Modular Intrusion Prevention System

Intrusion Prevention Systems are part of the defense-in-depth strategy of computing systems. One popular Intrusion Prevention System is called *fail2ban*. *fail2ban* monitors failed authentication attempts and temporarily blocks traffic from IP addresses that exceed a configurable number. E.g., *fail2ban* can block all traffic from IP address `1.2.3.4` if that IP address tries to log in more than 10 times in one minute.

In this project, you are called to create a modular, alternative, *fail2ban* monitor that can track failed authentication for SSH and for the administrative panels of `Joomla`, `WordPress`, and `phpMyAdmin`. Your tool should also have a web interface that an administrator can use to change the configured thresholds (`X` requests in `Y` minutes, blocked for `Z` time), view which clients and IP addresses are currently blacklisted, and remove blacklisted IP addresses.

Reporting

The project will have a final report. In this report, the project will be described as a scientific article. Each article must be 8 pages long (without the bibliography and appendices). The article must be written in `LaTeX` and it should follow the IEEE conference template. Finally, the submission of the article must be in Portable Document Format (.pdf). Ensure that you have a uniform style of writing.

This report should contain the following sections:

- ***Abstract:*** Usually less than 150 words.
- ***Introduction:*** Here the problem is explained, the research in this report is placed in the existing literature and in terms of state of the art, requiring a literature study.
- ***Background:*** You provide the knowledge that a non-familiar with the topic reader should have in order to follow up with your article.
- ***Methodology:*** You describe your approach.
- ***Experiments:*** Describe what you want to find out and how and why you have designed your experiments
- ***Results:*** A *dry* expose of the results of your experiments, including proper statistical analysis
- ***Discussion:*** You interpret the results of your experiments and place them in terms of what is known from the literature.
- ***Limitations:*** You mention the limitations of your work and how this can be improved in future work.
- ***Related Work:*** You describe articles that perform significant research in the area of this article.
- ***Conclusions:*** You draw your conclusions from your research and answer your research questions
- ***References:*** In your report, you should always cite if you are using ideas, methodologies, or software from others.

All teams should give a 15-minutes presentation, including a live demo!!!