Mason Competitive Cyber

Scrub Session - Intro to CLI & Linux

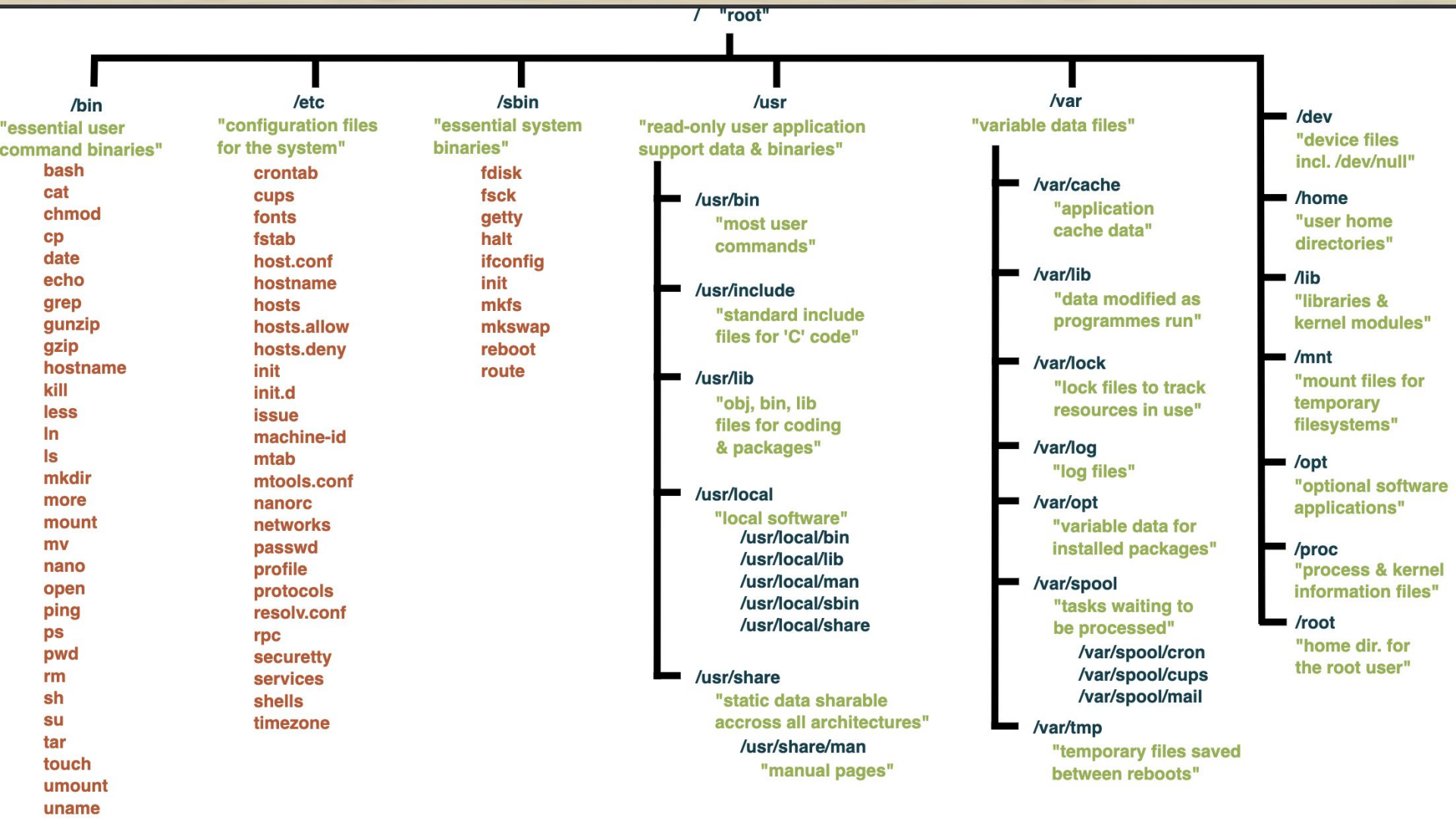
Upcoming Competitions

- National Cyber League Spring
  - March 19 - May 15
- CyberFusion State Cup (Team already full)
  - February 22-23
  - Take the crown back from UVA
- VT Summit
  - March 28
- PatriotCTF
  - April 11
- DawgCTF
  - April 11
- UMDCTF
  - April 18

What is Unix or Linux?

- Unix developed by Bell Labs in 1970s
  - First portable operating system
  - Written mostly in C
  - “Unix Philosophy” (Peter H. Salus, 1994)
    - Write programs that do one thing and do it well
    - Write programs to work together
    - Write programs to handle text streams, because that is a universal interface
- Linux kernel released by Linus Torvalds in 1991
  - Unix-like design
  - Many distributions
  - Runs virtually anywhere
    - 96.55% of web servers
    - 79.3% of smartphones, 60% of tablets
    - TVs, routers, consoles, smartwatches

*nix file system structure



What is CLI?

- CLI = Command Line Interface
- Method of interacting with system on a deeper level
- CLI Shells
  - Linux
    - sh, zsh, bash
  - Windows
    - Command Line, Powershell
- Different parts of a command line
  - Separated by spaces
    - Use “” for arguments with spaces in them

prompt command -Option --Long-Option argument

```
toaster@toasterbox:~$ ls -a
.  ..   .bash_history  .bash_logout
toaster@toasterbox:~$ _
```

Prompt

```
C:\Users\sova1>dir /a
 Volume in drive C is Local Disk 0
 Volume Serial Number is

 Directory of C:\Users\sova1

01/18/2020  04:11 PM    <DIR>
01/18/2020  04:11 PM    <DIR>
09/11/2018  08:02 PM
05/27/2018  03:08 AM    <DIR>
```

```
toaster@toaster:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .config
toaster@toaster:~$
```

Command

```
C:\Users\sova1>dir /a
 Volume in drive C is Local Disk 0
 Volume Serial Number is

 Directory of C:\Users\sova1

01/18/2020  04:11 PM    <DIR>          .
01/18/2020  04:11 PM    <DIR>          ..
09/11/2018  08:02 PM               862 .bash_history
05/27/2018  03:08 AM    <DIR>          .docker
```

```
toaster@toasterbox:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .config
toaster@toasterbox:~$
```

Option

```
C:\Users\sova1>dir /a
 Volume in drive C is Local Disk 0
 Volume Serial Number is

 Directory of C:\Users\sova1

01/18/2020  04:11 PM    <DIR>          .
01/18/2020  04:11 PM    <DIR>          ..
09/11/2018  08:02 PM               862 .bash_history
05/27/2018  03:08 AM    <DIR>          .docker
```

```
toaster@toaster:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .config
toaster@toaster:~$
```

Output

```
C:\Users\sova1>dir /a
 Volume in drive C is Local Disk 0
 Volume Serial Number is

 Directory of C:\Users\sova1

01/18/2020  04:11 PM    <DIR>          .
01/18/2020  04:11 PM    <DIR>          ..
09/11/2018  08:02 PM               862 .bash_history
05/27/2018  03:08 AM    <DIR>          .docker
```

pwd & ls examples

- pwd (Print Working Directory)
  - Prints absolute path to current directory

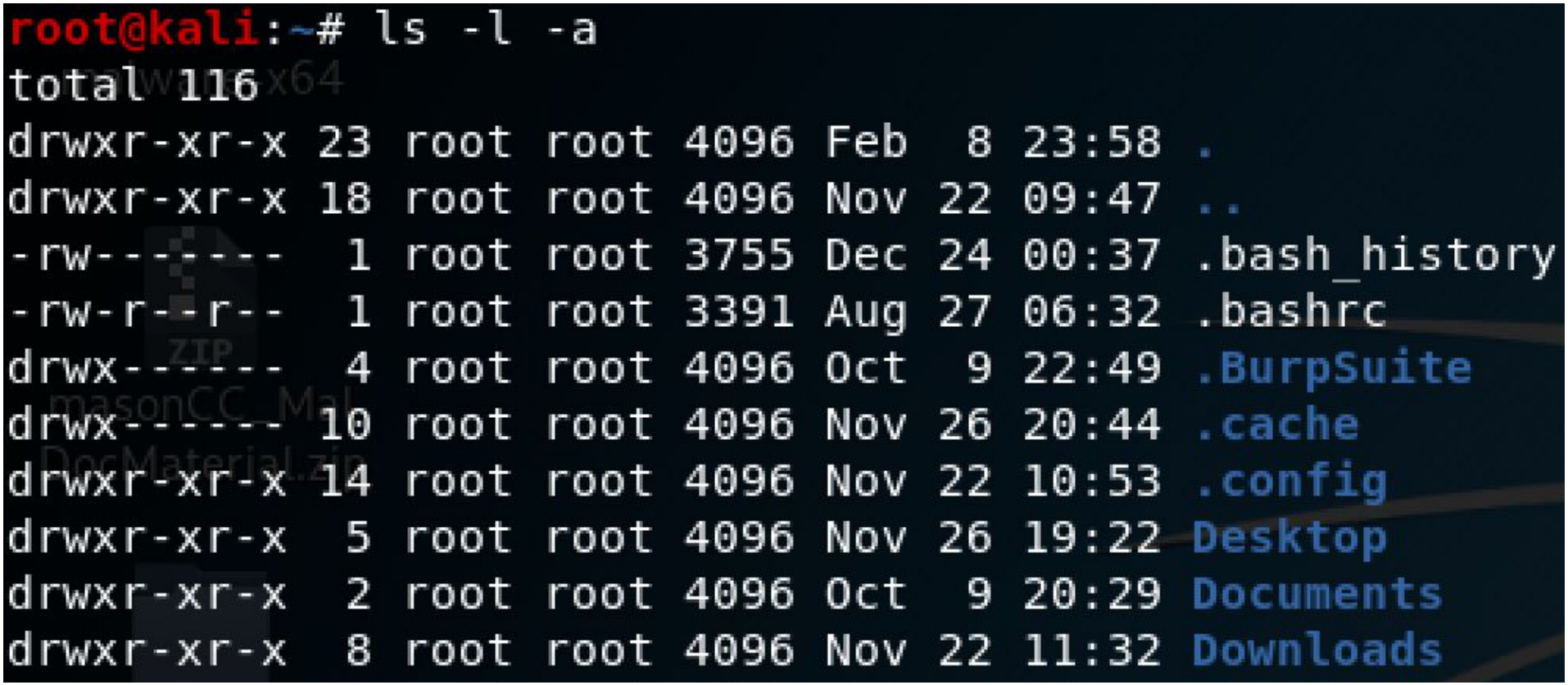
```
root@kali:~# pwd
/root
```

- ls (LiSt)
  - List files in a directory
  - -a shows even hidden files
  - -l shows files in list format with extra information

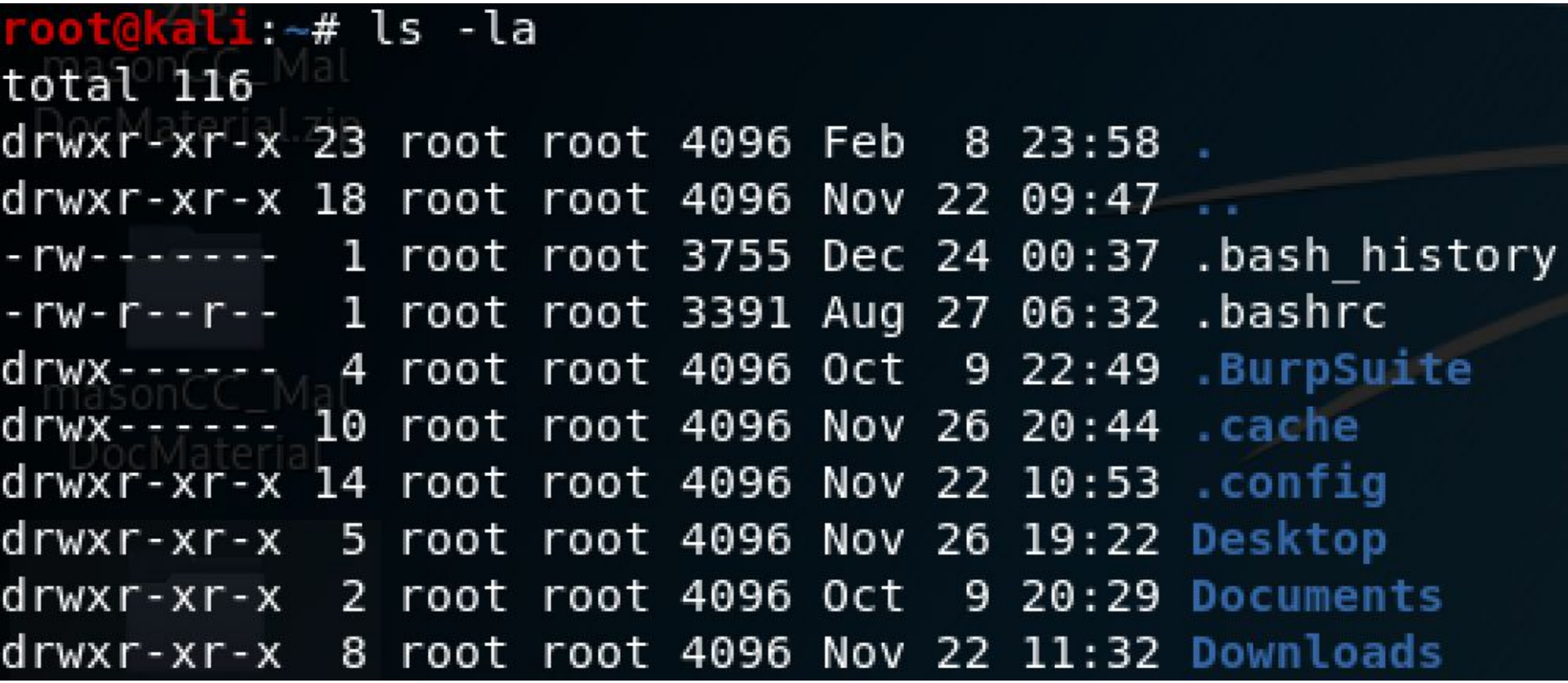
```
root@kali:~# ls
Desktop    Downloads  offshore  Public     Videos
Documents  Music      Pictures  Templates
```

```
root@kali:~# ls -a
.              .cache     .fr-PNoW77     .john      offshore  Templates
..             .config    .gnupg         .local     Pictures  Videos
.bash_history  Desktop    .ICEauthority  .mozilla   .profile  .zenmap
.bashrc        Documents  .install4j     .msf4      Public
.BurpSuite     Downloads  .java          Music      .ssh
```

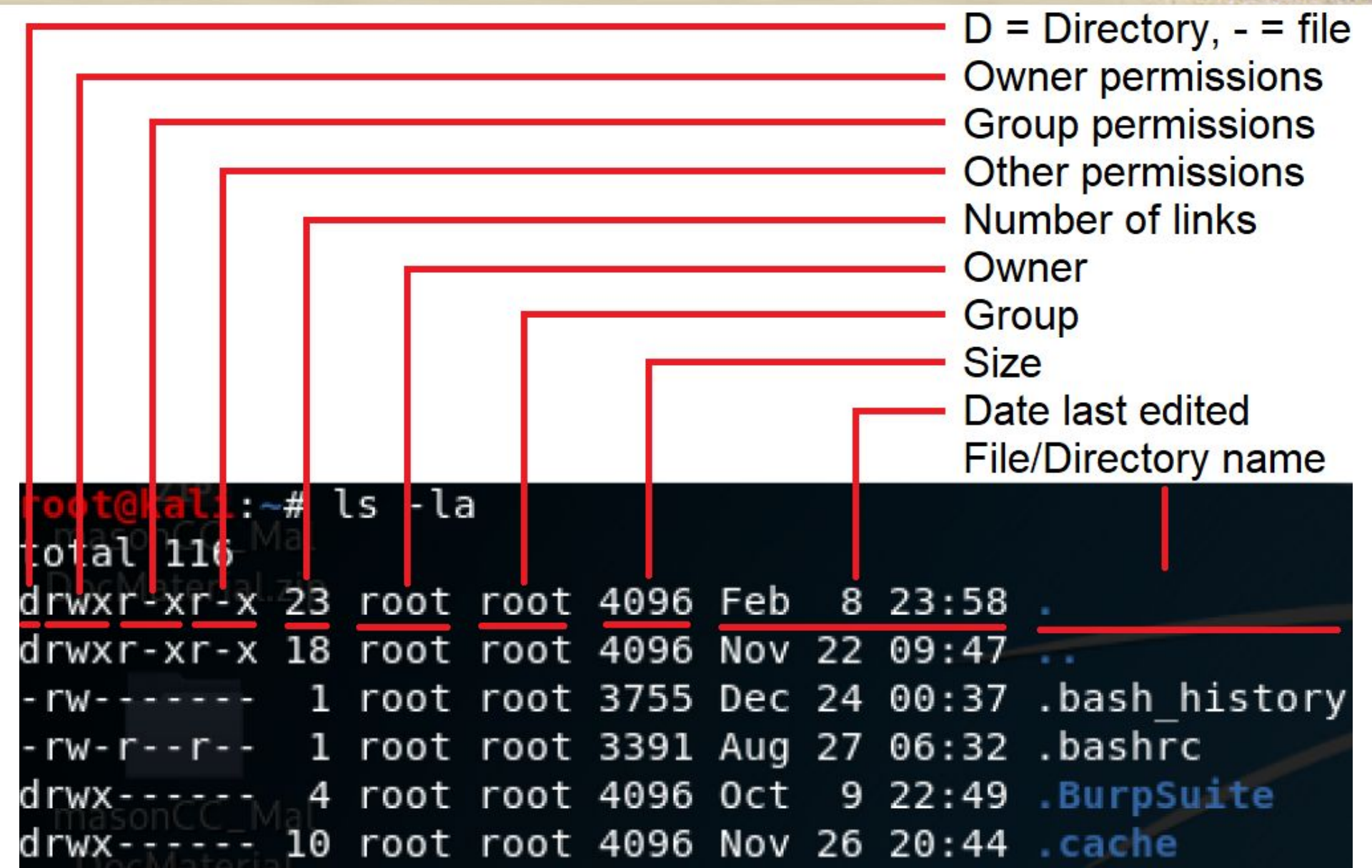
ls -l -a


root@kali:~# ls -l -a
total 116
drwxr-xr-x 23 root root 4096 Feb 8 23:58 .
drwxr-xr-x 18 root root 4096 Nov 22 09:47 ..
-rw------- 1 root root 3755 Dec 24 00:37 .bash_history
-rw-r--r-- 1 root root 3391 Aug 27 06:32 .bashrc
drwx------ 4 root root 4096 Oct 9 22:49 .BurpSuite
drwx------ 10 root root 4096 Nov 26 20:44 .cache
drwxr-xr-x 14 root root 4096 Nov 22 10:53 .config
drwxr-xr-x 5 root root 4096 Nov 26 19:22 Desktop
drwxr-xr-x 2 root root 4096 Oct 9 20:29 Documents
drwxr-xr-x 8 root root 4096 Nov 22 11:32 Downloads

ls -la


root@kali:~# ls -la
total 116
drwxr-xr-x 23 root root 4096 Feb 8 23:58 .
drwxr-xr-x 18 root root 4096 Nov 22 09:47 ..
-rw------- 1 root root 3755 Dec 24 00:37 .bash_history
-rw-r--r-- 1 root root 3391 Aug 27 06:32 .bashrc
drwx------ 4 root root 4096 Oct 9 22:49 .BurpSuite
drwx------ 10 root root 4096 Nov 26 20:44 .cache
drwxr-xr-x 14 root root 4096 Nov 22 10:53 .config
drwxr-xr-x 5 root root 4096 Nov 26 19:22 Desktop
drwxr-xr-x 2 root root 4096 Oct 9 20:29 Documents
drwxr-xr-x 8 root root 4096 Nov 22 11:32 Downloads

WHAT DOES ALL THAT MEAN??



When in doubt, --help

```
root@kali:~# ls --help
Usage: ls [OPTION]... [FILE]...
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.
  -a, --all                  do not ignore entries starting with .
  -A, --almost-all           do not list implied . and ..
      --author               with -l, print the author of each file
  -b, --escape               print C-style escapes for nongraphic characters
      --block-size=SIZE      with -l, scale sizes by SIZE when printing them;
                               e.g., '--block-size=M'; see SIZE format below
  -B, --ignore-backups       do not list implied entries ending with ~
  -c                         with -lt: sort by, and show, ctime (time of last
                               modification of file status information);
                               with -l: show ctime and sort by name;
                               otherwise: sort by ctime, newest first
  -C                         list entries by columns
      --color[=WHEN]         colorize the output; WHEN can be 'always' (default
                               if omitted), 'auto', or 'never'; more info below
  -d, --directory            list directories themselves, not their contents
  -D, --dired                generate output designed for Emacs' dired mode
  -f                         do not sort, enable -aU, disable -ls --color
  -F, --classify             append indicator (one of */=>@|) to entries
      --file-type            likewise, except do not append '*'
      --format=WORD          across -x, commas -m, horizontal -x, long -l,
                               single-column -1, verbose -l, vertical -C
```

When in even more doubt, man page it out

- man(ual) page
- e.x. man *command*

```
LS(1)                                User Commands                                LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List  information  about the FILEs (the current directory by default).  Sort entries alphabetically if none of -cftuvSUX nor --sort is speci-
       fied.

       Mandatory arguments to long options are mandatory for short options too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
              do not list implied . and ..

       --author
              with -l, print the author of each file

       -b, --escape
              print C-style escapes for nongraphic characters

       --block-size=SIZE
              with -l, scale sizes by SIZE when printing them; e.g., '--block-size=M'; see SIZE format below

       -B, --ignore-backups
              do not list implied entries ending with ~

       -c     with -lt: sort by, and show, ctime (time of last modification of file status information); with -l: show ctime and sort by name;  oth-
              erwise: sort by ctime, newest first

       -C     list entries by columns
```

cd (Change Directory)

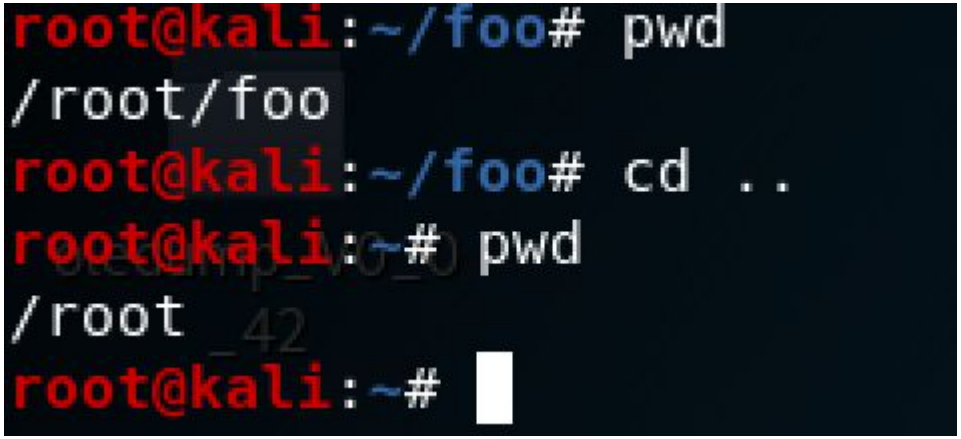
- Change working directory
- Absolute or relative path
  - Absolute e.x. /root/foo
  - Relative e.x. cd foo

```
root@kali:~# ls
Desktop  Documents  Downloads  foo  Music  offshore  Pictures  Public  Templates  Videos
root@kali:~# cd foo
```

```
root@kali:/home# cd /root/foo
root@kali:~/foo# pwd
/root/foo
```

cd (Change Directory) cont.

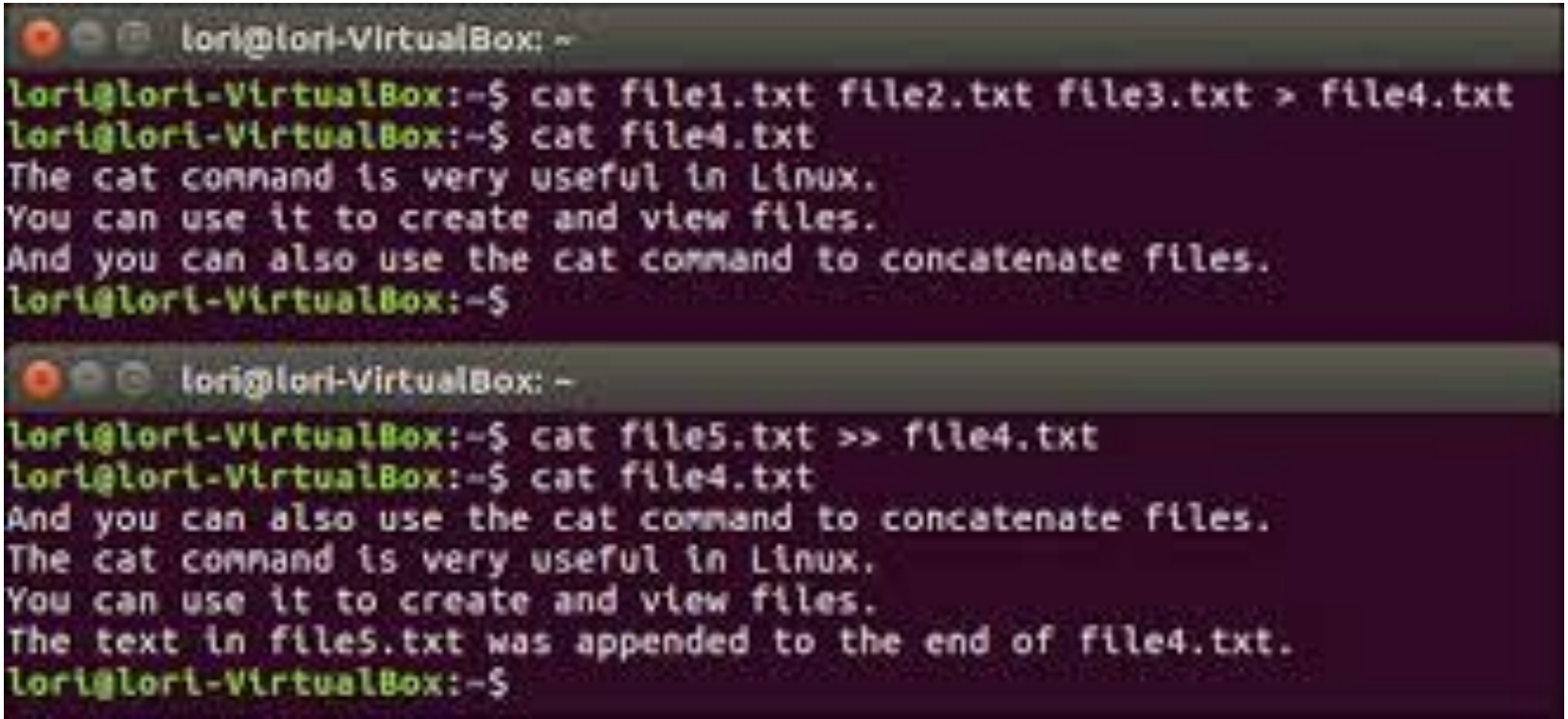
- “cd ..” goes up one directory level



- “~” points to user’s home directory
  - for regular user in /home
  - for root user /root

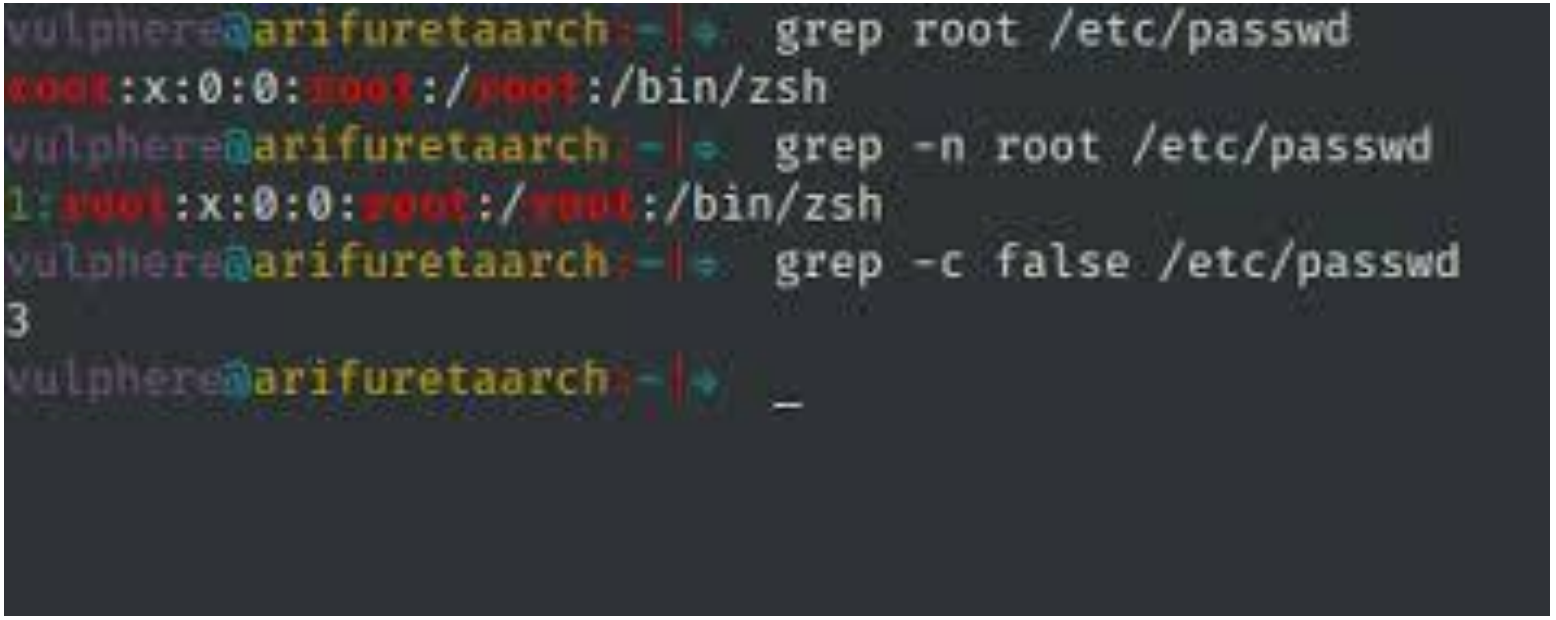
cat - concatenate

- Mostly use it to view contents of a file
  - `> cat file.txt` will print out the text inside of file.txt
- You can also concatenate files together into a new file
  - `> cat file.txt file2.txt > file3.txt` will concatenate file.txt and file2.txt and create a new file3.txt with the concatenation (or if file3.txt exists, it will just insert it into it)



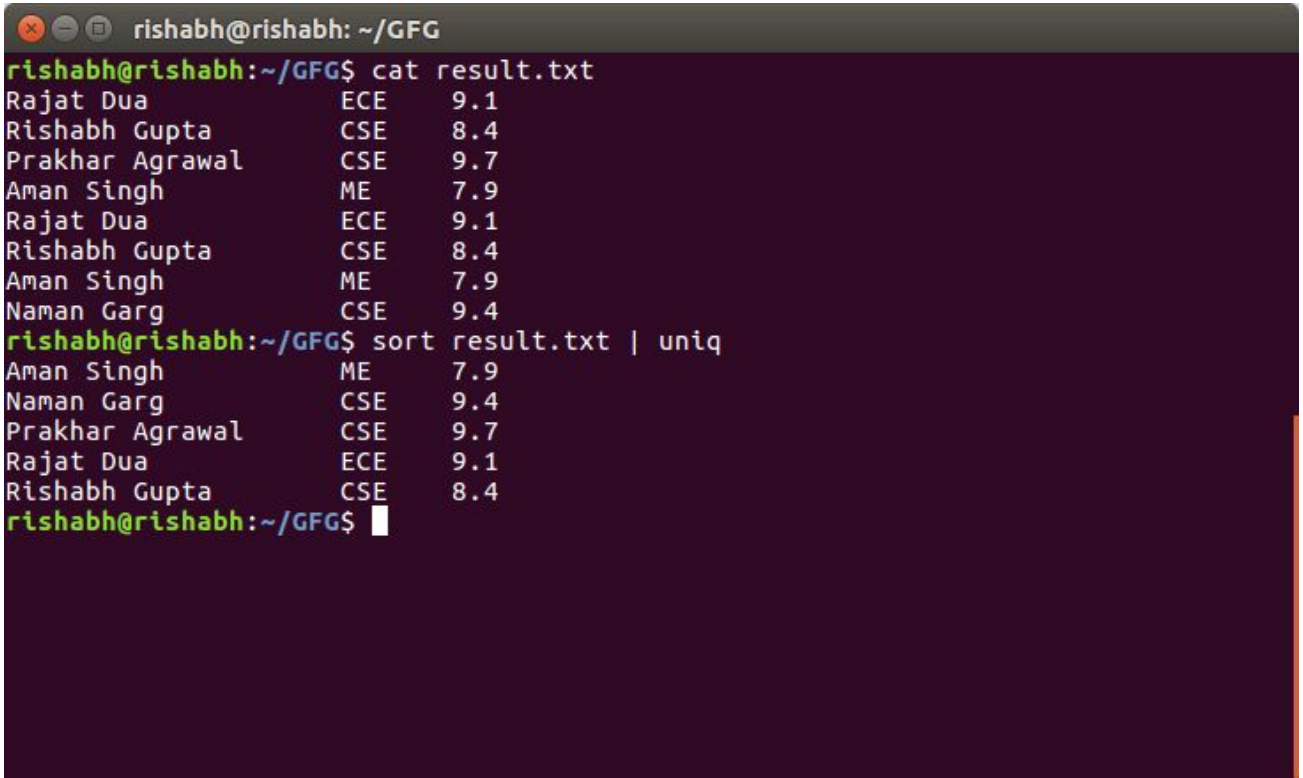
grep - search for stuff

- Syntax: grep [options] PATTERN [FILE...]
  - options are things like:
    - -i: ignore case
    - -c: count matching lines
- If you want to find the number of lines that the word flag appears in a text file file.txt, it would look something like:
  - > grep -c flag file.txt



| - “pipe”

- The vertical bar | is a way to transfer the output of one command into the input of another
- `> cat file.txt | grep flag`
  - This command uses the output of `cat file.txt` (just printing the insides of the file) and uses it as the input for grep (it becomes the file grep looks through to find the word flag)



Google Skills - Basically the most important part

- Challenge 1:
  - create a folder/directory
  - use “echo” to put text into a file
  - move that file into your new directory
  - use vi/vim to create a file and add text
  - copy that file into the new directory
  - rename the the copy of the file
- Challenge 2:
  - create a new user account and make them part of the “sudo” group
    - figure out what it means to be part of the “sudo” group
  - switch to that user and run some commands that require sudo
  - switch back to your normal user

CLI Challenges to Start With

TCTF (https://tctf.competitivecyber.club/):

- Grep 1
- Grep 2

picoCTF(https://2019game.picoctf.com/)

- “Only General Skills” problems
  - 2warm, let’s warm up, warmed up, bases
  - First Grep
  - Strings It
  - First Grep: II

OverTheWire Bandit (https://overthewire.org/wargames/bandit/)

Resources

- CTF Cheat Sheet (MasonCC document)
- https://picoctf.com/resources
- https://ctf101.org/
- https://trailofbits.github.io/ctf/intro/find.html

If you want to learn software exploitation, this is a good resource. It's hard and time consuming, but it does a good job at teaching.

- https://wargames.ret2.systems/

Proud Sponsors

Thank you to these organizations who give us their support

CACI

EVER VIGILANT

CRYPSIS™ BATTELLE

It can be done™

Social Media

@masoncompcyber

Title - Template Slide 1

- Body

Title - Template Slide 2