**objdump -D <filename>**

Disassembly the file into readable assembly code

**steghide extract -sf <image>**

**stegseek <img> rockyou.txt**

Finding passphrase for steghide. *Remember to create rockyou.txt first*

**time stegseek --seed**

**binwalk -e <file>**

Decompress a file that may other files.

**tshark -nr <pcappng file> -Y ‘dns’**

-Y ‘dns’ : display packet related to the (DNS) protocol

-nr <pcappng file> : read input file

**awk -e ‘{print $12}’**

Start print from the 12th character from each line of input

**sed -e ‘<s/\..\*//>’**

Discard the part from the first ‘.’ character to the end of line (Done with each line). Basically keep the first part until before ‘.’

**mv ~/.ghidra junk**

Sometimes ghidra freezes. This command will help.

**set $rip=<hex add>**

Kill the command in gdb mode. Effective for avoiding delay

**tar -xvzf <filename>**

Extract tar file

f: this must be the last flag of the command, and the tar **f**ile must be immediately after. It tells tar the name and path of the compressed file.

z: tells tar to decompress the archive using g**z**ip

x: tar can collect files or e**x**tract them. x does the latter.

v: makes tar talk a lot. **V**erbose output shows you all the files being extracted.

**cargo install pwninit**

Install pwninit

**export PATH=”$PATH:<directory>”**

Make a directory used globally

**(gdb) layout asm**

**(gdb) jump \*(main+104)**

Jump to the command from the 104th line of main. *Disassemble <function>* will help find command easier

**pdftotext <FILE>**

To see the text has been redacted in the pdf file

**git log**

See the actions in the folder

**git checkout <commit ID>**

Undo the action

**gnome-software --local-filename <filename.deb>**

Install deb file on ubuntu

**rockyou.txt**

World dictionary passwords (1 mil passwords).

**objdump -x <binary-file>**

Find the entry point (In case *info file* don’t work)

**x32/64dbg (in start menu)**

Debug window.exe file (good for PE32 file). Installing link is in useful link

**Mongodb**

**sudo systemctl start mongod** : Start MongoDB

**sudo systemctl status mongod** : Verify that MongoDB has started successfully.

**sudo systemctl stop mongod** : Stop MongoDB

**Upx -d <binary file>**

Decompressing binary file to debug

**patchelf --set-interpreter /path/to/lib.so.2 ./<exe file>**

Patching the exe file with lib.so.2

**ROPgadget --binary <exe file>**

**objdump -D libc.so.6 | grep \_puts.\*:**

Finding libc\_base address

**objdump -s -j .rodata libc.so.6 | grep -A 1 bin/sh**

Finding /bin/sh

**objdump -D libc.so.6 | grep system.\*:**

Finding system

**apktool d <filename>**

Decompile an apk file. To download apktool, use command “sudo snap install apktool”

**${parameter=<command>}**

Use a normal command. It’s part of shell syntax. Useful for platforms with spell check on.

**java -jar <your ctf file> <your class file>**

Decompile class file with a ctf file (a decompiler). To get a ctf file, visit:<https://www.benf.org/other/cfr/>

**zsteg <png file>**

Detect steganography cipher in png files.

**grep -r 'picoCTF' \***

Search all file and sub-directories contents for ‘picoCTF’ term.

**find <path> -name '<FileName>'**

Find filename in all directories and subdirectories.

**strings -t d disk.flag.img | grep flag.txt**

**ssh-keygen -lf <pub file>**

Viewing details of a pub file that contains a publica key.

**aircrack-ng -w rockyou.txt -b <BSSID> <pcap>**

Finding password from rockyou.txt to crack WPA/WPA2 handshake data in pcap file. BSSID is the MAC address of the access point (usually the destination address).

**flask-unsign --unsign --cookie <cookie> --wordlist wordlist.txt**

Try every password from wordlist.txt to decode flask session cookie.

**strings -a -t x** <filename>

-a: Print all strings without skipping any session

-t x: Print the offset of the string in hex (x)

**xxd -s 0x200400 -l 200** <filename>

-s <offset>: starting off set of hex dump

-l 200: specifying length of the dump to 200

**pngcheck -v <png file>**

Determine error in png file

**john <jwt file> --format=HMAC-SHA256 --wordlist=rockyou.txt**

Cracking password for signature from jwt file using rockyou.txt as password file. To download, go here: <https://github.com/openwall/john>