AUSTRALIA ECU EDITH COWAN UNIVERSITY		INTERNAL/ EXTERNAL Semester Two, 2019
Unit Code and Title	CSI2107 Software Reverse Engineering	**SAMPLE STANDARD EXAM**
Student Number	SURNAME/FAMILY NAME	OTHER OR GIVEN NAME/S
Please print clearly		

Duration 2 hours

Attempt All Questions

Marks Section A – 10 Marks
Section B – 20 Marks
Section C – 10 Marks

Type of Exam Closed Book Exam

Special Instructions Answer all questions in exam booklet provided

Do not commence reading or writing this examination until you are told to do so.

Section A – Multiple Choice

Answer ALL questions in this section in the following space in your exam booklet. Each question is worth 0.5 mark. For each question identify the most correct response (Circle the right choice). No negative marking.

Q1: Emulator converts one programming language to another language.

A. TRUE
B. FALSE

Q2: Software Reverse Engineers develop strategies to track down cyber criminals.

A. TRUE
B. FALSE

Q3: Hex Editor is used for dynamic analysis.

A. TRUE
B. FALSE

Q4: Radare2 is not used for static analysis.

A. TRUE
B. FALSE

Q5: RAX is 64-bit extension of EAX.

A. TRUE
B. FALSE

Q6: Which of the following can be used for static analysis?

A. ?
B. ?
C. ?
D. ?

Q7: OllyDbg is a dynamic analysis tool focussed on binary analysis.

A. TRUE
B. FALSE

Q8: Why Patching is important? Choose the appropriate options listed.

A. ?
B. ?
C. ?
D. ?

Q9: Multidimensional arrays are not multidimensional. Do you agree?

A. YES
B. NO

Q10: Identify the correct endianness of the following value: 0x123456. Choose the appropriate options.

A. ?
B. ?
C. ?
D. ?

Q11: Which of the following memory areas are dynamically allocated?

A. ?
B. ?
C. ?
D. ?

Q12: Which of the following system call tracers are available in both Linux and MacOS?

A. ?
B. ?
C. ?

Q13: Malware runs slowly when debugged?

A. False
B. True

Q14: Obfuscations can be defended using plugins such as _____.

A. ?
B. ?
C. ?
D. ?

Q15: Identify which of the followings can be used to find OEP.

A. ?
B. ?
C. ?
D. ?

Q16: Stuxnet can be used for wrapping a program?

A. TRUE
B. FALSE

Q17: What would you do when automated unpacking fails? Call 000?

A. TRUE
B. FALSE

Q18: Which of the following is used to write detection rules?

A. X64dbg
B. LordPE
C. YARA
D. Vera

Q19: Obfuscation is useful for cyber security.

A. TRUE
B. FALSE

Q20: Which of the following can be used for debugging detection?

A. ?
B. ?
C. ?
D. ?

Section B – Short Answer

Answer ALL questions in this section. Each question is worth five (5) marks

Q1) How can you find OEP? Explain the steps to be taken?

Q2) Compare and contrast Radare2 and Ollydbg.

Q3) Write a SNORT rule to meet the conditions as follows: $str = “Hacking You” and pe.entry_point as 0x12000 and import Cuckoo to check the traffic from “www.hack.com”

Q4) Explain Ransomware as a service and how honeyclient can be useful in this context.

Section C – Code Comprehension

Answer ALL questions in this section. Each question is worth five (5) marks.

Q1) Explain what the code shown in the following disassembly does, make sure to justify your answer.

```
01:  mov ebx, 5
02:  mov eax, 1
03:  XOR eax, ebx
04:  XOR ebx, eax
05:  XOR eax, ebx
```

Q2) The following code is obfuscated. Optimise the code to de-obfuscate and briefly discuss the obfuscation techniques used.

```
int f() {
     int x, y;
     x = 1;
     y = 2;
     x = 3;
     return x;
}
```

END OF EXAMINATION PAPER