ZEIT8020 S1 2023

Assignment 4: Practical Project

This is the fourth assignment, and it is worth **40%** of the total course grade. The assessment will evaluate your ability to understand and apply cyber offense concepts and tools (tradecraft) on a target of your choice. You will execute all steps in the cyber kill chain that can be legally executed against that target, such as passive reconnaissance. You will provide documentation that explains all steps you have taken, the strategies you have taken, and the outcomes.

You will also document and explain all additional steps you would have taken if you were not bound by legal constraints. One way to investigate and research these steps is by emulating the computer environment of the target by means of designing and creating Virtual Machines (VMs), virtually network them on a closed system, and execute the steps, i.e. much like you have done on the Cyber Range when doing Assignment 1. Another way is to formally agree with the target which actions you are allowed to take, and which not, i.e. somewhat like a penetration tester. Yet another way is by purely theoretic analysis. That is all up to you, as long as it serves the aim of the assessment well.

Choosing a target

The documentation must include a description of the target you chose and, possibly after having done some initial reconnaissance, the goal you want to achieve. It is strongly advised that you choose a challenging target/goal combination, as only then one or more successful exploits will optimally display your learning from the course. Explain why you have chosen this target/goal combination. If in doubt about the suitability of a target/goal combination, speak to your course convener.

In case you need permissions from the target, provide evidence of these permissions in the documentation. Properly research what you can and cannot do without permission. If, after having done your research, you are still in doubt, ask advice from the course convener. In any case, UNSW is NOT encouraging its students to perform illegal cyber offensive activities. The student bears responsibility for their actions.

Aims

The practical project must show how much the author learned about:

LO1. Conduct simple cyber offensive operations, *LO2.* Identify opportunities in defeating cyber threat actor tradecraft by understanding the full spectrum of offensive activities,

LO3. Improve an organisation’s security by understanding and acting on artefacts and signatures generated by cyber offensive activities,

LO4. Provide advice to policy makers on strategic issues regarding cyber capabilities, doctrine, and partnerships.

Constraints

Formatting your submission is your choice. It should at least contain a technical report which at least contains:

- An executive summary of <u>no more than 300 words</u>
- An introduction
- A description and justification of chosen target and goal
- A description of the chosen strategy / approach
- Results of your activities
- How does your work relate to the course material
- Conclusions
- References

The report may contain any further analysis of your findings and alternative approaches, and it may contain a variety of appendices, e.g. a copy of your note takings, screenshots, or VMs. **The maximum wordcount for the report is 3500 words** excluding Executive Summary, Figures, Tables, References, and Annexes. Anything above this wordcount will not be marked. The wordcount is a maximum wordcount, not a recommended wordcount. Conciseness will be rewarded.

Hints

- Choose a target-goal combination close to your interests and experience, for instance related to the topic of your Discussion Essay.
- An executive summary is not the same as an abstract. This assignment asks for an executive summary. See also the assessment guideline of Assessment 3.
- The introduction should include a clear scoping of the document. What is discussed and what is not, and why? Narrowing the scope of your document provides the space to tackle the chosen topic in more depth. However, narrowing the scope too much may limit you in displaying how well you master the breadth of the course material (see Aims).
- The introduction should also explain how the remainder of the document is structured.
- The conclusions should not contain any new material. They should just summarize what you conclude from your analysis.
- Use the APA referencing system for your citations.

Assessment

Assessment of the essay will be based on the assessment criteria guide as below:

- <u>Quality of the Executive Summary: 6 marks</u>
    - Is the Executive Summary comprehensive, easy to read, and convincing?
- <u>Introduction: 4 marks</u>

  - Does the introduction introduce and scope the executed work well, and introduce the remainder of the document well?
- Suitability and feasibility of the scenario: 12 marks
  - Is the scenario presented realistic and a representation of a legitimate organization and threat actor?
  - Is the background and context of the target, the goal, and the chosen strategy presented in sufficient detail to allow the reader to understand why the threat (or threats) exist(s) and that the chosen approach is feasible?
- Complexity and diversity: 20 marks
  - Does the author make effective use of a variety of tactics, techniques, and tools understood throughout this course?
  - Are the phases/steps applied distinct and well understood?
  - Does the author show understanding of the target's defenses, and can they realistically circumvent them?
  - Does the author show understanding of tradecraft to prevent detection?
- Quality of the conclusions section: 5 marks
  - Does the author provide a comprehensive set of valid conclusions that follow from the analysis in earlier sections?
- Writing style: 4 marks
  - Is the documentation well structured? Is information presented in a logical manner?
  - Does the author write succinct? Is information presented in a brief and accurate manner? Are references used correctly?

Submission

This is an individual assignment. The report must be submitted via the appropriate submission link provided on Moodle. The due date is **Friday 9 June 11.55 pm** Canberra time. In case the scenario is emulated with VMs, upload the VMs to your dedicated OneDrive storage, and provide a description of and links to them in the report. The same can be done with other appendices that require lots of storage capacity, e.g. videos. Another storage provider you can use is CloudStor.

The penalty for late submission will be 5% per calendar day, or part thereof, unless prior special consideration has been granted. Assessment items submitted more than 5 calendar days late will not be assessed and will receive a grade of zero. All requests for special consideration must be formally submitted via MyUNSW prior to the assessment due date.

Grading Criteria

For all scholarly assignments in this course, the grading criteria are qualitative in nature and based on the educational theory propounded by Biggs & Tang (2011)*.

High Distinction (HD) : 85-100%
The very best work that can be expected: beyond the level of a Distinction. The student chose a very challenging target-goal combination. The student shows an understanding of cyber offensive strategies and a mastering of tools and techniques that go in depth and breadth well beyond what has been presented in the course material. The student displays a high level of creativity and originality in the approach taken.

Distinction (DN): 75-84%
Distinguished understanding beyond the level of a Credit. The student chose a challenging target-goal combination. The student shows a deep understanding of cyber offensive strategies, tools and techniques as presented during the course, and shows that they can apply this knowledge and skills in a concerted fashion. The student shows some creativity and/or originality in the approach taken.

Credit (CR): 65-74%
Highly satisfactory understanding evident. The student chose a reasonably challenging target-goal combination. The student shows mostly correct understanding of cyber offensive strategies, tools and techniques as presented during the course, and shows, in some breadth and depth, that they can apply most knowledge and skills to achieve the goal, if not in a concerted fashion.

Pass (PS): 50-64%
The student chose a somewhat challenging target-goal combination. The student demonstrates an acceptable level of understanding of various cyber offensive strategies, tools and techniques as presented during the course. The student mostly shows that they can apply this knowledge and skills to achieve the goal.

------
*) Biggs J. B., Tang., K., Teaching for Quality Learning at University, 4th ed. Open University Press/McGraw Hill, 2011