- **Check if all the requirements from the template have been covered.**
  - Conclusion and Discussion is missing. Also vulnerability Scanning 2.3 is missing the table of "information about open ports".
- **Is the report written in a clear voice? Is it easy to follow?**
  - No, the report needs some fixing here, spelling, word order. Read through it thoroughly and fix these mistakes
- **Introduction:**
  - **Is the purpose of the report clear?**
    - Yes. The introduction is a bit casually written tho. The "word" "BAAAM" should not be used in a technical report. And the rest of the introduction is on the border to to informal language.
  - **Is it clear what is contained in this report?**
    - Yes. However we would like to see something that is not just another table of content. Maybe some description on what we will read about in the different chapters.
- **Description of OpenVAS setup**
  - We think this is well written. We would however like to see some of the content moved to other parts of the report. In chapter 2 you talk about fingerprinting and then you talk about fingerprinting in 2.2 and 2.3. Same for port scanning. So we think that you could move some of the information from 2.0 to 2.1, 2.2 and maybe 2.3.
  - We notice that you introduce the abbreviation OVAS and then you use openVas throughout the report instead. Decide on what you want to write. Compared to NVT that you present and then use throughout the report which is very nice for the reader.
  - In 2.2 you could swap the order of the paragraphs and merge them to one.
  - **Does the report explain the different components of the vulnerability assessment system used?**
    - yes.
  - **Does the report describe the scans that are performed (their configuration) and also a motivation for choosing them (what is their aim)?**
    - yes.
  - **Is it possible to repeat the scans (for result validation) based on the information presented here?**
    - Yes,many good pictures and information about what was used for the scan
- **Presentation of results**
  - This seems like a bit of work in progress and is not as polished as the start of the report. All references (to figure/table) are wrong. Lacking some tables.

- ○ In the end of results, 3.3 you meantion that you have 5 high security flaws but you list 6 things as main threats, this is a bit confusing but can probably easy be changed so that it is more clear and would then be a really good asset to the report.
  - ○ **Does the report contain results (most important ones) for each of the scans performed?**
    - ■ Mostly. Miss some tables.
  - ○ **Is there enough information describing the results in the report?**
    - ■ No. We would like to see some more information on open ports.
- ○ **Discussion of results**
  - ○ **Does the report contain a detailed discussion of most of the results obtained (at least for the most important ones)?**
    - ■ no
  - ○ **Are the suggestions and decisions properly motivated?**
    - ■ -
  - ○ **Are the initial recommendations updated (with the help of new results and findings)?**
- ○ **Conclusions**
  - ○ **Are the main findings of the report highlighted?**
    - ■ -
  - ○ **Do the authors present a strategy (a short list of actions) that can be followed to better secure the system?**
    - ■ -
- ○ **References**
  - ○ **Are the external sources used in the report properly referred to?**
    - ■ Yes.
- ○ **General**
  - ○
  - ○ **Are the figures and tables properly used and referred to?**
    - ■ Check all your references to figures, it seems like some are not working as you want. E.g. as in table ??.
    - ■ You don't have any tables only figures so done reference tables.
    - ■ Figure 6 and 7 are the same.
  - ○ **Grammar/structure of paper?**
    - ■ Needs a little work. Some grammatical errors. We think this can be solved if you proofread one extra time before sending it in.
  - ○ **Spelling errors (we hope all authors will use a spell checker before submitting the report, but please also comment if that is the case)?**
    - ■ A few spelling mistakes. Needs to be re-read.