Swinburne University of Technology

COS30015 Assignment 2

This assignment is worth 40% of the subject assessment.
Due Date: Thursday the 31 of October 2024 at 23:59

The assignment

This assessment comprises of **THREE** components:

- **Component 1 Incident Forensic Analysis** (15 marks)
- **Component 2 Incident Situational Report** (10 marks)
- **Component 3 Review of Literature** (10 marks)

The following provides a high-level description and task breakdown for each component.

Part A Incident Forensic Analysis Component

Description

You are required to forensically analyse artefacts provided by Starfleet to answer a series of questions. These questions help you piece together the **incident attack path**, identify **IoC** and **TTPs**, along with **assets** and **users** impacted. This allows you to provide a **summary** of events. To achieve this technically, you should make you of the labs and supplementary lecture content from week 6 onwards. You should also investigate via the Internet any additional information required. (PS: Given the project requires you to consider multiple artefacts which require investigation, resources like OpenAI will not assist. It could be used to complement your theoretical knowledge.)

Completing this to the best of your ability will assist with components 2 & 3. This scenario is fictitious, and no domains, IPs and malicious files should be interacted with in any form. All persons within the scenario are personas and not real entities, nor the target organisation.

Breakdown

- Refer to supporting files
    - **Assignment 2 Part A**
    - **samba_log.csv**
    - **DC.log.txt**
    - **memory_2024_Sep_12_215606.raw**
    - **Assignment 2 Part A Template**
- Read and understand each portion of the component, either in full or each portion sequentially and,

- Answer each portion's questions in the provided template (**Assignment 2 Part A Template**)
- Often this is to be a simple answer, such as an IP, domain, account, event, or a brief description
- There are no long answers
- Keeping track of the events in a timeline is suggested to assist with Component 2

Submission

- **Assignment 2 Part A Template**

Rubric

Description	**Great**	**Good**	**Basic**
Base questions [12 marks] answered correctly	1 point awarded per question (45 in total) – scaled between 0 and 12 marks		
HD attempted questions [3 marks] answered correctly	6 points awarded per question (4 in total) – scaled between 0 and 3 marks		

Part B Incident Situational Report

Description

You are required to take your findings and answers from Component 1 and write a Situation Report of the incident. It is meant to be a snapshot in time, reflecting an accurate and factual summary of the situation. Use the template provided, and again this does not need to be a lengthy in words, rather, capture the exact specifics which help relate the situation. The target audience can be considered a manager who is receiving an update. You will be able to also draw upon weeks 1 to 6 to assist with this.

Breakdown

- Use the provided template, refer to supporting file **Assignment 2 Part B Template**
- Either list or write a summary of your findings in the appropriate section(s)
- Keep in mind there is **no work count**, be mindful of ***who you are writing*** (a ***manager*** requiring an informative update)

Submission

- **Assignment 2 Part B Template**

Rubric

Description	Great	Good	Basic
Accounts **[1 mark]**	All impacted accounts identified	More than 50% of impacted accounts identified	Some impacted accounts identified
	1 point	0.5 points	0.25 points
Timeline **[1 mark]**	Incident timeline is accurate	Incident timeline is mostly correct	Incident timeline is partly correct
	1 point	0.5 points	0.25 points
Hosts **[1 mark]**	All impacted hosts identified with an appropriate impact severity	More than 50% of impacted hosts identified with an appropriate impact severity	Some impacted hosts identified
	1 point	0.5 points	0.25 points
IoCs **[1 mark]**	All IoC identified and their category (e.g., IP, Domain, Hash, Account, etc.)	More than 50% of IoCs identified	Some IoCs identified
	1 point	0.5 points	0.25 points
TTP **[2 marks]**	All TTPs identified	More than 50% of TTPs identified	Some TTPs identified
	2 points	1 point	0.5 points
Remediation advice **[4 marks]**	Remediation advice describes appropriate controls and mechanisms to remove, block or alert from the identified TTPs Recommendations are logical given the TTP remediation is being provided from	Remediation advice describes more than 50% appropriate controls and mechanisms to remove, block or alert from the identified TTPs Recommendations are logical given the TTP remediation is being provided from	Remediation advice describes some appropriate controls and mechanisms to remove, block or alert from the identified TTPs Recommendations are logical given the TTP remediation is being provided from
	4 points	2.5 points	1.5 points

Part C Review of Literature

Description

Having performed forensic analysis and consolidated your findings, you will review emerging technologies in which to defend against similar incidents. You will write an academic literature review from well respected cyber security conferences and journals.

The following links provide reference to the allowed journals and conferences only:

Conference:

- https://www.ndss-symposium.org/
- https://www.usenix.org/conference/usenixsecurity24
- ttps://www.sigsac.org/ccs/CCS2024/
- https://sp2025.ieee-security.org/

Note: the 2024 website has been provided for these conferences where there may be no literature available for this year, please look at previous years

Journals:

- https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9739
- https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6221036
- https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206
- https://dl.acm.org/journal/tops
- https://www.sciencedirect.com/journal/computers-and-security

Research Questions

You will be required to write your literature review in answering the following research questions

- ***What are the current trends to detecting and mitigating cyber threats like or closely related?***
    - Think – it uses machine learning, honeypots, statistics, a new log processing technique, etc.
- ***What data features are being used to aid detection or mitigation?***
    - Think – Are event IDs used, or the number of connections, etc.

You should **review** at least **10 papers**, but you can use any number of papers from the same sources for other requirements (such as explaining concepts or linking theories). The review should be a total of **2,000 words (+/- 10%).** Appendices and a list of references will not be included in the page count.

The following structure is required (rough word count given):

- Introduction (100 words)
- Approached to current trends (700 words)
- The use of features (700 words)
- Discussion (500 words)

A note about the discussion. You should evaluate the reviewed trend/feature literature and whether it is really applicable. Does the research approach work with any data and a broad range of threats for example, or does the data require lots of steps to be processed, or does it only work in a narrow focus. Think – would it work off the shelf and would applying this research be tricky and specific?

Breakdown

- Take your identified threats and TTPs and look for relevant literature
- Read, review literature, record interesting information about trends and features
- Likely record your information in a spreadsheet to help you organise it
- Write your review
- Keep in mind that it can only be from the provided sources and there is a word count

Submission

- **Literature Review with the first page as a cover letter.**

  The first page should be a filled-in copy of the **cover sheet** available on Canvas.
  - The second page must be a title page indicating:
  - The unit code and title,
  - The of the assignment,
  - The topic,
  - The author (name and student ID),
  - The submission date/time,
  - The due date/time.

Rubric

Description	Great	Good	Basic
Introduction [1 mark]	Introduction outlines the threat(s) and what the review is attempting to achieve by reviewing next-generation methods to detect, mitigate or	Introduction outlines the threat(s) and basic aims	An introduction is provided

	disrupt cyber attacks		
	1 point	0.5 points	0.25 points
Research Q1 **[3 marks]**	-Great attempt is provided to answer the selected question 10 or more references are used -Parallels are drawn between different papers -Trends, methods and challenges are discussed	-A good attempt is provided to answer the selected question 10 references are used -Parallels are drawn between different papers -Trends, methods and challenges are discussed	-Basic attempt is provided to answer the selected question -Less than 10 references are used
	3 points	1.5 points	0.5 points
Research Q2 **[3 marks]**	-Great attempt is provided to answer the selected question -10 or more references are used -Parallels are drawn between different papers -Features, data and challenges are discussed	-A good attempt is provided to answer the selected question -10 references are used -Parallels are drawn between different papers -Features, data and challenges are discussed	-Basic attempt is provided to answer the selected question -Less than 10 references are used
	3 points	1.5 points	0.5 points
Discussion **[3 marks]**	Demonstrates an great ability to engage deeply with the literature, offering insightful analysis and synthesis of the information Critically assess the strengths and weaknesses of research question findings	Demonstrates an good ability to engage with the literature, offering analysis and synthesis of the information Assesses the strengths and weaknesses of research question findings	Provides basic insights and draws appropriate conclusions
	3 points	1.5 points	0.5 points
Language and word count/Formatting **[3 marks]**	- Writing is of a high standard, academic language used, proofed, logical flow -Word count correct or within +/- 10%	-Academic language used, proofed, - logical Word count correct or within +/- 10%	-Writing is coherent but has minor grammatical errors or discussion inconsistency -Word count correct or within +/- 10%
	3 points	2 points	1 point
References	References greater than 10 for the actual literature	References are below the required 10 for the actual	References are below the required 10 for

[2 marks]	review IEEE style used	review IEEE style used	the actual review
	2 points	1 point	0.5 points

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 should spend at least 30 hours working on the assignment. You are encouraged to keep a log book for your project.

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 https://swinburne.instructure.com/ (Canvas) before the due date. Reports should be in commonly used PDF document format (.pdf).

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.

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