Linux

UBNetDef, Spring 2021

Week 5

Lead Presenter: Anthony JeanPierre

Agenda - Week 5

1. Linux
2. Terminal
3. Hands-on OverTheWire
4. Command Examples
5. Hands-on (Part 2)
6. Permissions
7. Hands-on (Part 3)
8. Security in Linux
9. HW

What is Linux?

- An operating system
- Open-source
- Different distributions (flavors of Linux)
- Two Major Families of Distros include:
  - Debian Based: Debian, Ubuntu, Kali, Mint, Pop
  - Red Hat: Red Hat, Fedora, CentOS, Rocky

Where is Linux used?

- Software Development
- Supercomputing
- Embedded Systems:
  - Hardware + Software
    - Fitness trackers, GPS systems, electronic calculators, cars, Androids
- Roku, Chromecast, Amazon Fire TV
- LAMP stack and web development

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

Why Linux?

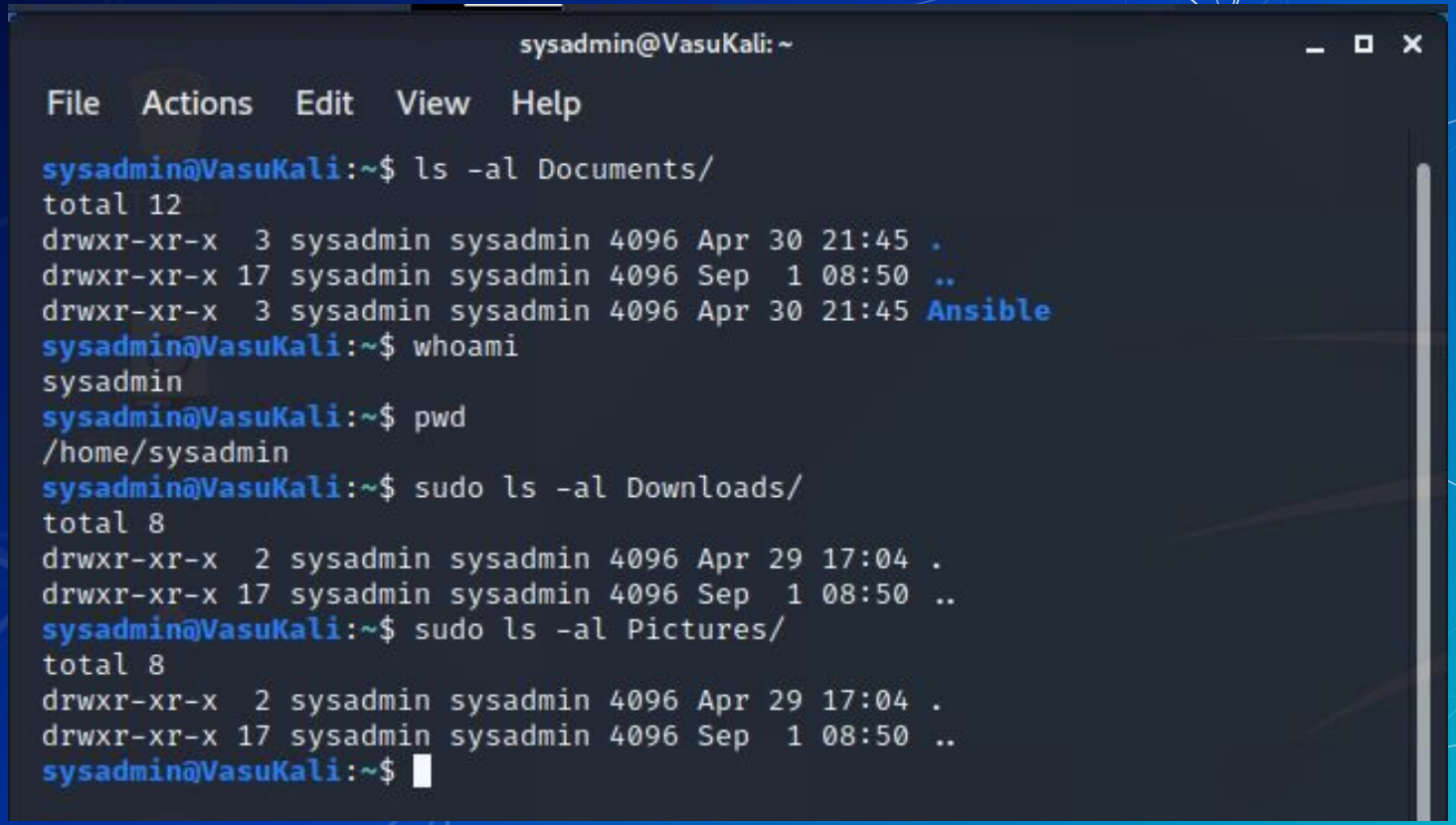
- Some distributions are FREE!
- Open source community
- Highly secure and stable
- Runs on any hardware
- Customizable to any use case!
- Lightweight
- Variety of distributions for different uses
  - What distros have you used??

Agenda - Week 5

1. Linux
2. Terminal
3. Hands-on OverTheWire
4. Command Examples
5. Hands-on (Part 2)
6. Permissions
7. Hands-on (Part 3)
8. Security in Linux
9. HW

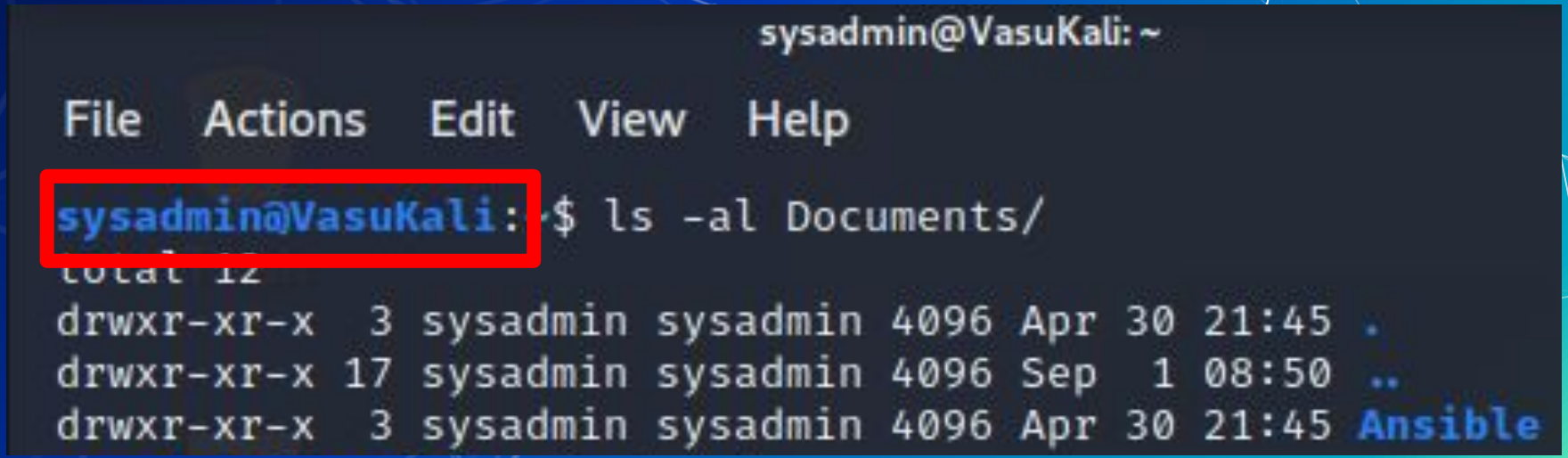
Terminal

- Another way to interact with your system
- Any GUI activity can be done here
- When have we used a terminal?


sysadmin@VasuKali: ~
File Actions Edit View Help
sysadmin@VasuKali:~$ ls -al Documents/
total 12
drwxr-xr-x 3 sysadmin sysadmin 4096 Apr 30 21:45 .
drwxr-xr-x 17 sysadmin sysadmin 4096 Sep 1 08:50 ..
drwxr-xr-x 3 sysadmin sysadmin 4096 Apr 30 21:45 Ansible
sysadmin@VasuKali:~$ whoami
sysadmin
sysadmin@VasuKali:~$ pwd
/home/sysadmin
sysadmin@VasuKali:~$ sudo ls -al Downloads/
total 8
drwxr-xr-x 2 sysadmin sysadmin 4096 Apr 29 17:04 .
drwxr-xr-x 17 sysadmin sysadmin 4096 Sep 1 08:50 ..
sysadmin@VasuKali:~$ sudo ls -al Pictures/
total 8
drwxr-xr-x 2 sysadmin sysadmin 4096 Apr 29 17:04 .
drwxr-xr-x 17 sysadmin sysadmin 4096 Sep 1 08:50 ..
sysadmin@VasuKali:~$

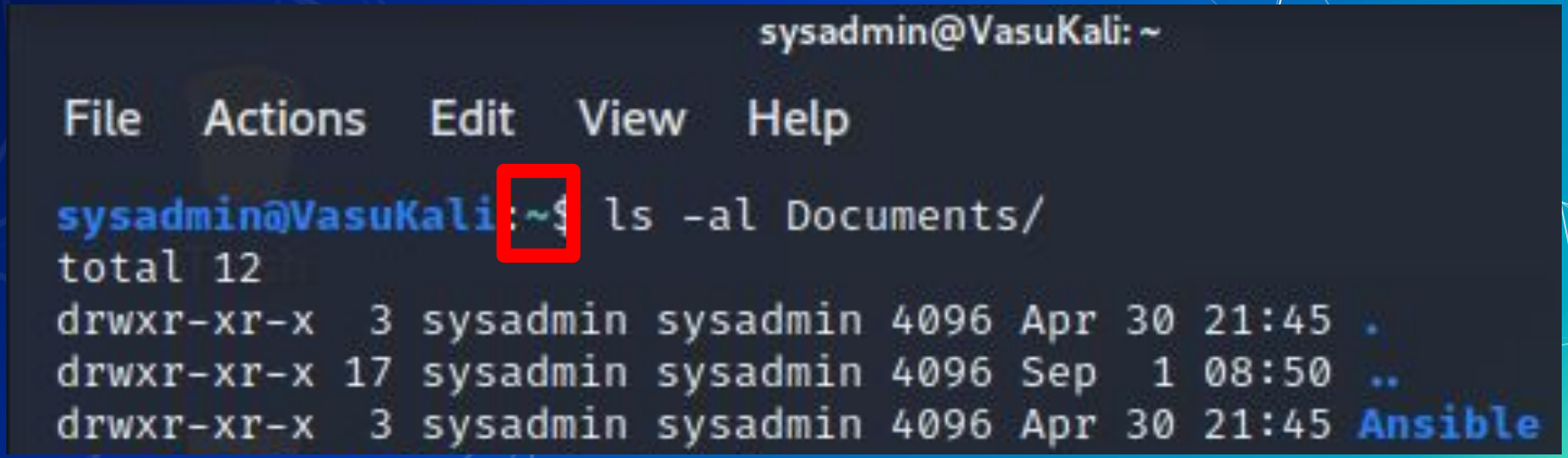
Terminal

- `sysadmin`: The username of the current user logged in
- `VasuKali`: The hostname of the server



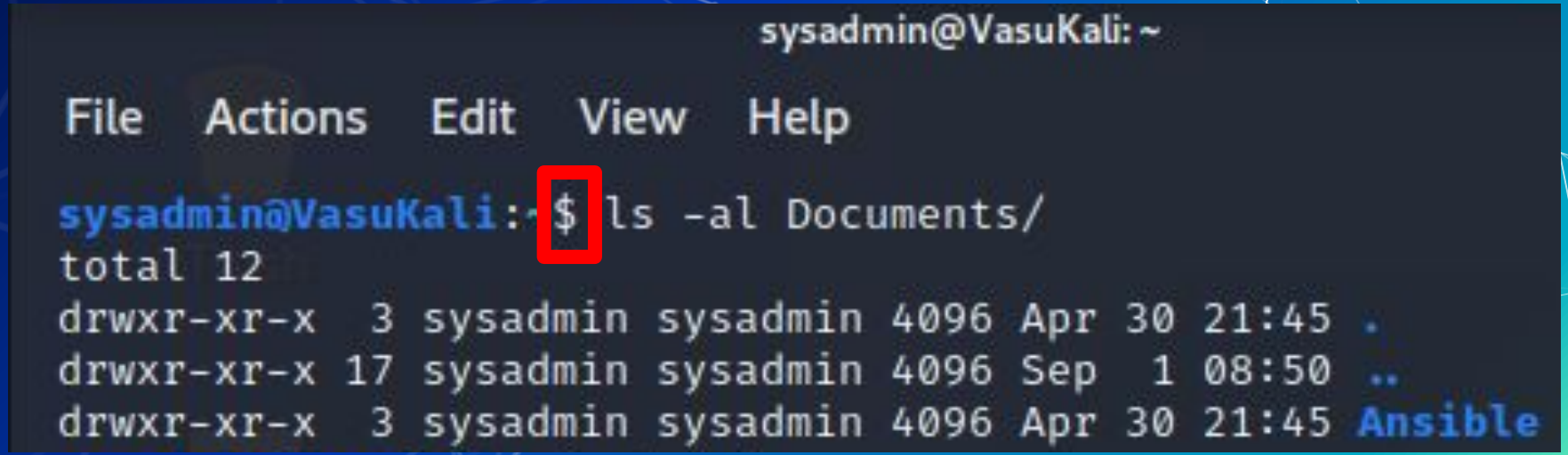
Terminal

- ~: The current directory



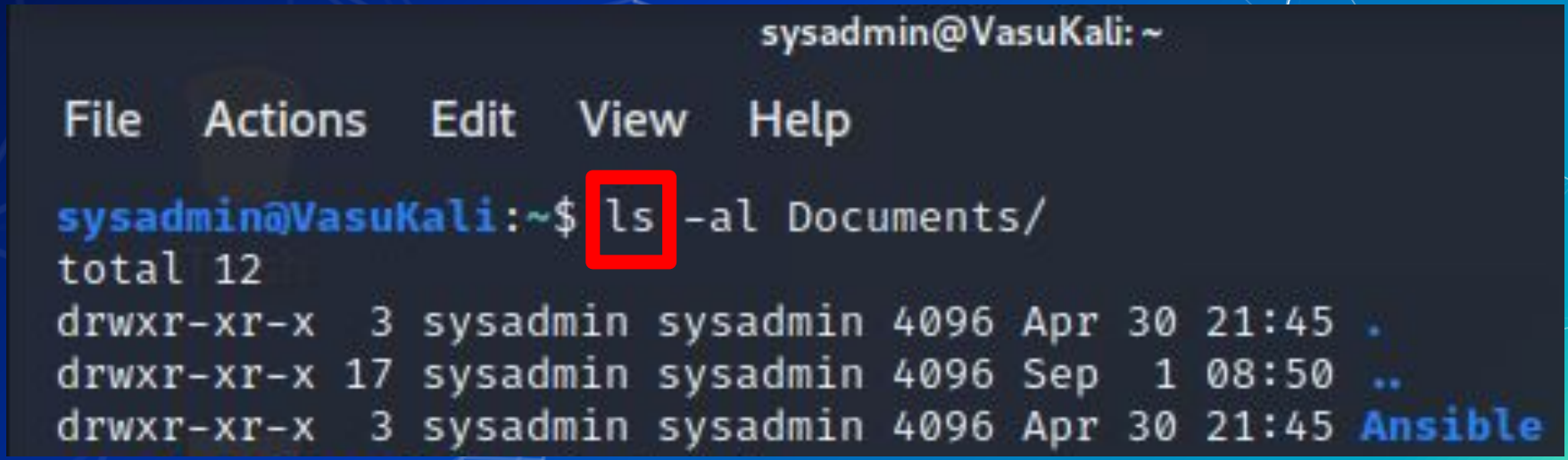
Terminal

- $: The prompt symbol.
- Denotes the end of the command prompt
  - User's keyboard input will appear next



Commands

- `ls` : A command
  - An instruction given by a user telling a computer to do something



Commands

- `-al`: 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.

```
sysadmin@VasuKali:~$ ls -al Documents/
total 12
drwxr-xr-x  3 sysadmin sysadmin 4096 Apr 30 21:45 .
drwxr-xr-x 17 sysadmin sysadmin 4096 Sep  1 08:50 ..
drwxr-xr-x  3 sysadmin sysadmin 4096 Apr 30 21:45 Ansible
```

Commands

- `Documents/` : An argument
  - File name referenced

```
sysadmin@VasuKali:~$ ls -al Documents/
total 12
drwxr-xr-x  3 sysadmin sysadmin 4096 Apr 30 21:45 .
drwxr-xr-x 17 sysadmin sysadmin 4096 Sep  1 08:50 ..
drwxr-xr-x  3 sysadmin sysadmin 4096 Apr 30 21:45 Ansible
```

Speaking of commands . . .

- What is a command?
  - 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): Action
  - Flag: variable
  - Argument: File name referenced

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 what is a flag?

```
[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 what is a flag?

```
[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
```

Let’s more talk about commands . . .

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

Basic Command Hints

- `cd` - change directory
  - `cd ..` → go to parent directory
  - `cd /` → go to root directory
  - `cd ~` → go to home directory
- `ls` - list all directories
- `ssh` - connect remotely to another machine
- `cat` - displays text
- ↑ (arrow key)- View previous command
- Tab Key - Autocomplete commands
- `sudo` - Run as administrator

Agenda - Week 5

1. Linux
2. Terminal
3. Hands-on OverTheWire
4. Command Examples
5. Hands-on (Part 2)
6. Permissions
7. Hands-on (Part 3)
8. Security in Linux
9. HW

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
- `ssh bandit0@bandit.labs.overthewire.org`

Discussion

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

Agenda - Week 5

1. Linux
2. Terminal
3. Hands-on OverTheWire
4. Command Examples
5. Hands-on (Part 2)
6. Permissions
7. Hands-on (Part 3)
8. Security in Linux
9. HW

Let’s go over some commands

Install vs Update vs Upgrade (Ubuntu)

- `apt-get install`
  - Installs packages
- `apt-get update`
  - Updates the list of available packages and their versions
  - **Does NOT install or upgrade any packages**
- `apt-get upgrade`
  - Installs newer versions of the packages you have

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

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 [**-T**type] [**-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 determine 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 variable **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)

`--help`

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

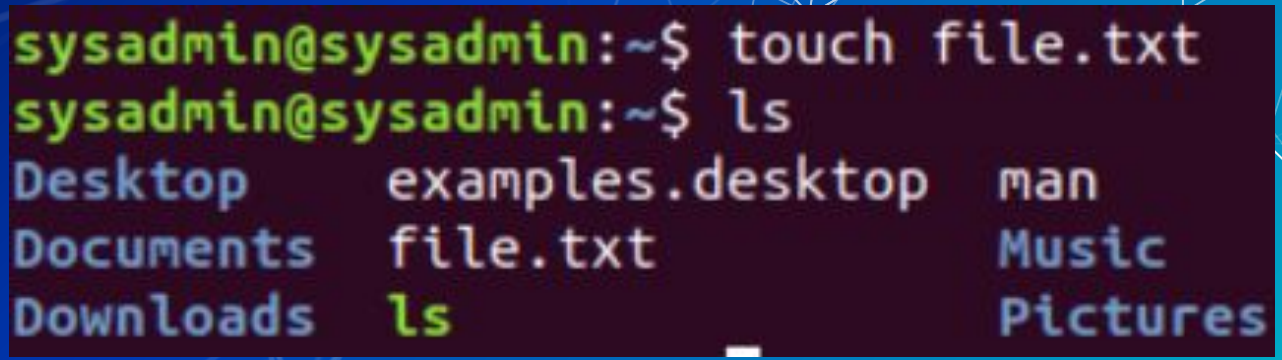
```
[03/01/21]seed@VM:~/labs$ cd --help
cd: cd [-L|[-P [-e]] [-@]] [dir]
    Change the shell working directory.

    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
```

ssh

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

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:~$
```

- 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

pwd

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

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

`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 n^{th} command
- **`!!` → executes the previous command**

`rm` & `mv`

- `rm` = “remove”
  - Deletes files or directories
  - `-d` flag → removes an empty directory
  - `-r` flag → delete directory and contents

- `mv` = “move”
  - Used to rename files
  - Moves a file from its current location to another location

`cp` & `mkdir`

- `cp` = “copy”
  - copies a file from its current location to another location
- `mkdir` = “make directory”
  - Lets you create folders

sudo

- `sudo` = “super user do”
- Run commands with elevated privileges
- sudo “command”
- `-i` flag . . → changes user to a root user

```
sysadmin@sysadmin:~$ sudo -i
[sudo] password for sysadmin:
root@sysadmin:~#
```

Root - What does it mean?

- Root as a user:
  - root is the username or account that by default has access to all commands and files.

Root - What does it mean?

- Root as a location:
  - The root directory (`/root`) - home directory of the root account
  - Everything is located in the / directory

Agenda - Week 5

1. Linux
2. Terminal
3. Hands-on OverTheWire
4. Command Examples
5. Hands-on (Part 2)
6. Permissions
7. Hands-on (Part 3)
8. Security in Linux
9. HW

Hands-on

Hands-on: (Part 2)

- `update` & `upgrade` your packages on `UbuntuClient`
  - Install `cowsay`
- Create a directory named '`SysSec`' in the root path
  - Move the directory to the `home` path
  - Copy the directory to to the `root` path
  - Remove '`SysSec`' from your machine

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

Break

Agenda - Week 5

1. Linux
2. Terminal
3. Hands-on OverTheWire
4. Command Examples
5. Hands-on (Part 2)
6. Permissions
7. Hands-on (Part 3)
8. Security in Linux
9. HW

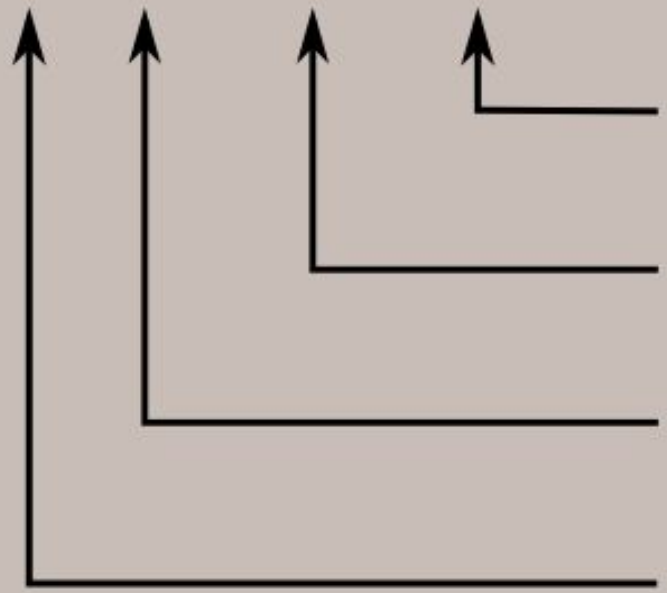
Let’s talk permissions

Permission Bits

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

Permission Bits

```
[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
```



Read, write, and execute permissions for all other users.

Read, write, and execute permissions for the group owner of the file.

Read, write, and execute permissions for the file owner.

File type:
- indicates regular file
d indicates directory

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>

```
[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
```

chown and chgrp

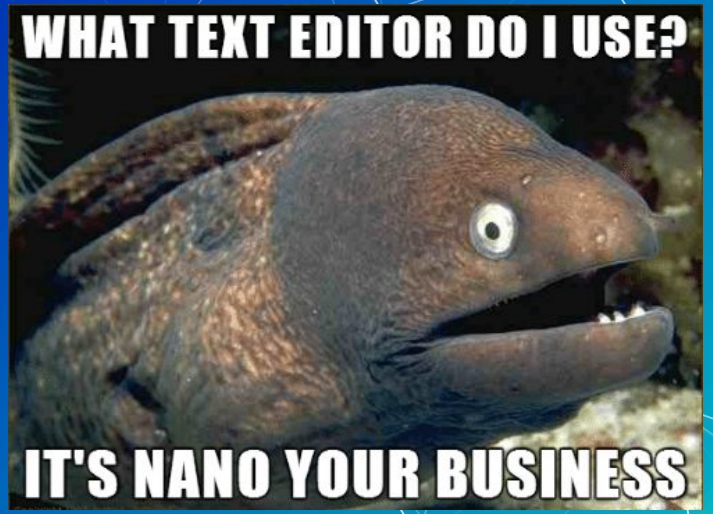
- `chown` lets you change the user who owns the file
  `chown <user> <path_to_file>`

- `chgrp` lets you change the group who owns the file
  `chgrp <group> <path_to_file>`

- `groups` lets you see what group you're in <groups>

Text Editors

- Used to edit files
- `vi`, `gedit`, `emacs`, `nano`, among others
- All programmers have different preferences:
  - `nano`, `gedit` = recommended for beginners
  - `vi` = advanced
- Good to learn multiple



Hands-on

Agenda - Week 5

1. Linux
2. Terminal
3. Hands-on OverTheWire
4. Command Examples
5. Hands-on (Part 2)
6. Permissions
7. Hands-on (Part 3)
8. Security in Linux
9. HW

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)

Hands-on: Permissions

- 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?

Hands-on: Permissions

- Change permissions of testdir to ***write-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?

Hands-on: Permissions

- Change permissions of testdir to ***`execute-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?

Hands-on: Permissions

- Change ownership to root - can you cd into the directory?
- Delete the directory → can you do it?

Agenda - Week 5

1. Linux
2. Terminal
3. Hands-on OverTheWire
4. Command Examples
5. Hands-on (Part 2)
6. Permissions
7. Hands-on (Part 3)
8. Security in Linux
9. HW

Linux and Security

Security-focused commands

- `ss` - 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

Security-focused commands

`ip a` - shows ip address

`ip r` - shows ip address

`whoami` - shows current user

```
sysadmin@sysadmin:~$ ip r
default via 192.168.254.254 dev ens192 proto dhcp metric 100
169.254.0.0/16 dev ens192 scope link metric 1000
192.168.254.0/24 dev ens192 proto kernel scope link src 192.168.254.52 metric 1
00
sysadmin@sysadmin:~$ whoami
sysadmin
```

Agenda - Week 5

1. Linux
2. Terminal
3. Hands-on OverTheWire
4. Command Examples
5. Hands-on (Part 2)
6. Permissions
7. Hands-on (Part 3)
8. Security in Linux
9. HW

Homework

Attendance