Reverse challenges notes :

linux :

file command :
not striped --> contains symbol names from the code , makes reverse much easier

Hex editor

strings command

rabin2 (radar)
command # rabin2 -zzq ./file

strace
ignore the first few lines (executable setup stuff)

ltrace
traces library calls like string compare

gdb
use extension pwndbg to make it look better
break *main
r
si: next step
ni: next instruction

ghidra

radar2
command : r2 ./file
aaaa --> analyze
s sym.main --> seek to main function
V --> enter visual mode

ldd
tells which linux dynamic libraries it requires

ls -l fd

netstat -a -c
-a --> show both listening and non listening sockets

Notes :

Reverse engineering

https://www.youtube.com/watch?v=28JHPOUZvDw

reverse tools
ida pro
gdb
radar2
https://onlinedisassembler.com/odaweb/oF1mMXDi

Windows registry :
Regedit tool

Static analysis

- Get File type and info
  - File (in linux)
  - Exeinfo pe (in windows)
  - Read the file header in any hex editor (check the most common formats)

- Tools to calculate the hash
  - Md5sum
  - Md5deep
  - Notepad++

- Tools information from a file's strings, functions, and headers
  - Strings.exe
  - Bintext.exe
  - Most of PE header browser extract strings

Packed Malware:

- If the malware was packed, it will contains very few strings.
- If upon searching a program with Strings, you find that it has only a few strings, it is probably either obfuscated or packed

- To unpack the malware, we need to know which packer used to pack it
- Most common packers are UPX, Aspack,...
- Tools :
  - PEiD
  - DIE
  - Exeinfo
  - PE

Resources:

- Resources are the objects used by the executable that are not considered part of it, such as icons, images, and menus.
- Some dropper store the dropped malware in resources.
- Tools:
  - Resource Hacker (can view, dump, and replace resources of the malware)

PE header:

- Another aspects we could know from PE header
  - Is malware for 32 or 64 systems
  - The date and time of compilation of the malware
  - Is it GUI or CLI
  - No. of sections

- Tools:
  - pestudio
  - Cff explorer
  - PEinfo