Linux

UBNetDef, Spring 2021

Week 5

Lead Presenter: Shreya Lakhkar

Special Thanks: Phil Fox

Agenda - Week

1. What is Linux?
2. Brief History
3. Why Linux?
4. Hands-on OverTheWire
5. Commands
6. Hands-on OverTheWire Contd.
7. Root
8. Text Editors
9. Permissions
10. Hands-on Permissions
11. Security in Linux
12. Homework Overview

What is Linux?

- An operating system
- Open-source
- Different distributions include:
  - Ubuntu
  - CentOS
  - Arch Linux
  - Debian
  - Fedora
  - Red Hat
  - and many more!

Where is Linux used?

- Software Development
- Embedded Systems
- Supercomputing
- Smart devices
- LAMP stack and web development
- And much more!!

History of Linux

1991: Linus Torvalds develops Linux as a personal project in Finland

1992: Linux gets released online for free

1996: Linux Mascot is created. His name → Torvalds UniX aka TUX!

2002: Red Hat Enterprise Linux released

2005: Linus Torvalds created Git to maintain Linux kernel

2009: Google announced Chrome OS based on Linux kernel

2013: Valve released SteamOS based on Debian (Linux distribution)

Why Linux?

- Some distributions are FREE!
- Open source community
- Highly secure and stable
- Runs on any hardware
- Customizable
- Variety of distributions for different uses

Let’s talk about commands . . .

- What commands have you used in Linux so far?
- What do these commands do?

Hands-on

Hands-on: OverTheWire

- **Add a rule in pfSense to allow TCP - source: your Linux client, destination: any, port: 2220**
- Go to https://overthewire.org/wargames/bandit/
- Follow the instructions and attempt levels 0→1, 1→2, 2→3, 3→4
- One person attempts a level and the others follow
- First one to get back to the main room wins bragging rights!

Discussion

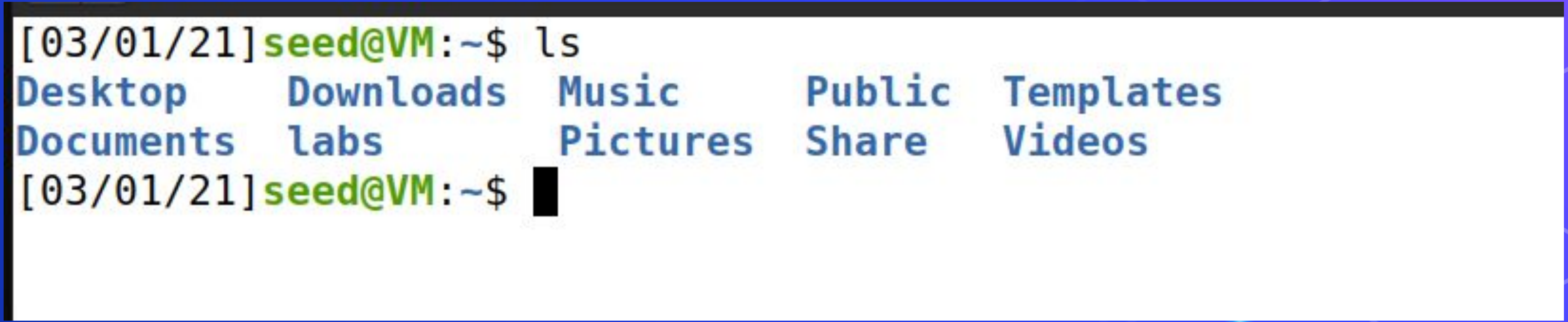
- What commands did you use in the activity?
- What do these commands do?

Speaking of commands . . .

- What is a command?
  - A way of communicating with the computer
  - An instruction given by a user telling a computer to do something
  - Issued by typing at the command line and pressing enter, which passes them to the shell.
- 3 components to a command…
  - Utility (required)
  - Flag
  - Argument

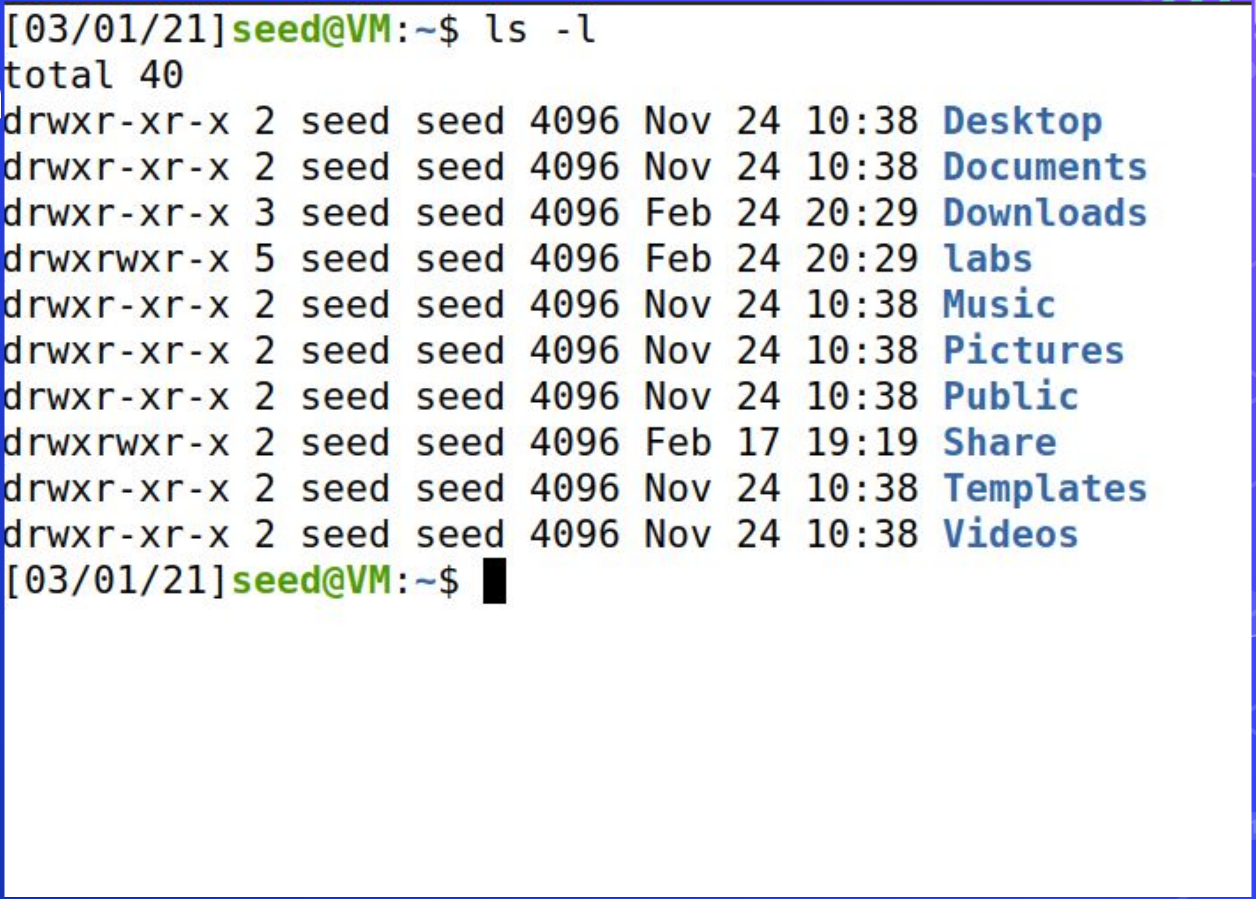
But what is a flag?

- A way to set options and pass in arguments to the commands you run.
- Commands change their behavior based on what flags are set.



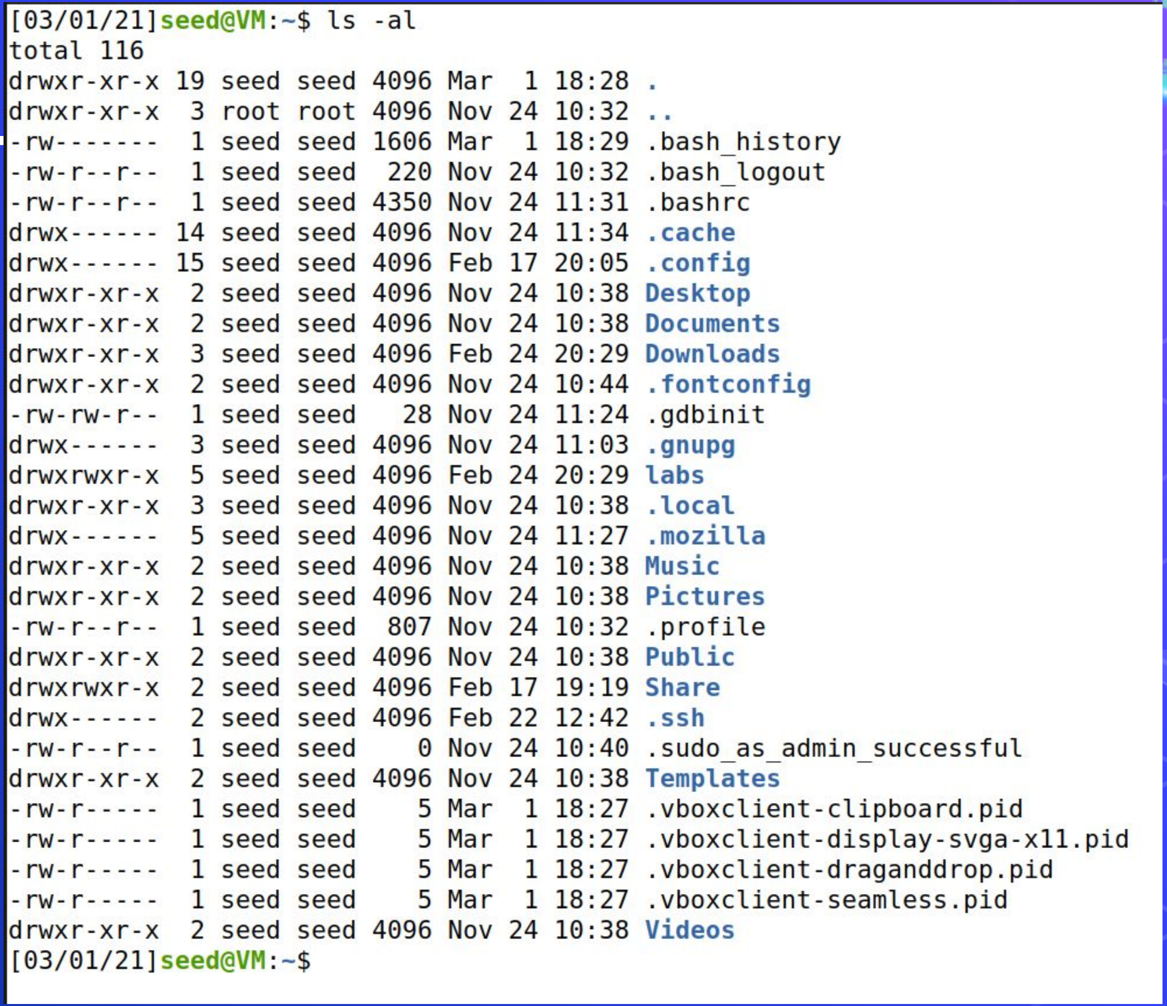
```
[03/01/21]seed@VM:~$ ls
Desktop    Downloads  Music     Public  Templates
Documents  labs       Pictures  Share   Videos
[03/01/21]seed@VM:~$ 
```

But wh



```
[03/01/21]seed@VM:~$ ls -l
total 40
drwxr-xr-x 2 seed seed 4096 Nov 24 10:38 Desktop
drwxr-xr-x 2 seed seed 4096 Nov 24 10:38 Documents
drwxr-xr-x 3 seed seed 4096 Feb 24 20:29 Downloads
drwxrwxr-x 5 seed seed 4096 Feb 24 20:29 labs
drwxr-xr-x 2 seed seed 4096 Nov 24 10:38 Music
drwxr-xr-x 2 seed seed 4096 Nov 24 10:38 Pictures
drwxr-xr-x 2 seed seed 4096 Nov 24 10:38 Public
drwxrwxr-x 2 seed seed 4096 Feb 17 19:19 Share
drwxr-xr-x 2 seed seed 4096 Nov 24 10:38 Templates
drwxr-xr-x 2 seed seed 4096 Nov 24 10:38 Videos
[03/01/21]seed@VM:~$ 
```

But wha

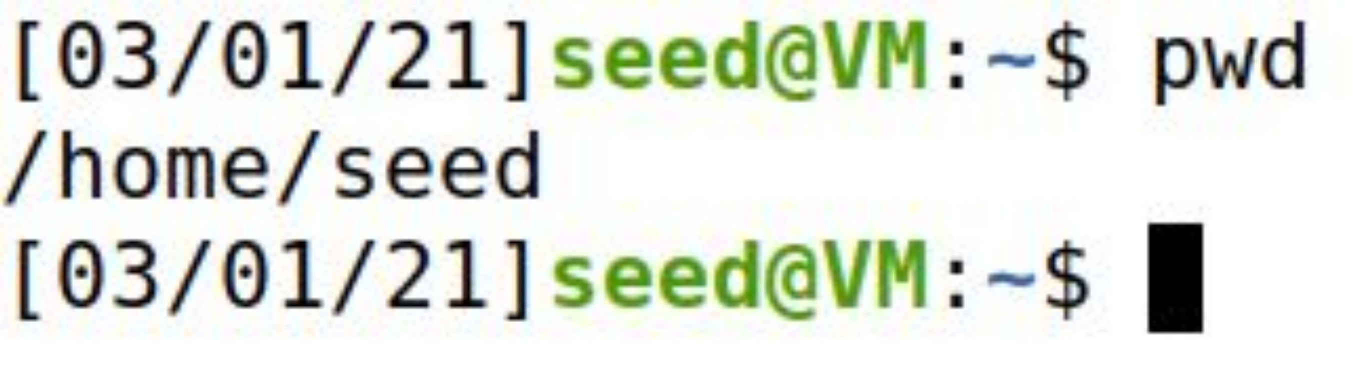


```
[03/01/21]seed@VM:~$ ls -al
total 116
drwxr-xr-x 19 seed seed 4096 Mar  1 18:28 .
drwxr-xr-x  3 root root 4096 Nov 24 10:32 ..
-rw-------  1 seed seed 1606 Mar  1 18:29 .bash_history
-rw-r--r--  1 seed seed  220 Nov 24 10:32 .bash_logout
-rw-r--r--  1 seed seed 4350 Nov 24 11:31 .bashrc
drwx------ 14 seed seed 4096 Nov 24 11:34 .cache
drwx------ 15 seed seed 4096 Feb 17 20:05 .config
drwxr-xr-x  2 seed seed 4096 Nov 24 10:38 Desktop
drwxr-xr-x  2 seed seed 4096 Nov 24 10:38 Documents
drwxr-xr-x  3 seed seed 4096 Feb 24 20:29 Downloads
drwxr-xr-x  2 seed seed 4096 Nov 24 10:44 .fontconfig
-rw-rw-r--  1 seed seed   28 Nov 24 11:24 .gdbinit
drwx------  3 seed seed 4096 Nov 24 11:03 .gnupg
drwxrwxr-x  5 seed seed 4096 Feb 24 20:29 labs
drwxr-xr-x  3 seed seed 4096 Nov 24 10:38 .local
drwx------  5 seed seed 4096 Nov 24 11:27 .mozilla
drwxr-xr-x  2 seed seed 4096 Nov 24 10:38 Music
drwxr-xr-x  2 seed seed 4096 Nov 24 10:38 Pictures
-rw-r--r--  1 seed seed  807 Nov 24 10:32 .profile
drwxr-xr-x  2 seed seed 4096 Nov 24 10:38 Public
drwxrwxr-x  2 seed seed 4096 Feb 17 19:19 Share
drwx------  2 seed seed 4096 Feb 22 12:42 .ssh
-rw-r--r--  1 seed seed    0 Nov 24 10:40 .sudo_as_admin_successful
drwxr-xr-x  2 seed seed 4096 Nov 24 10:38 Templates
-rw-r-----  1 seed seed    5 Mar  1 18:27 .vboxclient-clipboard.pid
-rw-r-----  1 seed seed    5 Mar  1 18:27 .vboxclient-display-svga-x11.pid
-rw-r-----  1 seed seed    5 Mar  1 18:27 .vboxclient-draganddrop.pid
-rw-r-----  1 seed seed    5 Mar  1 18:27 .vboxclient-seamless.pid
drwxr-xr-x  2 seed seed 4096 Nov 24 10:38 Videos
[03/01/21]seed@VM:~$
```

Let's go over some commands

pwd

- pwd = “print working directory”
- Tells you where you are



```
[03/01/21]seed@VM:~$ pwd
/home/seed
[03/01/21]seed@VM:~$ 
```

cd

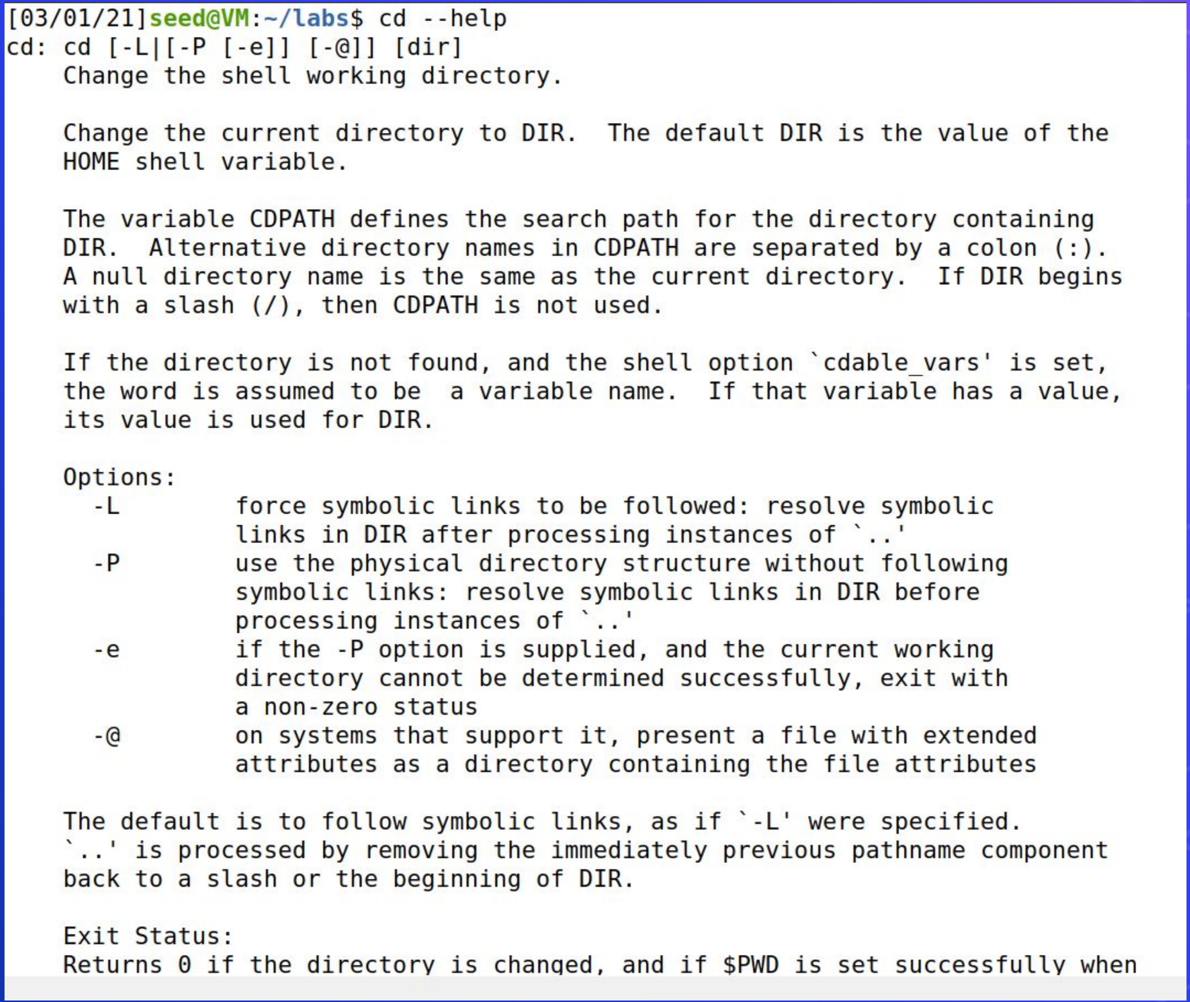
- cd = “change directory”
- Navigates from one folder to another
- cd .. → go to parent directory
- cd / → go to root directory
- cd ~ → go to home directory

ls

- ls = “list”
- Lists all the files in your directory
- Use flags for more information:
  - -a = lists hidden files
  - -l = shows permissions
- Can also list parent directory, root directory, and user’s home directory
  - Anyone remember how?

--help

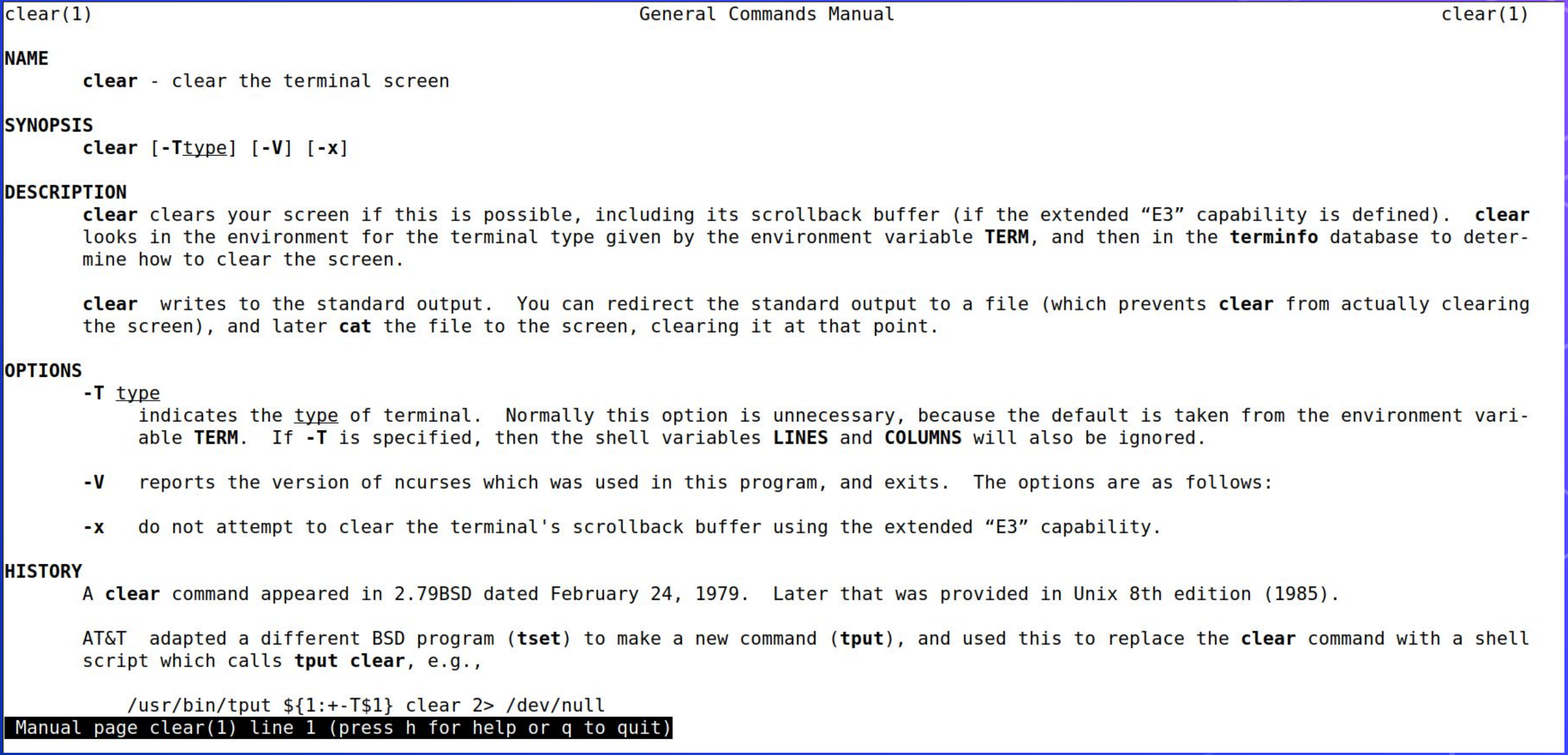
- Flag
- Lists the manual of the command
- Lists usage information and a list of options you can use with the command.



```
[03/01/21]seed@VM:~/labs$ cd --help
cd: cd [-L|[-P [-e]] [-@]] [dir]
    Change the shell working directory.

    Change the current directory to DIR.  The default DIR is the value of the
    HOME shell variable.

    The variable CDPATH defines the search path for the directory containing
    DIR.  Alternative directory names in CDPATH are separated by a colon (:).
    A null directory name is the same as the current directory.  If DIR begins
    with a slash (/), then CDPATH is not used.

    If the directory is not found, and the shell option `cdable_vars' is set,
    the word is assumed to be  a variable name.  If that variable has a value,
    its value is used for DIR.

    Options:
      -L        force symbolic links to be followed: resolve symbolic
                links in DIR after processing instances of `..'
      -P        use the physical directory structure without following
                symbolic links: resolve symbolic links in DIR before
                processing instances of `..'
      -e        if the -P option is supplied, and the current working
                directory cannot be determined successfully, exit with
                a non-zero status
      -@        on systems that support it, present a file with extended
                attributes as a directory containing the file attributes

    The default is to follow symbolic links, as if `-L' were specified.
    `..' is processed by removing the immediately previous pathname component
    back to a slash or the beginning of DIR.

    Exit Status:
    Returns 0 if the directory is changed, and if $PWD is set successfully when
```

man

- An interface to the system reference manuals
- Gives access to manual pages for command-line utilities and tools.



```
clear(1)                        General Commands Manual                        clear(1)

NAME
       clear - clear the terminal screen

SYNOPSIS
       clear [-Ttype] [-V] [-x]

DESCRIPTION
       clear clears your screen if this is possible, including its scrollback buffer (if the extended “E3” capability is defined).  clear
       looks in the environment for the terminal type given by the environment variable TERM, and then in the terminfo database to deter-
       mine how to clear the screen.

       clear  writes to the standard output.  You can redirect the standard output to a file (which prevents clear from actually clearing
       the screen), and later cat the file to the screen, clearing it at that point.

OPTIONS
       -T type
            indicates the type of terminal.  Normally this option is unnecessary, because the default is taken from the environment vari-
            able TERM.  If -T is specified, then the shell variables LINES and COLUMNS will also be ignored.

       -V   reports the version of ncurses which was used in this program, and exits.  The options are as follows:

       -x   do not attempt to clear the terminal's scrollback buffer using the extended “E3” capability.

HISTORY
       A clear command appeared in 2.79BSD dated February 24, 1979.  Later that was provided in Unix 8th edition (1985).

       AT&T  adapted a different BSD program (tset) to make a new command (tput), and used this to replace the clear command with a shell
       script which calls tput clear, e.g.,

           /usr/bin/tput ${1:+-T$1} clear 2> /dev/null
 Manual page clear(1) line 1 (press h for help or q to quit)
```

↑

- Up arrow on your keyboard
- Displays the last command you used
- Can keep pressing on the up arrow till you get to the command you want to use

history

- Displays the entire list of commands you have used since the start of the session.
- Use -c flag to clear the contents of the history file
- history n → shows the last n commands
- !n → executes the nth command
- !! → executes the previous command

ssh

- ssh = “secure shell”
- Lets you connect securely and remotely to another machine (replaced by Telnet)
- ssh bandit0@bandit.labs.overthewire.org

rm, mv, and cp

- rm = “remove”
  - Deletes files or directories
  - -d flag = removes a directory
- mv = “move”
  - moves a file from its current location to another location
- cp = “copy”
  - copies a file from its current location to another location

mkdir

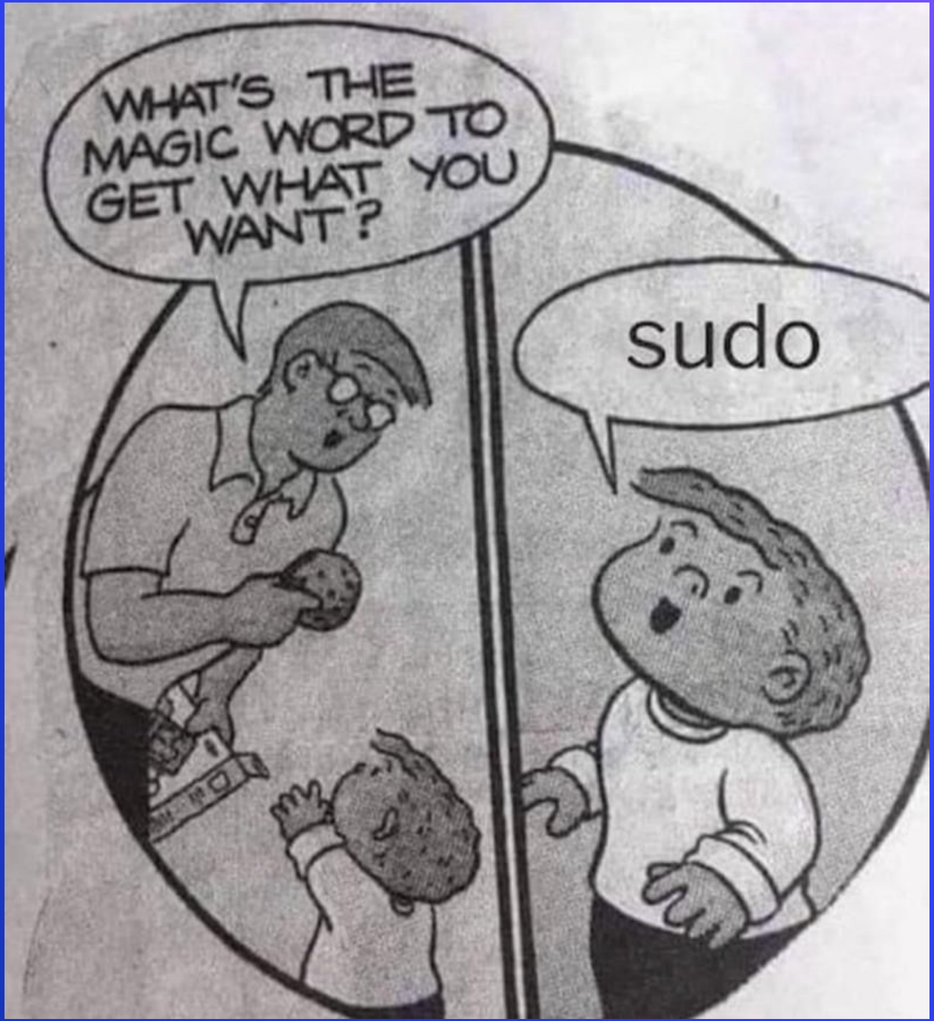
- mkdir = “make directory”
- Lets you create folders

Hands-on

Hands-on: OverTheWire (Part 2)

- Go to https://overthewire.org/wargames/bandit/
- Follow the instructions and attempt levels 7→8, 8→9, 9→10, 10→11
- ssh into bandit7@bandit.labs.overthewire.org -p 2220
  - password: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
- One person attempts a level and the others follow

Let’s talk permissions


WHAT'S THE MAGIC WORD TO GET WHAT YOU WANT?
sudo

Root - What does it mean?

- 2 roots:

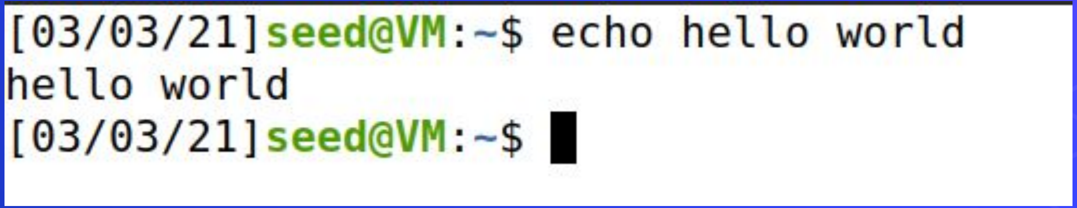
1. Root as a user:
   - root is the username or account that by default has access to all commands and files.
2. Root as a location:
   - The root directory (/root) - home directory of the root account
   - Everything is located in the / directory

touch

- touch lets you create, change and modify timestamps of files
- can create multiple files
- Use flags for additional specifications.

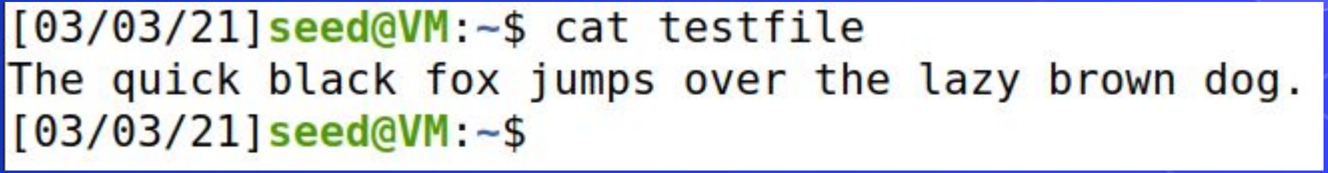
echo and cat

- echo = lets you display text in the terminal



```
[03/03/21]seed@VM:~$ echo hello world
hello world
[03/03/21]seed@VM:~$ █
```

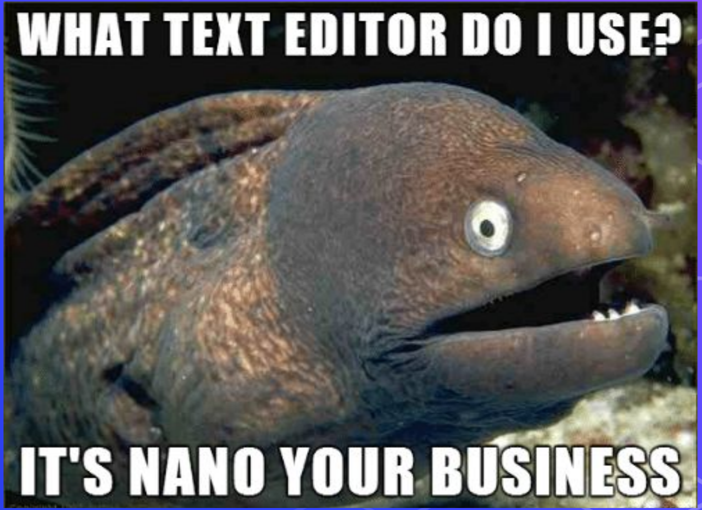
- cat = concatenate → lets you display text from files



```
[03/03/21]seed@VM:~$ cat testfile
The quick black fox jumps over the lazy brown dog.
[03/03/21]seed@VM:~$
```

Text Editors

- Used to edit files
- vi, gedit, emacs, nano, among others
- All programmers have different preferences:
  - nano, gedit = recommended for beginners
  - vi = advanced
- Some distributions might not have your preferred text editor, so good to learn others.

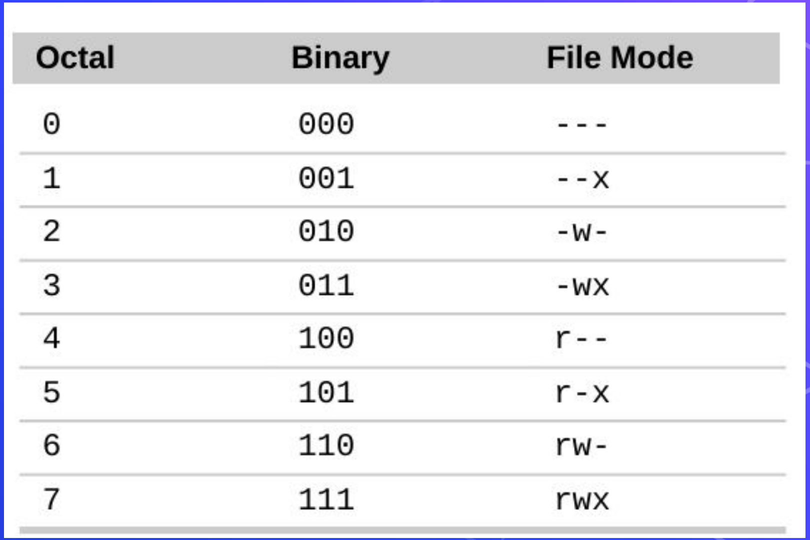


Permission bits

- Every file/directory is owned by a user.
- 3 levels of principals:
  - Owner
  - Group
  - World
- How do we view permissions?

Reading a Permission Entry

- <type flag> <user permissions> <group permissions> <world permissions>
- d rwx r-x r--
- Default permissions = 644
  - Read and write for owner
  - Read for group and the world.
- What is 755?
- What about 245?



Octal	Binary	File Mode
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x
6	110	rw-
7	111	rwx

chmod

- chmod = change file mode bits
- change file permissions
- chmod <permission> <filename>

chown and chgrp

- chown lets you change the user who owns the file

  chown <user> <path_to_file>

- chgrp lets you change the group who owns the file

  chgrp <group> <path_to_file>

Hands-on

Hands-on: Permissions

- Make a directory called testdir
  - In the directory, make a file called testfile and write something in it.
  - Write something in the file:
    - using a text editor
    - without using a text editor (using command line)
  - What are the default permissions of the file in binary bits? What about the directory?
- Change permissions of testdir to read-only for everyone and answer the following:
  - When you try to cd into the directory - what happens?
  - When you try to display the contents of the directory - what happens?
  - What about when you try to read the file?
- Do the same for write-only for everyone
- Do the same for execute-only for everyone
- Change ownership to root - can you cd into the directory?
- Delete the directory → can you do it?

Linux and Security

Security-focused commands

- netstat - shows list of open ports and connections
  - Lets you see which applications are listening to current traffic
- ufw - firewall → you can set firewall rules
- nmap - security scanner
  - “network mapper”
  - used to audit network security
  - Lets you scan a host to see what ports the host is listening to.
- last - to check login activity