

Command Line Kung Fu Commands Cheat Sheet

by karaliking

Disclaimer & Notes

I am not the author of this content. I simply, or not so simply, pulled out the commands and paraphrased from the discussions of the authors of Command Line Kung Fu. Every episode should be linked.

In some cases, I may have updated their commands if I noticed they were outdated.

I plan on continuing to add all episodes. Let me know what my errors are.

C:\> Windows

PS C:\> Windows Powershell

Unix

\$ OS X

```
Episode
            # dos2unix file.txt
            # sed 's/\r$//' file.txt >newfile.txt
Convert
Dos To
UNIX
Episode
            C:\> netsh firewall show portopening
                                                                         C:\> netsh firewall show allowedprogram
            show all ports allowed
                                                                          show all programs allowed
#2
Looking at C:\> netsh firewall show config
                                                                         # for type in nat mangle filter raw; do ipt
            show all config options
                                                                          list all iptables rules in all chains
the Config
of Built-In
Firewall
Episode
            C:\> for /L %i in (1,0,2) do @dir /b /a | find /c /v "" & ping -n 6 127.0.0.1>nul
#3
Watching
            # watch -n 5 'ls | wc -l'
the File
Count in a
Directory
Episode
            C:\> for /r c:\ %i in (*) do @echo %~zi, %i
            output to csv and sort in spreadsheet
#4
                                                                         # find / -type f -exec wc -c {} \; | sort -
Listing
            # du | sort -nr | head -100
            show top 100 largest directories in descending order
                                                                          show top 100 largest files in descending order
Files and
Their
```

```
Sizes
Episode
            C:\> FOR /F "tokens=1-5" %a in (lookups.txt) do @(@FOR /F "tokens=1-4 delims=." %i in ("%a") do @e
            \# \text{ sed 's/([0-9]*\)..([0-9]*\)..([0-9]*\)..in-addr.arpa domain name pointer\(.*\)\./\
Simple
            lookups.txt format: 208.251.16.10.in-addr.arpa domain name pointer server2.srv.mydomain.net.
Text
Manipu-
lation -
Reverse
DNS
Records
Episode
            C:\> FOR /L %i in (1,1,255) do @ping -n 1 -w 100 10.10.%i | find "Reply"
#6
Command-
           # for i in `seq 1 255`; do ping -c 1 -w 1 10.10.10.$i | tr \\n ' ' | awk '/1 received/ {print $2}'
Line Ping
Sweeper
Episode
            C:\> shutdown /a
                                                                         C:\> shutdown /r /t [#_seconds]
            abort shutdown
                                                                          to try delaying shutdown
#7
Aborting a
            # shutdown -c
                                                                         # shutdown -r +<#>
            cancel scheduled shutdown
                                                                          reboot in # minute(s)
System
Shutdown
Episode
            C:\> netstat -s
                                                                         C:\> netstat -s -p tcp
            all protocols
                                                                         all tcp
#8
Netstat
            # netstat -s
                                                                         # netstat -s | awk '/:/ { p = $1 }; (p \sim /^
            all protocols
                                                                          all tcp (works for OS X too)
Protocol
Stats
            C:\> find /v /n "" <file> | findstr /b /L [<#>]
                                                                         C:\> for /F "delims=[] tokens=2" %i in (tmc
Episode
            will prepend line numbers to output
                                                                         used to remove line numbers in output (save output of
#9
            # awk 'FNR = <#>' <file>
                                                                         # head -<#> <file> | tail -1
Display
                                                                          alternative command
the Nth
Line
Episode
            C:\> findstr /s /d:<dir>s /m <string> *.<filetype>
                                                                         C:\> findstr /s /m <string> <dir>*<filetype
            dir=absolute|relative, filetype=file extension
                                                                          alternative format
#10
            # find <dir> -type f -exec grep -l <string> {} +
Display
                                                                         # find <dir> -type f -print0 | xargs -0 gre
            more flexible, allows for multiple -exec predicates
                                                                         alternative safer command (except on Solaris =P)
Filenames
Containing
            # grep -irl <string> <dir>
                                                                         Additional Research Links
            slow for larger searches, easy to remember
                                                                          xargs vs exec uses & xargs vs exec efficiency
String
Within the
File
Episode
            C:\> dir /tc /od
             oldest first (/o-d will show newest first)
#11
Listina
            # ls -li <dir> | sort -n
            relative times from clustered inodes
Files by
Inode as a
Proxy for
Create
Time
Episode
            PS C:\> sls spammer@example.com -list -path qf* | rm -path {$ .Path -replace "\\qf","\[qd]f"}
             Note, this is PowerShell
#12
```

```
Deleting
            C:\> cmd.exe /v:on /c "for /f %i in ('findstr /m spammer@example.com qf*') do @set stuff=%i & del
Related
            # grep -l spammer@example.com gf* | cut -c3- | xargs -I {} rm gf{} df{}
Files
Episode
           DEPRECATED Nessus format, no longer necessary
#13
            C:\> for /F "delims=:| tokens=2" %i in ('findstr CVE-2008-4250 *.nsr') do @echo %i
Find
            # awk -F'|' '/CVE-2008-4250/ {print $1}' | sort -u
             funnel those IP addresses through to Metasploit's msfcli and get shell on all of them
Vulnerable
Systems
In A
Nessus
Export
                                                                           C:\> F7
Episode
            C:\> doskey /history
             up to 50 commands stored by default
                                                                           bring up prompt with history
#14
Command
            # CTRL+r
                                                                           # CTRL+p | CTRL+n
             find & run cmd containing string (ENTER | CTRL+g)
                                                                           previous or next command in history (up & down)
Line
(History)
            # !<string>:p
                                                                           # !<string>
            only display cmd, then !! to run
                                                                           run last cmd that starts with string
Shortcuts
            #!!
                                                                           #!-<#>
             run previous cmd
                                                                           run # previous cmd
            # <cmd> !$
                                                                           # <cmd> !-<#>$
             run a cmd with last argument of prev cmd (ALT+. also works)
                                                                           run a cmd with last argument of # prev cmd
            # <cmd> !*
                                                                           # <cmd> !-<#>*
             run a cmd with all arguments of prev cmd
                                                                           run a cmd with all arguments of # prev cmd
            # ^foo^bar
                                                                           # !:qs/foo/bar/
             run prev cmd replacing 1st instance of foo with bar
                                                                           run prev cmd replacing all instances of foo with bar
            # ^<string>
             run prev cmd removing 1st instance of string
Episode
            C:\> net user <user>
                                                                           C:\> dir /tc "C:\Documents and Settings\"
             last time password was set
                                                                           first logged in (before Vista)
#15.1
New User
            #awk -F: '/^<user>:/ {print $3 * 86400}' /etc/shadow
                                                                          # ls -ltd /home/<user>/.[^.]* | tail -1
            last time password was set (Epoch time)
                                                                           first logged in
Created
When?
Episode
            C:\> cscript c:\windows\system32\eventquery.vbs /L security /FI "id eq 642"
             using "audit account management" event log (XP & 03)
#15.2
New User
            C:\> wevtutil ge security /f:text "/q:*[System[(EventID=4720)]]" | more
             using "audit account management" event log (Vista+)
Created
When?
            # grep <user> /var/log/secure* | tail
             limited history (may be in /var/log/auth.log)
Cont.
            C:\> wmic gfe where hotfixid="KB958644" list full
                                                                           # rpm -qa --qf "%-30{NAME} %-15{VERSION} %{
Episode
             whether MS08-067 patch was installed and when
                                                                           RHEL report for all packages
#16
Got That
            # apt-show-versions -u
                                                                           $ ls -l com.apple.pkg.update.*
             Debian based (/var/cache/apt/archives may have install dates)
                                                                           OS X packages and timestamps
Patch?
            C:\> for /F %i in (names.txt) do @echo %i & nslookup -norecurse %i [DNSserver] | find "answer" & e
Episode
             names.txt contains names to check, DNSserver is optional chosen DNS server
#17
DNS
            # for i in `cat names.txt`; do host -r $i [nameserver]; done
             names.txt contains names to check, DNSserver is optional chosen DNS server
Cache
Snooping
            # rndc dumpdb -cache
             if you are the server
in a Single
```

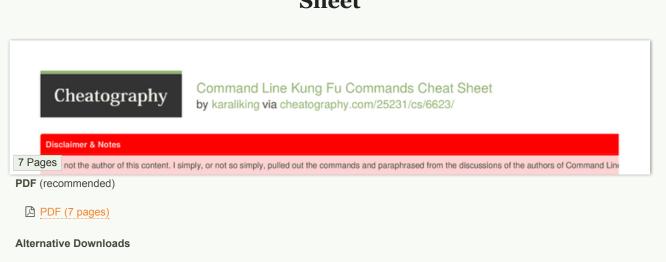
```
Command
            # lsof -a -c named -d cwd
            find the current working directory of the named process
Episode
            C:\> ipconfig /flushdns
                                                                       C:\> ipconfig /displaydns
#18
            # nscd -i hosts
                                                                       # netstat -rCn
            linux flush
                                                                        linux recent communication
Clearing
           $ dscacheutil -flushcache
The
                                                                       $ dscacheutil -cachedump -entries Host
            OS X flush
                                                                        OS X display cache
System
DNS
Lookup
Cache
Episode
            C:\> type nul > my file
                                                                       C:\> copy nul my file
                                                                        shorter command
#19
Clearing
           # cat /dev/null > my file
                                                                       # cp /dev/null my file
                                                                        shorter command
The
Contents
Of A File
Episode
            C:\> for /L %i in (1,0,2) do @(ping -n 1 HostIPaddr > nul || echo ^G) & ping -n 2 127.0.0.1 > nul
            not ^ and G, actually CTRL+g
#20
Ping Beep
           # ping x.x.x.x 2>&1 | awk -F: '/sendto:/ {print $3}' | say
of Death
            $ ping -A 192.168.1.1
```

 ▶ bash
 ▶ commandline
 ▶ command
 ▶ line
 ▶ shell
 ▶ fu
 ▶ cmdline
 ▶ kung
 ▶ kungfu

 ▶ commandlinekungfu

<u>+</u>

Download the Command Line Kung Fu Commands Cheat Sheet







Created By



Metadata

Languages: English

Published: 2nd February, 2016 Last Updated: 12th May, 2016

Rated: 5 out of 5 stars based on 2 ratings

Favourited By

Comments

No comments yet. Add yours below!

Add a Comment



Related Cheat Sheets

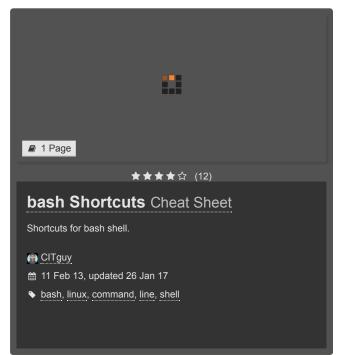




Latest Cheat Sheet



Random Cheat Sheet



About Cheatography

Cheatography is a collection of 6766 cheat sheets and quick references in 25 languages for everything from travel to language!

Behind the Scenes

If you have any problems, or just want to say hi, you can find us right here:

DaveChild

SpaceDuck

Cheatography

Recent Cheat Sheet Activity

Charles Duarte updated UV Cheatsheet.

1 day 7 hours ago

karlaxcr published Old British and Medieval Literature.

3 days 15 hours ago

1 week ago
© 2011 - 2025 Cheatography.com CC License Terms Privacy

■ Latest Cheat Sheets RSS Feed

Tamaranth updated Minecraft Item IDs.