# Research Assignment

# Hardware Vulnerability with Proof of Concept (PoC)

## Grade Value

* 10% of total grade.

## Guidelines

* You are allowed to reference the course materials and online content to complete the assignment.
* The PoC should be completed in a virtual machine, either Windows or Linux; whichever you would prefer.
* This report should be at least 8 pages long to cover the concepts.
* The PoC video should be 1-3 minutes long.
* This assignment should take an estimated 6 hours to complete.
* This assignment will be due 3 weeks from the assigned date.

## Requirements

* The PoC video must be provided in a format playable by [VLC media player](https://www.videolan.org/vlc/)
* The report must include a title page, a table of contents page, and headings for each section of the report.
* The report must include page numbers in the footer, the title of the report in the header, and your last name in the header.
* The document should use font size 12 with 1-inch margins
* The document should use the Arial or Calibri font
* This assignment will be completed solo
* References are required, refer to APA formatting citation guides at <https://library.nait.ca> or others guides online
* Microsoft Word is recommended to produce the report
  + Refer to the guide from NAIT ITS at <https://its.nait.ca/it_services?id=isd_kb_article_view&sysparm_article=KB0017926>
  + When logging into the Microsoft portal or Word, login with your @nait.ca account, unless you already have Microsoft Word through a personal or business account

## Assignment

* Research [a](https://meltdownattack.com/) recent hardware vulnerability, for example Meltdown which is an exploit for modern processors, and build a report on how the exploit works, what is/was vulnerable, and how to prevent exploitation from taking place. Once you have built the report, create a PoC on a virtual machine and record a demo of the attack taking place.
  + The resources section of this assignment will include various publicly available resources that can be used to execute this exploit
  + An example of PoC can be found on the 2nd link under resources (github) for Meltdown

## Resources

* <https://meltdownattack.com/>
* <https://github.com/IAIK/meltdown>
* <https://www.grc.com/inspectre.htm>
* <https://unix.stackexchange.com/questions/554908/disable-spectre-and-meltdown-mitigations>
* <https://superuser.com/questions/1283619/how-to-turn-off-kpti-to-improve-performance-in-fedora>
* <https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown/MitigationControls>

## Submission

* Report should be saved in .PDF or .docx file formats
* Video should be saved in .MP4 or other VLC-playable formats
  + If the file is too late to upload into Brightspace it will need to be transcoded using an application like Handbrake (<https://handbrake.fr/>) before uploading
* PoC/exploit code should be saved in its native format (.c, .py, etc.)
  + If Brightspace blocks the upload, compress into .7z, .zip or .tar
* Assignment file must be uploaded to the Brightspace assignment page prior to the due date.
* Late submissions will not be accepted

## Marking Rubic

Rubic is posted in Brightspace under the assignment

Screen Recorder:

<https://www.youtube.com/watch?v=xoe9ZOzlfnQ>

part of it demonstrating the PoC – can use tech jardon ot not.

Report, POC, code is a separate file each.

For Physical vulnerability assignment #2:

* shodan.io
* https://edmontontrafficcam.com/