Basics of Linux

CSeC, IITB

Objectives for Today

- Get started with Linux
- Familiarize yourself with terminal & basic commands
- Begin HACKING :)) (through hands-on activities)

Linux

- Open source “kernel”
  - Kernel is the central component of OS which has control over everything
  - facilitates interactions between hardware and software components
- Created in 1990s by Linus Torvalds and Free Software Foundation(FSF)
- Highly customizable, released under GNU General Public License (GPL)
  - ANYONE can run, study, modify, and redistribute the source code, or even sell copies of their modified code, as long as they do so under the same license.
- Popular OS based on Linux : Ubuntu, Kali, Parrot

Windows vs Linux

- Windows is primarily based on graphical user interface (GUI)
  - CLI is much powerful than GUI
  - GUI leads to restrictions for users
- Closed source, marketed while Linux is transparent, non-profit and well-documented
- Linux is easy modify and many several tools/libraries under GNU exist as foundation
  - Many popular languages like Python, Java have better support for Linux than Windows

Terminal and Shell

- Terminal is command line *interface*, whilst shell is command line *interpreter*
  - terminal is a wrapper program that runs a shell and shows input/output
  - Shell is the one that actually executes commands and sends output
- Default shell in Linux is Bash.
  - Bash itself is not much customizable.
  - Can use other shells like Z shell, FI shell etc.

Now, let’s actually do something!

After starting the terminal, it may look something like this:

enigma@enigma-machine:~/Desktop/code$ //your command goes after $

- Here, the username is ‘enigma’ and the host machine name is ‘enigma-machine’.

- The ‘$’ is a shell prompt and it means that it is ready to ready to accept new commands.
  Having ‘#’ instead of ‘$’ means that the user is root.
  You can spawn shell in sudo mode using command $sudo su

- The text in blue represents what *directory* you’re currently in.

Directory is file system that contains references to other files (& directories).

Now, we'll start looking at some of the commands

Try all of them on your terminal to learn 'em quick!

pwd

- “print working directory”
- print name of (absolute) current/working directory
- ~ denotes the home directory of the user
  - you can check the location using $echo $HOME
  - would (mostly) be /home/user_name

```
enigma@enigma-machine:~/Desktop/code$pwd
/home/enigma/Desktop/code
enigma@enigma-machine:~/Desktop/code$
```

man

- your bestest friend and guide when working with terminal
- “User Command Manual” for Linux
  - Also has “Programmer’s Manual” for functions/syscalls
- Usage: $man <command>

Eg:- try man man, man ascii, man printf, man gets, man scanf

- However, initially reading man pages can seem intimidating/confusing, so you can always use Google (or use ChatGPT)

ls

- List contents of current directory
- $ls does not show hidden files/directories by default
  - Hidden files/directories begin with dot ‘.’
  - Use $ls -a
- A common variant used is $ls -alht which shows information in long format with file sizes, permissions etc.

```
enigma@enigma-machine:~/Desktop/code$ls
hello.c  practise-code  shell-code.tar
enigma@enigma-machine:~/Desktop/code$
```

(tally the above output with the output of tree)

cd

- “change directory”
- Usage: $cd <dirr>
  - .. denotes the parent (upper) directory of the current working directory
  - . denotes the current directory

```
enigma@enigma-machine:~/Desktop/code$cd ..
enigma@enigma-machine:~/Desktop$cd ~
enigma@enigma-machine:~$
```

NOTE: $cd - will transport you back to your previous working directory

```
enigma@enigma-machine:~$cd -
~/Desktop
enigma@enigma-machine:~/Desktop$
```

Also, $cd ~ is same as $cd (i.e. no need to type the directory if you want to go to your home directory)

Tab Completion and Wildcard

- Tab can be used to complete file/directory name

```
enigma@enigma-machine:~/Desktop/code$ls
hello.c  practise-code 'aoidfa oiandf 094r20n4n -'  shell-code.tar
enigma@enigma-machine:~/Desktop/code$cd aoi    //tab after typing some initial chars
enigma@enigma-machine:~/Desktop/code$cd aoidfa\ oiandf\ 094r20n4n\ -
```

Wildcard pattern matches to everything that has the string as a prefix. For example “abc*” will match abc, abcd, abchello etc.
The use of the wildcard will become more apparent with some examples.

Reading file(s): cat & less

- concatenate files and print on the standard output
  - Usage: $cat <file_1> <file_2> …..
  - Will print contents of all the files on terminal screen (in order)
- less will display output one page at a time
  - Usage: $less <file_name>

Time For a Challenge!

Head to the linktree and download the challenges zip file by clicking on **basics of hacking: linux.**
Extract it and then unzip level 0 and open a terminal and cd into level 0.

Time For a Challenge!

PASSWORD FOR LEVEL 1:
CSeC{purp13}

tree

- might not be installed by default
- list contents of directories in a tree-like format
- Usage: $tree <dirr_name>
  - Default argument is current directory

```
enigma@enigma-machine:~/Desktop/code$tree .
.
├── hello.c
├── practise-code
│   ├── a.out
│   ├── array.c
│   └── script.py
└── shell-code.tar
enigma@enigma-machine:~/Desktop/code$
```

grep

- Your new favourite searching utility.
  - The command prints each occurrence of pattern (A regex) in the file into the
  - To search for a pattern in a file, use: $grep <pattern> <path_to_file(s)>
  - Very powerful utility. To learn more see the manual as well as regexes

```
enigma@enigma-machine:~/Desktop/code$grep “CSeC{*” ./name.txt
CSeC{Guess_You_Found_the_Flag}
```

You can also explore the following (quite useful) flags:
-r, -E, -n, -o, -v

Time For a Challenge!

Head to the linktree and download the challenges zip file by clicking on **basics of hacking: linux.**
Extract it and then unzip level 1. Cd into level 1 and begin solving!!

The password for level 1 is:
CSeC{purp13}

Time For a Challenge!

PASSWORD FOR LEVEL 2:
CSeC{gr3p_f7w!}

find

- search for files in a directory hierarchy
  - Contains various filters to search for, see in $man find
  - To search for file with specific name, use: $find <dir> -name <name>

```
enigma@enigma-machine:~/Desktop/code$tree
.
├── hello.c
├── practise-code
│   ├── a.out
│   ├── array.c
│   └── script.py
└── shell-code.tar
enigma@enigma-machine:~/Desktop/code$find practise-code -name a.out
practise-code/a.out
enigma@enigma-machine:~/Desktop/code$find . -name b.out
enigma@enigma-machine:~/Desktop/code$
```

echo

- To print into the terminal.

```
enigma@enigma-machine:~/Desktop/code$echo “Hello World”
Hello World
enigma@enigma-machine:~/Desktop/code$echo “Testing” >> file.txt
enigma@enigma-machine:~/Desktop/code$cat file.txt
Testing
enigma@enigma-machine:~/Desktop/code$echo “Resting” >> file.txt
enigma@enigma-machine:~/Desktop/code$cat file.txt
Testing
Resting
enigma@enigma-machine:~/Desktop/code$
```

This will be much more useful when writing bash scripts. For more info on scripting this link

file

- Determine file type (of argument)

```
enigma@enigma-machine:~/Desktop/code$tree
.
├── hello.c
├── practise-code
│   ├── a.out
│   ├── array.c
│   └── script.py
└── shell-code.tar
enigma@enigma-machine:~/Desktop/code$file hello.c
hello.c: C source, ASCII text
enigma@enigma-machine:~/Desktop/code$file practise-code
practise-code: directory
enigma@enigma-machine:~/Desktop/code$
```

Time For a Challenge!

Head to the linktree and download the challenges zip file by clicking on **basics of hacking: linux.**
Extract it and then unzip level 2. Cd into level 2 and begin solving!!

The password for level 2 is:
CSeC{gr3p_f7w!}

Time For a Challenge!

PASSWORD FOR LEVEL 3:
CSeC{f1l3?}

cp, mv

- To copy/move files/directories from one directory to another
- Usage: $cp/mv <source file/dir> <destination>
- Subtle use: To rename files using terminal, mv is supposed to be used
    - $mv <old_file_name> <new_file_name>

```
enigma@enigma-machine:~/Desktop/code$ls
hello.c  practise-code  shell-code.tar
enigma@enigma-machine:~/Desktop/code$mv hello.c hello_world.c
enigma@enigma-machine:~/Desktop/code$ls
hello_world.c  practise-code  shell-code.tar
```

rm

- Removes files / directories
- By default, it will only remove file
  - Usage: $rm <file_name>
- To remove a directory, we use ‘recursive flag’ -r
  - Remove a directory: $rm -r <dir_name>
- To remove ‘read only’ files, use ‘force flag’ -f
  - Should be used VERY CAREFULLY! (could lead to removal of important OS files)

```
enigma@enigma-machine:~/Desktop/code$ls
hello_world.c  practise-code  shell-code.tar
enigma@enigma-machine:~/Desktop/code$rm -r practice-code/
enigma@enigma-machine:~/Desktop/code$ls
hello_world.c  shell-code.tar
```

ssh

- “secure shell”
- provides secure connection between two hosts over an insecure network
- Usage: $ssh user_name@host -p <port_no>

Resources For Further Learning

OTW:Bandit

- Follow the URL to access Over The Wire Bandit's webpage:

https://overthewire.org/wargames/bandit/bandit0.html

- Follow the instructions given on the page
- SSH using the command $ssh bandit0@bandit.labs.overthewire.org -p 2220
- The password for level 0 is 'bandit0'
- Now go as per the instructions on the web-page and try to get the passcode!

List of Resources

- Over the Wire: Bandit
- Program Misuse - pwncollege
- PicoCTF: practise
- The Linux command line for beginners: Ubuntu
- An A-Z Index of the Linux command line: bash + utilities
- Man7

Jumping into CTFs

After you are comfortable with Linux and Python, and want to participate in CTFs, you can look at various CTF events at https://ctftime.org/

Q&A

Thank you!

Good luck for your journey ahead

Bonus Challenge!!!!

Head to the linktree and download the challenges zip file by clicking on **basics of hacking: linux.**
Extract it and then unzip level 3. cd into level 3 and begin solving!!
First look at the README (using cat ofc)

The password for level 3 is:
CSeC{f1l3?}