$ gpg -c test.tar
$ tar -czv stuff|openssl des3 -salt -k secretpassword | dd of=stuff.des
# decrypt
$ gpg test.tar.gpg
$ dd if=stuff.des3 |openssl des3 -d -k secretpassword|tar xz
```

Split big archive

```
split -b 700m archive.tar part  
cat part* > archive.tar
```

Installed pkgs size

freebsd

```
pkg_info -as | perl -pe '$/=')"; s/\n*Information for (.*)?:[\n\s]*Pack  
  
# ubuntu  
dpkg-query -W --showformat='${Installed-Size} ${Package}\n' | sort -n
```

Compare 2 directory

```
diff -qr dir1 dir2
```

WGet ALL site

```
wget -m -k -nv -np -p --user-agent="Mozilla/5.0 (compatible; Konqueror/
```

Mount with SSH

```
apt-get install sshfs
mkdir ~/music
sshfs <remote_ip>:/music ~/music/
fusermount -u ~/music/
```

Boot in DOS

```
apt-get install syslinux
cp /usr/share/syslinux/memdisk /boot
wget -O /boot/Dos6.22.img http://www.allbootdisks.com/downloads/Disks/
# add to /boot/grub/menu.lst
title MSDOS
root(hd0,0) # Номер диска изменить на нужный
kernel /memdisk
initrd /Dos6.22.img
```

Remove all tables from MySQL DB

```
mysql -u root -ppassword -Ddb-name -e 'show tables;' | grep -v 'Tables_'
for table in `cat /tmp/tables_list`; do mysql -u root -ppassword -Ddb-n
```

Resize jpg for web

```
for i in *.jpg; do convert -resize 640x480 -quality 85 $i small-$i.jpg;
```

Postfix redirect outbound mail

```
# all outbound mail redirect to local <username>
$ postconf -e user_relay=username
$ postmap /etc/postfix/transport
$ postconf -e transport_maps=hash:/etc/postfix/transport
# add to /etc/postfix/transport
localhost :
* local:username
```

RM: Argument list too long

```
find | xargs --no-run-if-empty -n 500 rm -f
```

Rootkits check

```
apt-get install rkhunter
rkhunter --update
rkhunter --check
```

Restore deleted files

```
lsof | grep storage.db
memcached 22073 memcachedb 15u      REG           8,1 8809027993
/proc/22073/fd
find /path/memcachedb/ -inum 14221332 -exec cp {} /var/tmp/storage.db \
```

Flush linux disk cache

```
sudo sh -c 'sync; echo 3 > /proc/sys/vm/drop_caches'
free && sync && echo 3 > /proc/sys/vm/drop_caches && free
```

Firewall-cmd open http port 80

```
# open
$ firewall-cmd --zone=public --add-port=80/tcp --permanent
$ firewall-cmd --reload
$ iptables-save | grep 80

# to block
$ firewall-cmd --zone=public --remove-port=80/tcp --permanent
$ firewall-cmd --reload
```

Auditd

```
# install
$ $ sudo yum list audit audit-libs

# /etc/audit/auditd.conf
max_log_file = 30
max_log_file_action = ROTATE
sudo service auditd restart

# Generating Audit Reports
$ sudo aureport -x --summary
$ sudo aureport --failed
$ sudo aureport -f -i
```

```

# view the current set of audit rules
$ sudo auditctl -l
# current status of the audit system
$ sudo auditctl -s
# add rule fo file
$ auditctl -w path_to_file -p permissions -k key_name
$ sudo auditctl -w /etc/hosts -p wa -k hosts_file_change

# /etc/audit/rules.d/audit.rules
-w /etc/hosts -p wa -k hosts_file_change
$ sudo auditctl -l
# add rule for dir
$ sudo auditctl -w /etc/sysconfig/ -p rwa -k configaccess
$ sudo ausearch -k configaccess

# system call rules
$ auditctl -a action,filter -S system_call -F field=value -k key_name
$ sudo auditctl -a always,exit -F arch=b64 -F "auid>=1000" -S rename -S
$ sudo auditctl -a always,exit -F arch=b64 -F auid=1001 -S open -k user

# removing audit rules
$ sudo auditctl -W /etc/passwd -p wa -k passwdaccess

```

Create dark directory

```

# read file only if you know it name
mkdir darkroom
chmod a-r+x darkroom

```

File attributes Linux-Unix


```
# linux
chattr +i vip_file
lsattr vip_file
chattr +a vip_file

# freebsd
chflags schg vip_file
chflags noschg vip_file
ls -lo vip_file

# freebsd flags
acrh
opaque
nodump
sappnd
schg
sunlnk
uappnd
uchg
uunlnk
```

Iptables to limit connections

```
IPT=/sbin/iptables
# Interface id
INET_IF=eth0
# Http Port
HTTP_PORT=80
# Max connection in seconds
SECONDS=100
# Max connections per IP
BLOCKCOUNT=10
# Default action can be DROP or REJECT
DACTION="DROP"
```

```
$IPT -I INPUT -p tcp --dport ${HTTP_PORT} -i ${INET_IF} -m state --stat  
$IPT -I INPUT -p tcp --dport ${HTTP_PORT} -i ${INET_IF} -m state --stat  
  
# for test we can use  
ab -c 100 -n 1000 http://ip.ad.dr.es/  
iptables -vL
```

Reboot linux with kernel panic

```
# /etc/sysctl.conf  
kernel.panic = 15  
$ sysctl -p
```

Linux-Unix-IT Tips and Tricks #3 was published on July 01, 2015 and last modified on July 01, 2015.

0 Comments

EK BLOG

 Login ▾

 Recommend

 Tweet

 Share

Sort by Best ▾



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 



Name

Be the first to comment.

 Subscribe

 Add Disqus

 Disqus' Privacy Policy

DISQUS

YOU MIGHT ALSO ENJOY

(VIEW ALL POSTS)

- [Move from HDD to SSD with ArchLinux](#)
- [Linux SysAdm/DevOps Interview Questions](#)
- [ArchLinux Installation Guide](#)

