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In some cases, I may have updated their commands if I noticed they were outdated.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

Episodes #1-10

Episode #1
Convert Dos To UNIX

```
# dos2unix file.txt
```

```
# sed 's/\r$//' file.txt >newfile.txt
```

Episode #2
Looking at the Config of Built-In Firewall

```
C:\> netsh firewall show portopening
```
show all ports allowed

```
C:\> netsh firewall show allowedprogram
```
show all programs allowed

```
C:\> netsh firewall show config
```
show all config options

```
# for type in nat mangle filter raw; do iptables -t $type
```
list all iptables rules in all chains

Episode #3
Watching the File Count in a Directory

```
C:\> for /L %i in (1,0,2) do @dir /b /a | find /c /v "" & ping -n 6 127.0.0.1>nul
```

```
# watch -n 5 'ls | wc -l'
```

Episode #4
Listing Files and Their Sizes

```
C:\> for /r c:\ %i in (*) do @echo %~zi, %i
```
output to csv and sort in spreadsheet

```
# du | sort -nr | head -100
```
show top 100 largest directories in descending order

```
# find / -type f -exec wc -c {} \; | sort -nr | head -100
```
show top 100 largest files in descending order

Episodes #1-10 (cont)

Episode #5
Simple Text Manipulation - Reverse DNS Records

```
C:\> FOR /F "tokens=1-5" %a in (lookups.txt) do @(@FOR /F "tokens=1-4 delims=." %i in ("%a") do @echo %l.%k.%j.%i %e)
```

```
# sed 's/\([0-9]*\)\.\([0-9]*\)\.\([0-9]*\)\.\([0-9]*\).in-addr.arpa domain name pointer\(.*\)\./\4.\3.\2.\1\5/' lookups.txt
```

lookups.txt format: 208.251.16.10.in-addr.arpa domain name pointer server2.srv.mydomain.net.

Episode #6
Command-Line Ping Sweeper

```
C:\> FOR /L %i in (1,1,255) do @ping -n 1 -w 100 10.10.10.%i | find "Reply"
```

```
# for i in `seq 1 255`; do ping -c 1 -w 1 10.10.10.$i | tr \\n ' ' | awk '/1 received/ {print $2}'; done
```

Episode #7
Aborting a System Shutdown

```
C:\> shutdown /a
```
abort shutdown

```
# shutdown -c
```
cancel scheduled shutdown

```
C:\> shutdown /r /t [#_seconds]
```
to try delaying shutdown

```
# shutdown -r +<#>
```
reboot in # minute(s)

```
# shutdown -r hh:mm:ss
```
reboot at hh:mm.ss (24 hr clock)

Episode #8
Netstat Protocol Stats

```
C:\> netstat -s
```
all protocols

```
# netstat -s
```
all protocols

```
C:\> netstat -s -p tcp
```
all tcp

```
# netstat -s | awk '/:/ { p = $1 }; (p ~ /^[Tt]cp/) { print }'
```
all tcp (works for OS X too)

Episodes #1-10 (cont)

Episode #9 Display the Nth Line

```
C:\> find /v /n "" <file> | findstr /b /L [<#>]
```
will prepend line numbers to output

```
# awk 'FNR = <#>' <file>
```

```
C:\> for /F "delims=[] tokens=2" %i in (tmp.txt) do
```
used to remove line numbers in output (save output of prev

```
# head -<#> <file> | tail -1
```
alternative command

Episode #10 Display Filenames Containing String Within the File

```
C:\> findstr /s /d:<dir>s /m <string> *.<filetype>
```
dir=absolute|relative, filetype=file extension

```
# find <dir> -type f -exec grep -l <string> {} +
```
more flexible, allows for multiple -exec predicates

```
# grep -irl <string> <dir>
```
slow for larger searches, easy to remember

```
C:\> findstr /s /m <string> <dir>*<filetype>
```
alternative format

```
# find <dir> -type f -print0 | xargs -0 grep -l <st
```
alternative safer command (except on Solaris =P)

Additional Research Links

xargs vs exec uses & xargs vs exec efficiency

Episode #11 Listing Files by Inode as a Proxy for Create Time

```
C:\> dir /tc /od
```
oldest first (/o-d will show newest first)

```
# ls -li <dir> | sort -n
```
relative times from clustered inodes

Episode #12 Deleting Related Files

```
PS C:\> sls spammer@example.com -list -path qf* | rm -path {$_.Path -replace "\\qf","\[qd]f"}
```
Note, this is PowerShell

```
C:\> cmd.exe /v:on /c "for /f %i in ('findstr /m  spammer@example.com qf*') do @set stuff=%i & del qf!stu
```

```
# grep -l spammer@example.com qf* | cut -c3- | xargs -I {} rm qf{} df{}
```

Episodes #1-10 (cont)

Episode #13 Find Vulnerable Systems In A Nessus Export

DEPRECATED Nessus format, no longer necessary

```
C:\> for /F "delims=:| tokens=2" %i in ('findstr CVE-2008-4250 *.nsr') do @echo %i
```

```
# 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

Episode #14 Command Line (History) Shortcuts

```
C:\> doskey /history
```

up to 50 commands stored by default

```
C:\> F7
```

bring up prompt with history

```
# CTRL+r
```

find & run cmd containing string (ENTER | CTRL+g)

```
# CTRL+p | CTRL+n
```

previous or next command in history (up & down)

```
# !<string>:p
```

only display cmd, then !! to run

```
# !<string>
```

run last cmd that starts with string

```
# !!
```

run previous cmd

```
# !-<#>
```

run # previous cmd

```
# <cmd> !$
```

run a cmd with last argument of prev cmd (ALT+. also works)

```
# <cmd> !-<#>$
```

run a cmd with last argument of # prev cmd

```
# <cmd> !*
```

run a cmd with all arguments of prev cmd

```
# <cmd> !-<#>*
```

run a cmd with all arguments of # prev cmd

```
# ^foo^bar
```

run prev cmd replacing 1st instance of foo with bar

```
# !:gs/foo/bar/
```

run prev cmd replacing all instances of foo with bar

```
# ^<string>
```

run prev cmd removing 1st instance of string

Episodes #1-10 (cont)

Episode #15.1 New User Created When?

```
C:\> net user <user>
```
last time password was set

```
#awk -F: '/^<user>:/ {print $3 * 86400}' /etc/shadow
```
last time password was set (Epoch time)

```
C:\> dir /tc "C:\Documents and Settings\"
```
first logged in (before Vista)

```
# ls -ltd /home/<user>/.[^.]* | tail -1
```
first logged in

```
C:\> dir /tc C:\Users\
```
first logged in (Vista+)

Episode #15.2 New User Created When? Cont.

```
C:\> cscript c:\windows\system32\eventquery.vbs /L security /FI "id eq 642"
```
using "audit account management" event log (XP & 03)

```
C:\> wevtutil qe security /f:text "/q:*[System[(EventID=4720)]]" | more
```
using "audit account management" event log (Vista+)

```
# grep <user> /var/log/secure* | tail
```
limited history (may be in /var/log/auth.log)

Episode #16 Got That Patch?

```
C:\> wmic qfe where hotfixid="KB958644" list full
```
whether MS08-067 patch was installed and when

```
# apt-show-versions -u
```
Debian based (/var/cache/apt/archives may have install dates)

```
# rpm -qa --qf "%-30{NAME} %-15{VERSION} %{INSTALLTIME:date}\n"
```
RHEL report for all packages

```
$ ls -l com.apple.pkg.update.*
```
OS X packages and timestamps

Episodes #1-10 (cont)

Episode #17 DNS Cache Snooping in a Single Command

```
C:\> for /F %i in (names.txt) do @echo %i & nslookup -norecurse %i [DNSserver] | find "answer" & echo.
```
names.txt contains names to check, DNSserver is optional chosen DNS server

```
# for i in `cat names.txt`; do host -r $i [nameserver]; done
```
names.txt contains names to check, DNSserver is optional chosen DNS server

```
# rndc dumpdb -cache
```
if you are the server

```
# lsof -a -c named -d cwd
```
find the current working directory of the named process

Episode #18 Clearing The System DNS Lookup Cache

```
C:\> ipconfig /flushdns
```

```
# nscd -i hosts
```
linux flush

```
$ dscacheutil -flushcache
```
OS X flush

```
C:\> ipconfig /displaydns
```

```
# netstat -rCn
```
linux recent communication

```
$ dscacheutil -cachedump -entries Host
```
OS X display cache

Episode #19 Clearing The Contents Of A File

```
C:\> type nul > my_file
```

```
# cat /dev/null > my_file
```

```
C:\> copy nul my_file
```
shorter command

```
# cp /dev/null my_file
```
shorter command

Episodes #1-10 (cont)

Episode #20 Ping Beep of Death

```
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

```
# ping x.x.x.x 2>&1 | awk -F: '/sendto:/ {print $3}' | say
```

```
$ ping -A 192.168.1.1
```

By **karaliking**
cheatography.com/karaliking/

Published 2nd February, 2016.
Last updated 24th April, 2016.