Ethical Student Hackers

$ beginners_linux

SHEFFIELD | Ethical Student Hackers

Breaking into security.

The legal bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

SHEFFIELD Ethical Student Hackers
Breaking into security.

Code of Conduct

- Before proceeding past this point you must read and agree our Code of Conduct, this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://wiki.shefesh.com/

SHEFFIELD Ethical Student Hackers
Breaking into security.

Just how ethical is hacking?

- Are you interested in ethics and / or debate? Join us on Thursday the 8th of October for a collaboration with Sheffield Debating Society.
- We need TWO volunteers from the society to participate in the debate, but anyone can watch.
- Email us at ethicalhackers@sheffield.ac.uk or contact a member of the committee if you're interested in taking part!

SHEFFIELD Ethical Student Hackers
Breaking into security.

What is linux?

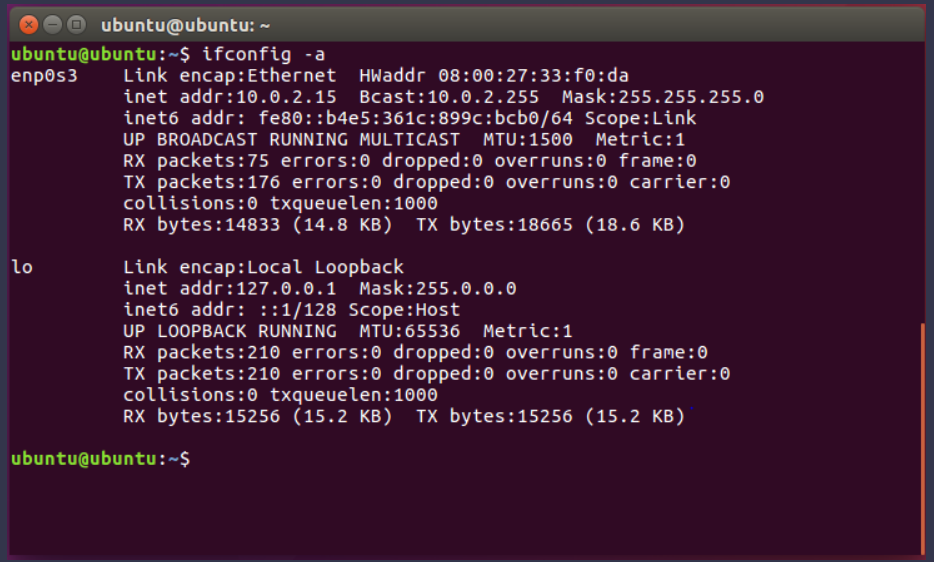
Command Line

Step 1: Open the terminal (Ctrl+Alt+T)

Apps -> Terminal on OS

Bash or WSL on Windows

ALT : https://bellard.org/jslinux/



Basic Commands

Try as we go along!

pwd : This will tell you what directory you are in

mkdir <name> : This will create a folder with the name of your choice

cd <name> : This command will allow you to navigate into the folder you just made . Cd by itself navigates to the home directory.

touch <filename> : You can create a new file in this directory

ls :Use this command to see the file you just created

Challenge #1

More Commands

- Echo “hello” (will print hello to the console)
- Cp file_name directory/to/move/it/to
- Cat file.txt (shows files content)

CHALLENGE

1- Make a new file and add whatever contents you want

2- Make a new directory

3- Copy that file into your new directory

4- Display the contents of the file in the terminal

Basic Commands

Sudo

Run commands as admin.

Can change read write execute permissions of a file with ‘chmod’.

Piping

Sends the output of one command to another -> |

eg) ls | grep examplefile.txt

Flags

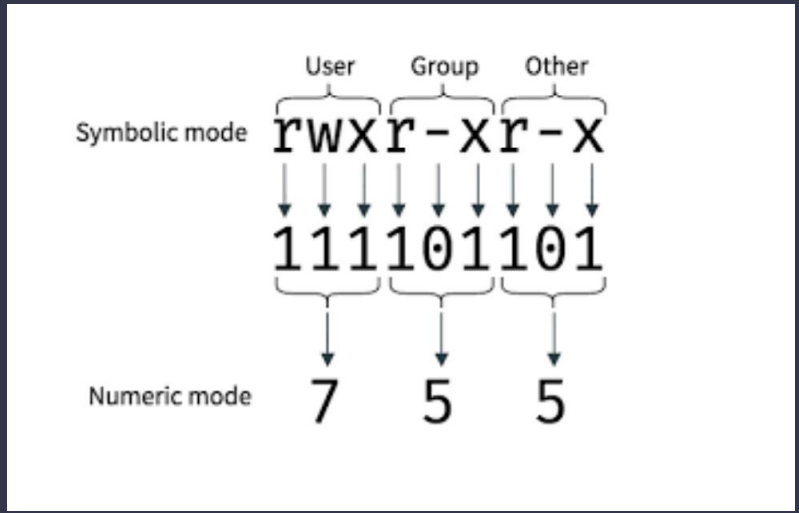
Apply additional information with the use of a dash and a filter

eg) ls -l
Use man to see all possible flags

Permissions

whoami • The symbol after the ~ is also a useful indicator • # denotes you are root (highest privilege)

Dont use ‘sudo’ unless you need to- can lead to vulnerabilities



Challenge #2

More Commands

- **Find <filename> :searches if a file with your search term exists**
- **Sort <filename> : orders the contents of the file**

CHALLENGE

1- create a file with a list of words (one on each line)

2 - sort the contents of the file and pipe it into a new file

3 - move back a directory and use find to search for the file you made (will need a recursive flag)

4 - edit your file using vim file_name, nano file_name and then gedit file_name. Explore these text editors. (May want to google how to use vim)

5- change permissions of the file so the user can read write but not execute

SHEFFIELD Ethical Student Hackers
Breaking into security.

Bandit

Test your Skills:
Over The Wire

Bouncing Around Bandit

- OverTheWire hosts a number of simulated hacking challenges of varying difficulties; Bandit serves as a beginner's intro to the Linux command line.
- Normally you need to complete the levels in order (completing each level gives the password for the next), but we'll be skipping around a bit during this session.
- Instructions for completing each level can be found here: https://overthewire.org/wargames/bandit
- This is meant to be quite interactive! Please contribute your ideas as we go along!

Sheffield Ethical Student Hackers
Breaking into security.

Using SSH

```
ssh -p 2220 bandit0@bandit.labs.overthewire.org
```

ssh stands for “secure shell” and is used to open an encrypted remote connection to another computer

-p 2220 is an example of a flag argument, in this case specifying the port to connect to; 22 is the default.

bandit0 is the name of the user we’d like to log in as. This user must exist on the remote machine.

bandit.labs.overthewire.org is the address of the machine we’d like to login to

SHEFFIELD Ethical Student Hackers
Breaking into security.

Put on Your Bandit Mask...

- Now that we've gone through a couple of levels together, it's your turn to drive! As homework, you should try to make your way through all of the Bandit challenges from start to finish. You can start with the instructions here: https://overthewire.org/wargames/bandit
- If you get stuck we'll be posting the solutions in a weeks time. Until then, feel free to message on the Discord and someone will help you out.
- If you are looking to practice the basics some more before taking on Bandit, you can check out https://cmdchallenge.com/
- Additionally, you can check out the more cybersecurity-focused Linux challenges on this week's worksheet. You can find all of our worksheets here: https://shefesh.com/wiki/worksheets

Any Questions?

www.shefesh.com

SHEFFIELD Ethical Student Hackers

Breaking into security.