# Malware Analysis Project

1. Weightage: **40%**
2. Groups of **max 4 people** per group.
3. You choose group and name group based on APT malware name. Any name is fine.
4. Your instructor will have intermittent meetings with the group. During those meetings you will present your network diagrams and a tools list and talk about your progress. You will receive a mark associated with these meetings which will be added to the final project grade.
5. You will need to do a presentation of your project to the class. You will need to do a PowerPoint presentation.
6. Reports will be submitted (the format to be provided to you).
   1. Who is on the team
   2. Sample chosen
   3. Environment setup
   4. Screenshot showing all relevant data to back up your analysis
   5. Tools used
   6. Final Report to include:
      1. The output of the tools
      2. Will show why you changed tools if you made a change.
      3. Errors and strange behaviors
      4. How you resolved these problems or workarounds implemented.
      5. Show clearly the static and dynamic analysis process and how the 2 approaches to determine the results found.
7. Have to prepare a new VM.
   1. This should be separate from current projects/machines. To eliminate possibility of contamination
8. Manual testing vs Sandbox
   1. You are required to do both Manual analysis and sandbox analysis
   2. No online sandbox, but you can use something like Cuckoo or another offline sandbox.
      1. This shows how to test automation
9. Choose 1 sample/group – don’t go crazy.
   1. Do some research and find a sample you can manage at your level of understanding
10. Due date **Aug17, 2025**.
11. Websites for samples and configuration documentation are show below. You can choose another sample but be mindful of the time it takes and the effort required to complete the process. Make it challenging (**PLEASE BE CAREFUL THESE SAMPLES ARE DANGEROUS**).
    1. <https://github.com/topics/malware-samples>
    2. <https://www.malwaretech.com/2017/11/creating-a-simple-free-malware-analysis-environment.html>
    3. <https://www.alienvault.com/blogs/security-essentials/building-a-home-lab-to-become-a-malware-hunter-a-beginners-guide>
    4. <https://oalabs.openanalysis.net/2018/07/16/oalabs_malware_analysis_virtual_machine/>
    5. <https://www.sans.org/reading-room/whitepapers/threats/malware-analysis-environment-design-artitecture-1841>
    6. <https://github.com/a0rtega/pafish>
    7. <http://byte-atlas.blogspot.com/2017/02/hardening-vbox-win7x64.html>
    8. <https://blog.christophetd.fr/malware-analysis-lab-with-virtualbox-inetsim-and-burp/>