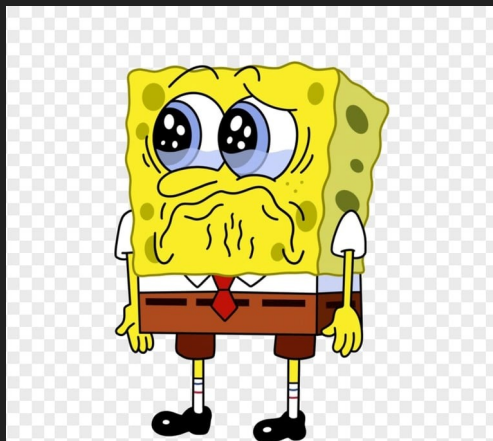# Using the Linux Command Line

Gotta start somewhere

We should get comfortable with the command line

A lot of hacking has to do with the command line

(You get to learn wayy more about how your OS system actually works)

I just wanna hack the mainframe

We're going to walk through the first few challenges of a beginner wargame

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

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

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

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

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

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

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

To start the game, let's SSH into their server!

SSH stands for Secure Shell, and it is a network protocol used to securely access and manage remote computers and servers over a potentially unsecured network, such as the internet. SSH provides a secure way to log into and execute commands on a remote machine, as well as transfer files between computers. It was designed to replace older, less secure protocols like Telnet and RSH (Remote Shell).

Figure 7.1 Remote login is a lot like astral projection.
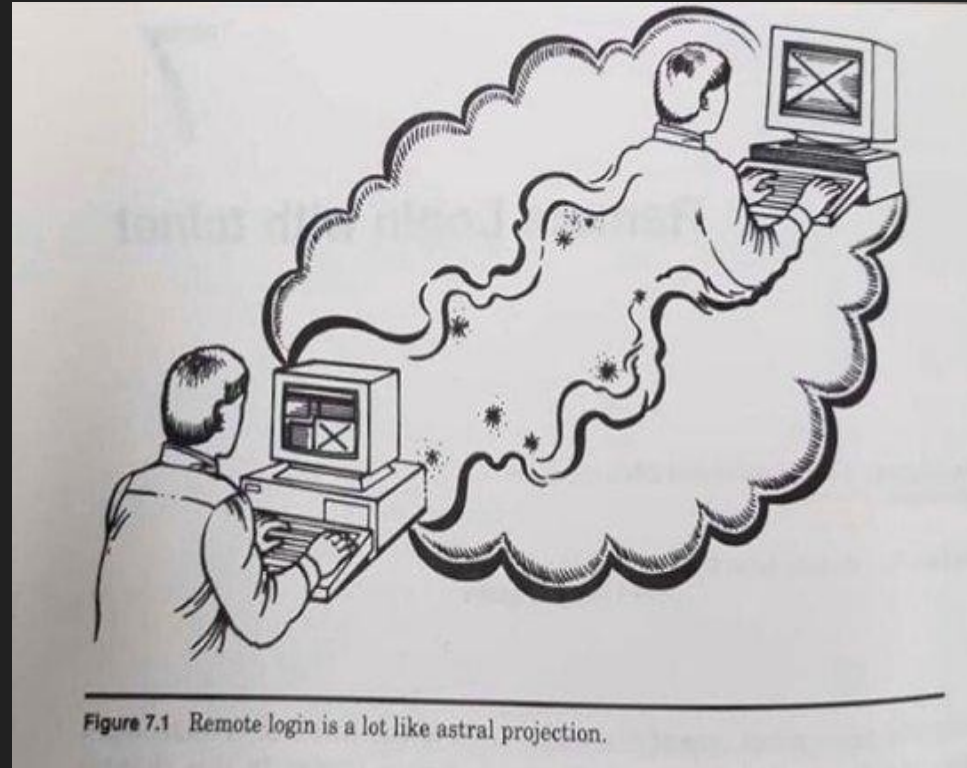
This is typically how you would use the command….

```
C:\Users\micha>ssh bandit0@bandit.labs.overthewire.org
```

"ssh" denotes to the command to ssh to something.
"bandit0" refers to the user that you will be logged in as when you enter the server's terminal
"bandit.labs.overthewire.org" refers to the address to connect to, where the server is located

Note: Domain names and ip addresses can be used interchangeably for the server connection.

If I try to run this command, it no worky… what's going on?

```
C:\Users\micha>ssh bandit0@bandit.labs.overthewire.org
The authenticity of host 'bandit.labs.overthewire.org (16.16.8.216)' can't be established.
ECDSA key fingerprint is SHA256:IJ7FrX0mKSSHTJ63ezxjqtnOE0Hg116Aq+v5mN0+HdE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'bandit.labs.overthewire.org,16.16.8.216' (ECDSA) to the list of known hosts.

                   This is an OverTheWire game server.
           More information on http://www.overthewire.org/wargames

!!! You are trying to log into this SSH server on port 22, which is not intended.

bandit0@bandit.labs.overthewire.org: Permission denied (publickey).

C:\Users\micha>
```

As mentioned in the server's banner, we can't connect because we're using the incorrect port!

Introducing the MAN page - short for manual

When in doubt of using a specific command, make use of the "man" command.

For most commands that you will be using, it provides a very neat and descriptive summary of what that command can do and its options

If you want to find specific information quickly, make use of hitting that "/" key to search specifics

We can apply this to our ssh problem!

```
C:\Users\micha>ssh -p 2220 bandit0@bandit.labs.overthewire.org
```

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

```
bandit0@bandit.labs.overthewire.org's password:
```

www. `---` ver   '---' he   '---" ire.org

Welcome to OverTheWire!

Since this is a rush job, i can't show man here, but it should look cool on your end. WINDOWSSSSS >:()

You're now an elite hacker

🔥🔥🔥
🔥🔥🔥🔥🔥🔥

Not yet, you need more training

And we'll need to make sure that you're already familiar with these commands..

ls

cd

cat

file

man — just covered!!

ssh —- just covered!!

For the first 2 challenges.. we're going to learn a little bit about

FILE DESCRIPTORS
HIDDEN FILES - File system goodies

WTF are file descriptors?