Rules and Grading

You should form teams of 2 or 3 people, and pick a team name. Then have each team member go to \url{http://lacalsrv6.epfl.ch/itse/register} and enter the same team name.

\textbf{WARNING:} do not start solving problems before all team members are registered, or they will be unable to join.

Each lab will consist of a list of tasks, where you will usually be asked to answer with a keyword. Each question starts with a maximum amount of points. The easiest questions start at 55 points, and the hardest go to 500. The first team to answer gets the maximum number of points, the second get one less, and so on, but the value of a question will not drop below 90\% of its maximum value.

You will be asked to provide the answers to the question on the relevant web pages. Go to \url{http://lacalsrv6.epfl.ch/itse/lab} to see a list of labs. Their links will be enabled friday at 15:00, and you will have the whole week to answer the questions, up to next friday 15:00.

If the answer is recognized correct, it will show green, and you will be awarded the points immediately. If it is not correct, it will show red. If it is unknown, it will show yellow; you can either wait for a TA to review your answer, and mark it correct or incorrect, or you can submit something else.

There is no penalty for submitting a few wrong answers and retrying. There will, however, be a penalty for bruteforcing the answers. (Some exercises might require brute force, but not on the answer submission interface.)

For each question you are given a regex matching the correct answer. This
should clear up any ambiguities over the format of the answer (spaces, capital letters, etc...) 

Along with the answer, you may provide a line of comment explaining how you got the answer, the tools you used, etc. There will be many ways to solve each task, and points will be awarded for unique and original solutions you are the first to come up with. There is an incentive to discover your own techniques, rather than just copying from your classmates.

Cheating will be sanctioned with a 0 grade for the week. Here is how we define cheating:

- copying solutions from another groups IS CHEATING
- exploiting an unforeseen vulnerability in one of the exercises, or solving it in a completely different but much easier way, IS NOT cheating (and may give you a better score)
- exploiting a meta-vulnerability in our grading system IS NOT cheating (and will be rewarded as responsible disclosure, if you tell us about it).
- exploiting a denial-of-service vulnerability, or otherwise willfully hampering the ability of other groups to do their work, IS CHEATING.

Work environment setup

Most of the work of the later weeks will take place inside a single VirtualBox VM, itself containing several virtual systems.

Download the virtual machine image here: [http://lacalsrv6.epfl.ch/itse2014.ova.torrent](http://lacalsrv6.epfl.ch/itse2014.ova.torrent) To run the image you need VirtualBox, which is freely available for several platforms at [http://www.virtualbox.org](http://www.virtualbox.org) (Or installable from your package manager if you are running Linux).

The VM is shipped with conservative settings. If you have a powerful and/or recent computer, you can adjust a few settings to make it run better:

- In System/Motherboard, increase Base Memory if you can afford it; cache memory will help reduce disk latencies.
- In System/Processor, increase the number of processors to match the number of cores on your physical machine, or a bit less.
- In System/Acceleration, enable VT-x/AMD-V and Nested Paging if your CPU supports them

Once the VM has booted, you can login as root using the password itse2014.
Working safely

If you feel unsafe about working as root, you may create yourself a regular user.

In any case, remember to snapshot your VM, that will allow you to easily revert to a good state if you accidentally destroy something important.

Starting X

Start the windowing system with the `startx` command. When the task bar shows up on the bottom, open a terminal by right-clicking the background and pick `xterm`.

Keyboard layout

If you need to change the keyboard layout, use the `loadkeys` if you work in text mode, or use `setxkbmap` if you use graphical mode.

Saving your work

For safety reasons, communication between the VM and the outside world is initially forbidden.

If you want your VM to be able to communicate with the outside world, start networking with `/etc/init.d/net.eth0 start`.

You may start an SSH server in the main container of the VM.

Besides SSH, you can also mount a shared folder between your host and your VM, to transfer files back and forth. Mounting it inside the host is left as an exercise. Check the VirtualBox shared folders settings, and use the `vboxsf` filesystem to mount.

Warmup

Now that you are root on the main host, answer the following questions:

- What is the name of the distribution running in the VM?
What is the name of the virtualisation solution running inside the VirtualBox host? At which level does the virtualisation occur? (******-based) Why do you think we used this one?

Can you find the data pertaining to the other machines inside the main host? How many of them are there? Can you find the names of the other virtual machines?

What is the network subnet used by the host and the other machines? Can you map the internal network? What are the addresses used by them?

Crackme (Quite easy)

Download the crackme executable from [http://lacalsrv6.epfl.ch/itse/files/reversel](http://lacalsrv6.epfl.ch/itse/files/reversel). It will require you to enter a password. Your goal is to find the correct password. Any technique will do.

Javascript (Quite easy too)

There is a highly secured web page on [http://lacalsrv6.epfl.ch/itse/js1](http://lacalsrv6.epfl.ch/itse/js1). Break into it, find the correct PIN code. Explain in three words what is in general completely wrong with this approach to security.

Forensics (A bit more intricate)

A malevolent employee has stolen a confidential technology from your company but was caught by an IDS. Identify the technology that was stolen. You may download the capture from from [http://lacalsrv6.epfl.ch/itse/files/forensics01.pcap](http://lacalsrv6.epfl.ch/itse/files/forensics01.pcap)

Hint: you can use wireshark to analyze the trace. Then, you are on your own :D

- Find the username of the thief
- Find the name of the stolen technology