# Pen-testing efficacy human research proposal.

The participants will be given tasks to solve.

## Tasks description

**Scope.**

* Each task will consist of a virtual machine with at most 1 intended vulnerability. Some machines will not have any vulnerabilities. Participants don’t know if they do.
* Participant’s objective is to determine whether there is a vulnerability in the machine and, if he finds it, to obtain a “flag” from the system as the proof of successful exploitation.
* Participant may be given access to the source code, stripped of any comments. Whether he has this access or not is determined at random. This intends to simulate “hacker” and “pen-tester” scenarios.
* Participant will be given access to the service where he can request that the authorised user clicks on a link. This simulates a *social engineering* attack. Using the service to obtain the flag in case when it was not necessary consists a failure.
* Time limit for each task is an hour. Not finding the flag in time results in “there is no vulnerability” response.
* Vulnerabilities were found not to be detected by automated tools. In case they are, their exploitation must be hard to exploit if they are to be added.
* Types of vulnerabilities will correspond to edges controlled by Application security and/or Network security.
* **Each task is solved individually.**

**Measurements.**

* Success/failure.
* Source availability.
* Time taken.
* Used tools.

**Participants**

* Members of Armia Prezesa, 56th hacking team in the world according to CTFtime.org will be invited to participate.
* Members of affiliated teams in the TOP 100 may also be invited.
* £10 compensation, if possible, will be more than enough to gather participants.
* Successful participant will contest at least 5 tasks.