

picoCTF toolkit

- [Tools in picoCTF](#)
- [chroot to other linux drive from img](#)

Tools in picoCTF

1. category

1. tool

1. format

1. link(s)

2. if anything below format is empty / incomplete its probs coz i havent used it enough or forgot about how to use it when i wrote this, and or its self explanatory

1. description if applicable

1. sub notes

1. end with a RTFM for any more info coz if you need any more info it could be outdated this is just to quick remember things exist / how to download it

2. General Exploit tools

1. pwntools

1. Python, CLI

1. <https://docs.pwntools.com/en/stable/>

1. pwntools is a CTF framework and exploit development library. Written in Python, it is designed for rapid prototyping and development, and intended to make exploit writing as simple as possible.

1. if you do `import pwn` or `from pwn import *`, you will have access to everything you need to write an exploit.

2. Pwntools is best supported on 64-bit Ubuntu LTS releases (14.04, 16.04, 18.04, and 20.04). Most functionality should work on any Posix-like distribution (Debian, Arch, FreeBSD, OSX, etc.). so get ready to use wsl or a linux machine :D

1. if you must use python 2 u need a specific version of pip

```
$ apt-get update
$ apt-get install python python-pip python-dev git libssl-dev
libffi-dev build-essential
$ python2 -m pip install --upgrade pip==20.3.4
$ python2 -m pip install --upgrade pwntools
```

2. otherwise python 3 works as normal

```
$ apt-get update
$ apt-get install python3 python3-pip python3-dev git libssl-dev
libffi-dev build-essential
```

```
$ python3 -m pip install --upgrade pip
$ python3 -m pip install --upgrade pwntools
```

3. When installed with `sudo` the above commands will install Pwntools' command-line tools to somewhere like `/usr/bin`. An error will occur, so add `~/.local/bin` to your `$PATH` environment variable.

3. heres a link to the tutuorial

<https://docs.pwntools.com/en/stable/intro.html#tutorials>

3. Disk Analasys

1. Autopsy

1. GUI

1.

2. Sleuthkit

1. CLI

3. fls

1. cli

```
1. $ fls -o 360448 disk.flag.img 3981
r/r * 2082(realloc):  flag.txt
r/r 2371:  flag.uni.txt
```

4. icat

1. cli

1. read sector data

```
1. $ icat -o 360448 disk.flag.img 2371
picoCTF{flag_you_arnt_allowed_to_get_for_free}
```

5. Gunzip

1. CLI

1. man gunzip

2. works on .gz files

3. using ``gunzip disk.flag.img.gz`` basically spits out the copressed file then deletes file from the few times ive used it but idk

6. Dump the partition table of the disk image. We want to find the offset to the main partition:

```
$ mmls disk.flag.img

DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

Slot	Start	End	Length	Description
000: Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001: -----	0000000000	0000002047	0000002048	Unallocated
002: 000:000	0000002048	0000206847	0000204800	Linux (0x83)
003: 000:001	0000206848	0000360447	0000153600	Linux Swap / Solaris x86 (0x82)
004: 000:002	0000360448	0000614399	0000253952	Linux (0x83)

4. Packet Sniffer?

1. wireshark
 1. gui
2. tshark
 1. cli

5. files?

- 2.** find
 1. cli

1. `find / -type f -name "*flag*" -print`

6. general linux commands that i keep forgetting

1. uname -a
 1. general system informatiojn
2. lshw
 1. hardware info
3. lscpu
 1. cpu info
4. free -m
 1. memory info
5. df -h
 1. disk usage
6. lsusb
 1. usb devices
7. ip addr
 1. network config
8. ifconfig
 1. other network config
9. htop
 1. cli task manager
10. ps aux
 1. lists pid/tasks
11. lshw
 1. ???

chroot to other linux drive from img

```
└─(root@NaruZKurai)-[~]  
└─# mmls flag_drive.img
```

```
mmls flag_drive.img
```

DOS Partition Table

Offset Sector: 0

Units are in 512-byte sectors

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001:	-----	0000000000	0000002047	0000002048	Unallocated
002:	000:000	0000002048	0000206847	0000204800	Linux (0x83)
003:	000:001	0000206848	0000411647	0000204800	Linux Swap / Solaris x86 (0x82)
004:	000:002	0000411648	0000819199	0000407552	Linux (0x83)

```
└─(root@NaruZKurai)-[~]  
└─#
```

```
sudo mkdir /mnt/flag_drive
```

```
sudo mount -o loop,offset=$((2048*512)) flag_drive.img /mnt/flag_drive #Linux (0x83) is after offset 2047 *512 bytes so 2048
```

```
sudo mount -t proc /proc /mnt/flag_drive/proc
```

```
sudo mount -o bind /sys /mnt/flag_drive/sys
```

```
sudo mount -o bind /dev /mnt/flag_drive/dev
```

```
sudo chroot /mnt/flag_drive #possibly need to add /bin/bash or /bin/sh or depending on the operating system fish or ash or whatever else that system uses. look in /bin/ to see what shell it uses
```

#and just coz im hella forgetfull

```
find / -type f -name "*words*" 2>/dev/null
```

#im serious super forgetfull

```
grep -R "picoCTF{" / 2>/dev/null
```