# Junior hacker training

Welcome! You are a junior hacker, who only recently entered the top-secret school of a legendary master hacker, preceded by incredible legends. Today is your first day of field training, and the master will take you to one of his favorite workplaces -- a crowded urban settlement. What makes such a common place really special? A lot of people without the knowledge of information security basics, with dozens of unsecured routers and default passwords, which invite you to visit their local networks.

You are in a car at the urban settlement parking lot. The master brought his laptop with Kali Linux that, together with his advice, you can use in today's outdoor training. The main goal of today's training is simple: to steal anything that can be valuable.

## Disclaimer

This game is for educational purposes only. Unauthorized use of the tools that are incorporated into the game is illegal. The story is fictitious.

## License



## Level 1: Getting to know the environment

**Learning outcomes**:

The player learns to orient in Kali Linux and its tools.

**Task assignment**:

The master handed you a laptop, saying to you: "You studied hard in the past weeks. Now, you are ready for real-world hacking training, but you need the right equipment. In today's lecture, I will teach you using Kali Linux and show you some of its basic functionality, which will make hacking easier.

Firstly, Kali is not just another Linux-based system. It contains many handy hacking tools, which I want you to try today. We can't avoid using Nmap, which is a tool for network scanning: it prints the IP addresses of connected hosts and their running services. But my all-time favorite tools are for password cracking, such as John the ripper, Hydra, or fcrackzip. We will try to find an opportunity for you to try some of them out. When the time is right for using the tool, I'll tell you. If you can't figure out how to use the tool, write the suffix `--help` to get detailed instructions.

Secondly, get acquainted with the command line that you will use to work with Kali Linux. Log in as the user `root` with the password `toor`, look around your file system, and note the arrangement of files and directories. You will need this knowledge when you hack into another Linux machine."

The flag for this level is the command suffix (option) used for printing more information about some tool (there are two possibilities, submit the longer one).

**Estimated duration**:

3 minutes

## Level 2: Looking for server’s IP address

**Learning outcomes**:

The player learns to use nmap tool to scan IP addresses and discover the host's running services.

**Task assignment**:

You already managed to guess the password on a Wi-Fi router with the master's help (12345678, really?!), so you have already accessed the local network of one household. At the same time, you saw the other machines' IP addresses in the router's web UI. There are 2 machines with IP addresses: 10.1.26.4 and 10.1.26.9.

The master told you that your goal is to gain access to the server. Since there 2 machines in the network, scan the hosts and recognize the server's IP address. You can recognize the server by its running services.

The flag is the port number on which the file sharing service is running on the server's machine.

**Estimated duration**:

5 minutes

## Level 3: Connect to the server

**Learning outcomes**:

Player learns how to log in remotely using SSH.

**Task assignment**:

You know the IP address of the server, it was easy, right? Now comes the more interesting part of how to use this knowledge to your advantage. Connect remotely to the server and use legitimate credentials. The master told you that the login details will most likely one of these: admin/password, admin/123456 or admin/admin. It's worth trying, isn't it?

The flag is the entire command for logging into the server.

**Estimated duration**:

5 minutes

## Level 4: Find interesting files

**Learning outcomes**:

The player becomes familiar with the Linux file system and copy ZIP file using SCP.

**Task assignment**:

You are already logged in to the server. Now is the time to find something exciting and ideally compromising, but we don't know exactly what we are looking for. However... do you still remember the list of services running on the server based on the Nmap scan? You already discovered that the server runs the NFS service. NFS protocol is used for file sharing and remote access to files over a computer network. Maybe this server is used to back up data. Try to look whether the admin's home directory stores any files. Then, copy a useful file to your attacker machine.

The flag is the name of the only ZIP file (including the extension) located in the home directory.

**Estimated duration**:

5 minutes

## Level 5: Crack the password to the zip

**Learning outcomes**:

The player learns to crack a ZIP's password using the fcrackzip tool.

**Task assignment**:

You have found out that some accounting company's files have been uploaded to this server. And you have a ZIP file with a promising name in your hands, but unfortunately, it is password-protected. The master advised you that a password cracking tool called Fcrackzip was installed on his Kali machine. Find out how you could break the password and reveal the content of the ZIP.

The flag is the password to the ZIP.

**Estimated duration**:

10 minutes

## Level 6: Disable access to the server for an authorized user

**Learning outcomes**:

The player learns how to change the password to the server machine.

**Task assignment**:

Congrats! You have completed your today's training, and the master praised you as one of his best students. In addition, you gained a folder with prominent invoices, and it's up to you what you'll do with them. But you don't want to just leave without fun. Finally, change the admin's password on the server so that a legitimate user will not be able to access their data.

The flag is the command for changing the password (including username).

**Estimated duration**:

5 minutes