A35060

Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers



UNIVERSITY OF BIRMINGHAM

School of Computer Science

Fourth Year Undergraduate/Postgraduate

06-34233

LM Forensics, Malware, and Penetration Testing

Main Summer Examinations 2025

Time allowed: 2 hours

[Answer all questions]

Turn Over

Note

Answer ALL questions.

Question 1

(a) Before a pen test starts the scope of the pen test must be clearly defined. Imagine that you work for a company commissioning a pen test and it is your job to define the scope. Give two examples of things that you think it is the most important that the pen test covers and explain why they are important. **[10 marks]**

(b) Give two examples of things that you would define as out of scope for a company pen test and explain why they would be out of scope. **[10 marks]**

(c) PCI-DSS requires that companies carry out regular scans for unauthorised wireless access points. Imagine that you work for a company which finds an unauthorised wireless access point set up by an employee. The employee argues that the access point uses WPA2 and therefore is not a security risk. Is the employee correct? If so explain why, if not explain all of the reasons why the access point is a risk to the company. **[14 marks]**

Question 2

You are tasked to reverse engineer a suspicously looking binary executable file.

(a) Name 3 static binary analysis tools or utilities of your choice for the initial investigation of this file. For each tool/utility, briefly explain its capabilities and how it could help you in 1–2 sentences. **[9 marks]**

(b) While reverse engineering the binary, you find the following function:

```
00000000000011cd <CM0jNJqGW>:
11cd:       51                      push   rcx
11ce:       31 c0                   xor    eax,eax
11d0:       39 c6                   cmp    esi,eax
11d2:       7e 09                   jle    11dd <CM0jNJqGW+0x14>
11d4:       80 34 07 42             xor    BYTE PTR [rdi+rax*1],0x42
11d8:       83 c0 01                add    eax,0x1
11db:       eb f3                   jmp    11d0 <CM0jNJqGW+0x7>
11dd:       31 c0                   xor    eax,eax
11df:       ff d7                   call   rdi
11e1:       31 c0                   xor    eax,eax
11e3:       5a                      pop    rdx
11e4:       c3                      ret
```

Your task is to explain the purpose of this function. Try to answer the following questions in 1–2 sentences each:

(i) What does the instruction at address 0x11d4 do?

(ii) What is the purpose of the `jle` and `jmp` instructions at addresses 0x11d2 and 0x11db?

(iii) How many arguments does this function take, and what was their likely data type?

(iv) What is the purpose of the `call` instruction at address 0x11df?

[14 marks]

(c) Does this function indicate the presence of malicious behaviour in the binary? Choose two indicators to support your answer and explain your reasoning. **[10 marks]**

Question 3

You've been called in as a digital forensic investigator to analyse a hard drive seized in a high-stakes criminal case. Investigators suspect that a sophisticated malware attack has compromised the system, and it's your job to uncover the truth. The hard drive is still inside the computer, and you must determine what happened, how it happened, and what evidence can be recovered.

(a) Describe in detail, with references to proper guidelines, the process you would take to analyse the hard drive and recover a proper forensic image **[10 marks]**

(b) A forensic image has been acquired and loaded into Autopsy, an open-source digital forensics platform. The investigator reviews the file system activity. Below is an excerpt from the Autopsy Timeline Analysis module:

File Name	File Path	Created TS	Last Accessed TS	Last Modified TS	File System
notes.txt	C:\Users\Admin	24-02-10 14:25:10	24-02-10 14:32:55	24-02-10 14:32:00	NTFS
backup.zip	E:\Recovered\	23-12-15 18:45:30	24-02-10 14:30:45	23-12-15 18:45:30	NTFS
exploit.dll	C:\Windows\System32\	24-02-10 14:33:10	24-02-10 14:33:20	24-02-10 14:33:10	NTFS
hidden.log	D:\Old_Drive\Hidden\	18-07-12 09:15:22	24-02-10 14:31:30	18-07-12 09:15:22	FAT32

Examine the above excerpt and provide a report on possible anomalies, specifically identify. (1) What are the anomalies in the timestamps, (2) is there any forensic evidence of tampering with files. Make sure to explain how you came to these conclusions and any further analysis you may conduct to verify these statements. **[15 marks]**

(c) The police investigators, without forensic analysis, are suspicious of backup.zip, can you provide evidence as to whether it was copied from another device? Make sure to reference tools you would use. **[8 marks]**

This page intentionally left blank.

A35060 **LM Forensics, Malware, and Penetration Testing** **Non-alpha only**

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or Tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.