Swinburne University of Technology

COS30015 Assignment 1

This assignment is worth 40% of the subject assessment.

Due Date: 5th Sep at 23:59pm

Introduction

This assessment requires students to develop a deeper understanding of cyber security threats from both an attacker and defenders' perspective. In addition to learning further about offensive and defensive security, it also requires students to engage in industry leading frameworks (such as MITRE ATT&CK and the ACSC's Essential 8).

Students are required to consolidate and develop practical application of learning outcomes, applying skills through case study analysis, design and planning, categorisation, analysis, and evaluation of tools, TTPs, threats and procedures.

ALL topics should be done in a virtual environment, without Internet access and attempted safely. **Do not use any commercial services or Internet apps. Do not run or complete any tasks on your host device and should not impact other devices outside of your virtual lab**. Again, do not use the Internet, real or live malware, live systems or applications on the Internet (Email for example), only within virtual machines. You may use lab virtual machines or build your own to complete the assignment. Talk with your tutor if you need clarification.

Attack & Security Tools

Topic overview: You are required to choose ONE attack and ONE security tool from one of the following topics. You need **ONLY** complete **ONE** topic:

- Authentication
- Resource Hijacking
- Malicious Software/Activity
- Sniffers
- Denial of Service

Requirements: You will need to research ONE tool attacker's use (offensive), and ONE security tool used to counter or detect attackers in the area chosen (defensive). Your assignment involves **running both tools**, evaluating and analysing their use in means to **evade or detect** threats/detection. That is, how are you going to use these tools? To show how attackers can bypass detection, or how tools can be used to detect/restrict this threat type? Or show how both operate? From this perspective, you should perform a case study of your

chose area outlining the threat, table and justify your choice of tools (over others), determine metrics used to determine how effective the usage from your viewpoint is, outline your testing scenario and what MITRE TTPs will be used. Then install, run and demonstrate the use of tools, producing some output or results from both offensive and defensive positions. You should analyse the results (best run the tools once and show what happens when security controls are not in place, the apply the security controls and run again). Finally, evaluate the usage and results from both attacker and defender perspectives, and potential impact, discussing Essential 8 mitigations, and comparing your scenario TTPs against similar threats.

Key steps:

- Determine which threat type you choose
- Perform a case study outlining the background of this threat, typical adversary trade craft, the potential impact for an organisation
- Justify your threat choice
- Compare attacker and defender tools for this threat type, evaluating them of a criteria of your choice (e.g., ease of installation, complexity, amount of documentation and support, what the tool can do), choose your two tools and justify your choice
- Propose a testing scenario, outline what will be done, which tools will be use (e.g., run attacker tool against web server doing Syn Flood without a Firewall, then deploy said Firewall and configure rules which mitigate a Syn Flood)
- Map this testing scenario to MITRE TTPs
- Outline metrics which specify a win for either the attacker tool or defender's tool
- Deploy your environment, run your scenario, record your output
- Analyse your scenario and what happened before and after you applied your defenders' tool
- Evaluate this scenario, is it a win for the attacker or defender
- Outline any Essential 8 mitigations which apply to this scenario given the potential impact
- Highlight the TTPs contained within the scenario against similar threats using MITRE ATT&CK Navigator and outline briefly the commonality

References

All externally sourced information (i.e. not common knowledge or course material) must be cited. Referencing conventions required for this unit is the IEEE referencing style. See https://ieeeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf

Helpful information on referencing can be found at https://www.swinburne.edu.au/library/referencing/

Each citation must have a corresponding reference at the back of the report. ALL REFERENCES MUST BE CITED. There is no minimum requirement for the number of references.

Amount of work

Each student is required to spend a minimum of 30 hours on the assignment. You are encouraged to maintain a logbook to document your project progress.

Marks will be allocated depending on the amount of original work submitted. 0 Mark will be given for plagiarised and/or un-attributed work. eForensic examination of the assignment will be carried out to verify its authenticity.

Submission

Submissions should be made **through Canvas** before the due date. ***Late submissions*** will be **penalised** by **10%** per day (for 5 days maximum), submissions which are 5 days after due date will not be allowed and 0 mark will be given.

- Reports must be in the commonly used **PDF** document format (.pdf) and should **not exceed 15 pages** in length.
- The **first page** should contain a filled-in copy of the **cover sheet** available on Canvas.
- The second page must be a **title page**, which includes:
    - The unit code and title,
    - The name of the assignment,
    - The topic,
    - The author (name and student ID),
    - The submission date/time,
    - The due date/time.
- **Pages must be numbered** starting with the first page AFTER the cover sheet and title page.
- A table of contents is **NOT** to be used
- The word count is defined at ***3,500 words (+- 10%)***.
- **Appendices** and a list of **references** are **not to be included** in the page count.

Misc

- It's best to avoid quotes, so write without them
- If you change words around to get around Turnitin you still might receive 0 marks. It's best to write in your own words
- A **Turnitin score of 10** is the maximum allowed
- Any submissions with photos to avoid detection will result in an instant 0
- Photos of others writing, tables will get 0
- Images used from others work will get a mark of 0, best make your own diagrams
- Writing about industry technology, giving the strengths and weakness of things will score very low
- Don't just give screenshots of you using tools, it's ¼ of the work required

- **<u>Again, don't just run some tools and not write anything else for the other sections, this is not enough to pass</u>**
- **<u>Again, see above. You need to do a case study, evaluate and map things out, run the tools from both perspectives and then evaluate the result.</u>**

<u>Grading and Rubric</u>

This assignment will be graded as Fail, Pass, Credit, Distinction or High Distinction. Note that minor deductions may be made for small errors in content or style.

Performance Levels/ Criteria	**N (0–29)**	**N (30–49)**	**P (50–59)**	**C (60–69)**	**D (70–79)**	**HD (80–100)**
<u>Criteria 1: Planning and Justification</u> Scenario, choice of tools, threat/topic choice	There is little to no evidence of understanding the security challenges, tools, threats and where they exist within the cyber security landscape.	Marginal evidence is given, with some basic justification.	Moderate evidence, considers the landscape and relatedness to modern challenges and relevance.	Well-presented justification with examples. Moderate consultation of the landscape considered. Topic, tools, scenarios presented logically.	Significant level of justification has been provided with relevant examples. Significant consultation of the landscape considered through reference. Topic, tools, scenarios presented logically.	Case study provided. High level of justification has been provided with relevant examples. Landscape challenges have been highly consulted through reference, needs outlined and choice of tools, scenarios and topics argued well. Links to TTPs, metrics have been defined.
<u>Criteria 2: Application and Documentation</u> Running of tools or solution, analysis software, etc., and the knowledge, security aspects. Assignment documentation as a whole	Minimal application of tools etc. With little documentation and explanation. Report is of a low standard.	Basic application of tools etc. With basic documentation and explanation. Report is of a basic standard.	Moderate application of tools etc. With moderate documentation and explanation. Report is of a good standard.	Well-presented implementation of tools or analysis. Both attacker and defender knowledge has been outlined. Report is of a moderate standard.	Highly documented implementation of tools or analysis. Attack, defence and impacts have been explained behind tools, analysis. Report is of a high standard.	In-depth documentation and high functionality configured. Leading tools have been chosen and working. Security functionality usage (Goodware/Malware) is discussed in-depth. Report of is excellent quality.
<u>Criteria 3: Analysis</u>	A low-level of analysis is presented.	Basic analysis is presented.	Moderate analysis is presented.	Well-thought-out analysis is presented.	Highly thought-out analysis is presented.	Excellent analysis is presented.

Understanding the results achieved, analysing the impact/use/practicality/ etc.	Concepts, impact, challenges and considerations are brief, or not given.	Concepts, impact, challenges, and considerations are basic, with some detail.	Concepts, impact, challenges and considerations are well considered, with good detail. The student has demonstrated moderate knowledge to analyse Criteria 3.	Logical in nature, covering both attacker and defender concepts, impact, challenges and considerations. These have been giving moderate depth. The student has demonstrated a good level of knowledge to analyse Criteria 3.	Connections are made across the topic and security landscape. The analysis has been linked to aims. Both attacker and defender concepts, impact, challenges and considerations were presented. These have been given considerate depth. The student has demonstrated a high level of knowledge to analyse Criteria 3.	Thorough and high evaluation of tools, threats, challenges, usage, results is given. The analysis is linked to aims, discussing the results obtained given configurations and usage. The student has demonstrated excellent level of knowledge to analyse Criteria 3.
Criteria 4: Evaluation Effectively judge/critique/summarise the result, challenge, usage Outline mitigations and potential impact of the scenario Compare TTPs and/or threat/need within the security landscape	Little to no evaluation is given. Project relies more on demonstrating common knowledge of tools, threats, challenges, results.	Simple evaluation is given. Project has more demonstration of common knowledge of tools, threats, challenges, results.	Evaluation of activity, threats, challenges, results is given. Basic insight is provided and judged.	Moderate evaluation of tools, threats, challenges, usage, results is given. Some depth and contrasting are provided. Some support is given. Essential 8 mitigations and risks are discussed at a basic level, along with mapped TTPs.	Good evaluation of tools, threats, challenges, usage, results is given. Depth is shown, and contrasting and consideration is provided. Moderate support through reference is given. Essential 8 mitigations and risks are discussed, along with mapped TTPs.	Both attacker and defender concepts, impact, challenges and considerations are compared and contrasted. These have been given considerate depth while linking TTPs, Essential 8. Connections are made across the topic and security landscape, along with future challenges. Essential 8 mitigations and risks are discussed in depth, along with mapped TTPs.