Cardiff School of Computer Science and Informatics

Coursework Assessment Pro-forma

Module Code: CMT121
Module Title: Penetration Testing and Malware Analysis
Lecturer: George Theodorakopoulos
Assessment Title: Penetration Testing and Malware Analysis
Assessment Number: 1
Date Set: 25 October 2021
Submission Date and Time: 14 January 2022 at 9:30am via Learning Central
Return Date: 11 February 2022

This assignment is worth 100% of the total marks available for this module. If coursework is submitted late (and where there are no extenuating circumstances):

1. If the assessment is submitted no later than 24 hours after the deadline, the mark for the assessment will be capped at the minimum pass mark;
2. If the assessment is submitted more than 24 hours after the deadline, a mark of 0 will be given for the assessment.

Your submission must include the official Coursework Submission Cover sheet, which can be found here:

https://docs.cs.cf.ac.uk/downloads/coursework/Coversheet.pdf

Submission Instructions

There are two Tasks in this coursework: Task 1 (T1) is on Malware Analysis and Task 2 (T2) is on Vulnerability Assessment. In addition to the official Coursework Submission Cover sheet (see above), you should submit two reports (PDF or Word file).

Description		Type	Name
Cover sheet	**Compulsory**	One PDF (.pdf) file	[student number].pdf
T1 report	**Compulsory**	One PDF (.pdf) or Word file (.doc or .docx)	T1_[student number].pdf/doc/docx
T2 report	**Compulsory**	One PDF (.pdf) or Word file (.doc or .docx)	T2_[student number].pdf/doc/docx

Any deviation from the submission instructions above (including the number and types of files submitted) will result in a 10% reduction in marks for the corresponding Task.

Staff reserve the right to invite students to a meeting to discuss coursework submissions

---

Assignment

There are two Tasks in this coursework: T1 is to analyse malware and it is worth 30 marks. T2 is to test a vulnerable Virtual Machine image and it is worth 70 marks.

For T1, you will be given access to two pieces of malware. You will analyse both and write a report with your conclusions. You should submit your report as a PDF or Word file. The report should be **at most 1000 words**. Anything beyond the first 1000 words will not be marked.

For T2, you will be given two VM images: one is a Kali Linux VM from which you will conduct your attacks against the other VM (Ubuntu Linux), which contains at least 7 vulnerabilities. Your task is to follow a systematic process to find and exploit the vulnerabilities in the Ubuntu VM, propose fixes for the vulnerabilities that you find, and finally write a report with your findings and your recommendations. You should submit your report as a PDF or Word file. In total, the report should be **at most 3000 words**. Anything beyond the first 3000 words will not be marked.

Learning Outcomes Assessed

1. Perform static and dynamic malware analysis to explain the malware's anatomy, its effects on a system and its spreading behaviour.
2. Identify, evaluate, and recommend, with justification, a selection of configurations and countermeasures to reduce the likelihood and impact of potential security attacks.
3. Perform application penetration testing to identify system and network security vulnerabilities and exploit them.
4. Explain how to detect and react to network intrusions.
5. Explain how web browsers are used to exploit vulnerabilities and inject malicious code into web services (e.g. cross-site scripting).

Criteria for assessment

	Fail (0-49%)	**Pass (50-59%)**	**Merit (60-69%)**	**Distinction (70-100%)**
Approach	Random steps taken to conduct static and dynamic malware analysis and to identify system, web application, and network vulnerabilities. Many inappropriate tools chosen.	Clear understanding of relevant tools and methods, but with some unsystematic or unjustified deviations from proper methodology.	Systematic methodology chosen. Adopts appropriate methods and tools	Exceptional scholarship shown in choice and application of methodology. Justification of choices and good evidence of understanding alternatives.
Results	Very few or no relevant malware behaviour discovered. Superficial demonstration of only basic skills in malware analysis and pentesting.	Adequate discovery of behaviour and vulnerabilities, but some relevant ones are missing. Some competency in analysis/pentesting shown, but with clear limitations. Recommendations for countermeasures are present but limited in quantity or quality.	Most relevant malware behaviour and system, web application, and network vulnerabilities found. Skilful tool usage. Effective recommendations for fixing vulnerabilities.	Extensive discovery of relevant malware behaviour and system, web application, and network vulnerabilities. Wide range of skills shown and executed with precision. State-of-the-art recommendations for fixes and countermeasures.
Argument	Many factual or technical errors. Identification of security vulnerabilities is not linked to evidence.	Arguments contain some errors or invalid statements/facts are presented. Some evidence is provided, but linkage to identified vulnerabilities is not strong or it could be easily questioned.	Significant ability illustrated for logical and technically valid arguments. Findings are clearly linked to evidence.	Scientifically and technically correct statements, with no nuances missed. Evidence provided is both adequate to support the conclusions and it has no reasonable alternative interpretations.
Presentation	Significant lack of clarity and/or coherence. Unstructured report. Minimal awareness of technical terminology.	Communication is adequate to get the point across but requires some effort to understand. Good attempt to provide structure to the report, but with limitations (e.g. information that should	Clear and concise language. Well-structured into sections. Uses standard technical terminology.	Clear, precise, to-the-point description with no ambiguities nor irrelevant information included. Logical structure, easy to follow with

		be in one section appearing in another). Some but not many misunderstandings of terminology.		appropriate use of screenshots. Displays excellent command of technical terminology.

Feedback and suggestion for future learning

Feedback on your coursework will address the above criteria. Feedback and marks will be returned on or before 31 January 2022 via Learning Central.

Detailed Instructions

Task 1: Malware Analysis – 30 marks

As explained above, you will be given access to two pieces of malware. You must perform static and dynamic analysis on both to collect evidence and complete the following sub-tasks by referring to the evidence you collected:

1. List the malware's significant imports and strings, and its host-based and network-based indicators. (10 marks)
2. Describe how the malware works. (10 marks)
   Specifically for the malware called "sample.dat", your response should explicitly also answer the following questions:
   a. What is the AES Key, IV used by the malware sample?
   b. What are the commands the malware sample runs?
3. Describe the purpose the malware tries to achieve. (10 marks)

Your report must clearly separate your responses to each of these sub-tasks**.**

Task 2: Vulnerability Assessment – 70 marks

The VM images that you will be provided with are linked together in a network topology. You will log into the Kali Linux VM and you will conduct all your attacks from that VM. You should not modify the network topology. You should clearly follow a systematic pentesting methodology, you should clearly identify and describe each vulnerability you find and how you exploit it, and you should clearly recommend, with justification, a selection of configurations and countermeasures for fixing it.