# Hacking labs

**Target device** - browser
**Target audience** - 17-18 teens interested in hacking
**Outcome** - labs and sandbox that provide hands on experience with hacking to systems

## Lab structure

First user is presented with step by step tutorial how to achieve certain goal. Then with this knowledge he has to use it without guidance, in slightly changed enviroment

## Lab 1 - basics of command line

**Learning goal:** Teach how to use commands bellow:

- cd
- rm
- ls, ls -l
- touch
- cat
- vim(maybe)
- ssh

## Final task

SSH into system with default credentials(user: root, password: root) and remove specific file.

## Infrastructure requirements:

- one machine with public ip and ssh enabled

## Lab 2 - DDoS attack

**Learning goal**: show how to create and execute bash(or python) script . Commands needed

- while loop
- ping system call

## Final task

Take down static website server

## Infrastructure requirements:

- one webserver with weak CPU - nginx or something simmilar

# Lab 3 - Http sniffing

**Learning goal:** Show how to capture network traffic and how to interpret the package content

# Final task

Capture network traffic and get password of a user

# Infrastructure requirements

- Server with http website, form with password in the header
- Client sending the http request

# Lab 4 - PHP script insertion

This one I am not sure. Generally in some webpages you can upload your own files, like `.img` files. Instead of uploading a picture you can upload PHP script with `.img` extensions that is executed when presenting webpage. It can do many things, like shutting down the server.

# Final task

The easiest would be to shut down the system, but it's kinda boring. You could also upload the script that creates privileged user and then get into the system.

# Infrastructure requirements

- Server with imgur like website

# Additional requirements

- website that interacts with the rest of devices, with help notes on the same webpage
- server that check user progress