Swinburne University of Technology
Faculty of Science, Engineering and Technology

COS30015 IT Security Assignment

This assignment is worth 40% of the subject assessment.
Due Date: Sunday the 30th of October 2022 at 23:59pm

Introduction:

Any IT graduate involved in IT security will need to be able to adapt and respond to unfamiliar and changing security threats and to evaluate and use new tools. To be capable in their profession, graduates need to be able to **apply** skills through **design** and **planning**, **categorisation**, **evaluation** and **analyse** of tools, techniques, threats and procedures.

The assignment:

Choose ONE topic only from the following study areas:

Attack & Security Tools

Select one of the following topics and choose 1 attack **and** 1 security tool:

- Trojans and Backdoor
- Viruses and Worms
- Sniffers
- Phishing
- Denial of Service
- Buffer Overflows

You will need to research 1 tool attacker's use, and 1 security tool used to counter attackers in the area chosen. 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 this threat type? Or show how both operate? From this perspective, you should justify your choice (over others), install, run and demonstrate the use of tools, producing some output or results. You should analyse and evaluate the usage and results from both attacker and defender perspectives, and potential impact. Be sure to discuss threats and countermeasures of these risks.

Device Hardening

Select one of the following topics:

1. Lock down a PC which would be connected to the Internet
2. Design and test a home security lab (locking down multiple devices found at home)

There exist many different guides to harden devices. You are required to follow one (of a reputable source) and evaluate its effectiveness. You should choose a hardening guide, and outline a use case and example scenario (that is, what needs to be locked down given what threats). This device should be locked down following best practices of the guide. **You then are required to evaluate the effectiveness of the guide** in using a range of tools found in Kali Linux or other well regarded tools. You should justify your guide and attacker tools, analyse and evaluate the hardening strategy and results.

Vulnerability Analysis or Exploitation

Select one of the following topics:

1. Prepare and test detailed instructions for modifying a game console
2. Audit the memory management of a complex C or C++ program. You should use buffer-overflow detection software for this

These choices allow you to recreate known modifications, attack, or construct a use case for vulnerability exploration. You should document the implementation of a modification, paying close attention to explaining and analysing the techniques. Or, you should document the challenges, application and effectiveness of auditing memory management. For either of these, you should link security and computing theory to practical application for evaluation. You are required to document and analyse the impact of either, evaluate countermeasures and the practicality of either (modification or exploration).

Attacker or Malware Analysis

Select one of the following topics:

1. Using scripts and web services, trace (over 50) spam e-mails to their source as best as you can, try to detect them
2. Analyse and document some malware which you have caught

These choices allow you to:

To evaluate the spam, you are required to implement a spam detection engine (either in R or Python: there are many resources and datasets on GitHub). After investigating the sources of your spam, you should outline the purpose of the spam and impact it may have. Then you should first train and test a detection model, and have it predict the emails you obtained. You should analyse and evaluate the usage and results (confusion matric metrics) from both attacker and defender perspectives, and include language, topics, spam technique (to trick the target or bypass the filter) along with visualisation.

You are to use forensic tools to analyse the malware. You can use static or dynamic tools, or a combination of both. Examples (but not limited to) of these a Cuckoo, REMnux, IDA Pro. Your evaluation should be in comparison to older versions of the malware family or against recent examples which are similar, and the challenges surrounding detection and mitigation. Examples of this evaluation could be: the change in behaviour, the means the malware obfuscates its behaviour, or how it interacts within an operating system, and thus the impact and challenges it presents. Along with your evaluation, you also need to document the justification of tools, threat definition and challenges, and analysis methodology.

Custom

1. Develop your own procedure (subject to approval by the convenor)
   *Submissions to the convenor should be made before the 24 September 2020.

Custom projects should have clearly defined aims, objectives, and targets. If you seek to propose your own, you should draft a proposal. In doing so, projects can be evaluated so they can be achieved and meet suitable quality. **Some security projects will be provided** where you have the opportunity to collaborate with some Swinburne researchers. There will be a fixed set of projects, and these will require a high skill level and time to complete.

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 plagiarized and/or un-attributed work. eForensic examination of the assignment will be carried out to verify its authenticity.

Grading and Rubric

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)**
Criteria 1: Planning and Justification Scenario, choice of tools,	There is little to no evidence of understanding the security challenges, tools, threats and where they exist	Marginal evidence is give, 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,	Significant level of justification has been provided with relevant examples. Significant consultation of the landscape considered	High level of justification has been provided with relevant examples. Landscape challenges have been highly consulted through reference, needs outlined and choice of tools,

threat/topic choice	within the cyber security landscape.			tools, scenarios presented logically.	through reference. Topic, tools, scenarios presented logically.	scenarios and topics argued well.
10 Marks	2	3-4	5-6	6-7	7-8	8-10
Criteria 2: Application and Documentation 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 (Goodware/Malware) is discussed in-depth. Report of is excellent quality.
10 Marks	2	3-4	5-6	6-7	7-8	8-10
Criteria 3: Analysis Understanding the results achieved, analysing the impact/use/practicality/etc.	A low-level of analysis is presented. Concepts, impact, challenges and considerations are brief, or not given.	Basic analysis is presented. Concepts, impact, challenges and considerations are basic, with some detail.	Moderate analysis is presented. Concepts, impact, challenges and considerations are well considered, with good detail. The student has demonstrated moderate knowledge to analyse Criteria 3.	Well-thought out analysis is presented. Logical in nature, covering both attacker and defender concepts, impact, challenges and considerations. These have been give moderate depth. The student has demonstrated a good level of knowledge to analyse Criteria 3.	Highly-thought out analysis is presented. 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.	Excellent analysis is presented. Connections are made across the topic and security landscape, along with future challenges. The analysis has been linked to aims. Both attacker and defender concepts, impact, challenges and considerations are compared and contrasted. These have been given considerate depth. The student has demonstrated excellent level of knowledge to analyse Criteria 3.
10 Marks	2	3-4	5-6	6-7	7-8	8-10
Criteria 4: Evaluation Effectively judge/critique/summarise the result, challenge, usage 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. However, some simple evaluation is shown.	Evaluation of tools, 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 is provided. Some support is given.	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.	Thorough and high evaluation of tools, threats, challenges, usage, results is given. Depth is shown, and contrasting and consideration is provided across previous, current and future factors. Relevant and evaluated support through reference is given.
10 Marks	2	3-4	5-6	6-7	7-8	8-10

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) and should not exceed 15 pages in length. 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 authors (by 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. Appendices and a list of references will not be included in the page count.

Late submissions will be penalised by 10% per day (for 3 days maximum), submissions which are 3 days after due date will not be allowed and 0 mark will be given.

References

All externally sourced information (i.e. not common knowledge or course material) must be cited. Referencing conventions required for this unit are: Vancouver (as used by IEEE).
Helpful information on referencing can be found at https://guides.lib.monash.edu/citing-referencing/vancouver
https://ieeeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf

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.