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

Forensics, Malware and Penetration Testing

Main Summer Examinations 2024

Time allowed: 2 hours

[Answer all questions]

Turn Over

Note

Answer ALL questions. Each question will be marked out of 20. The paper will be marked out of 60, which will be rescaled to a mark out of 100.

Question 1

(a) Imagine that you have been asked to penetration test a company's network, what would you try first? Describe the method you would use and the kinds of vulnerabilities you might find. **[8 marks]**

(b) Give an example of a vulnerability that you would expect could be found by an automatic vulnerability scanning tool, and explain why the tool could reliably find it. **[6 marks]**

(c) Give an example of a vulnerability that you would expect could **not** be found by an automatic vulnerability scanning tool, and explain why automated tools would find it hard to detect such attacks. **[6 marks]**

Question 2

(a) Describe the fundamental differences between dynamic and static analysis in the context of malware analysis. Discussion should include, scope, applicability, advantages and limitations **[4 marks]**

(b) Consider a scenario where you are analysing a piece of malware that exhibits polymorphic characteristics, making it difficult to analyse using static methods alone. Describe how you would apply dynamic analysis to investigate this malware. **[6 marks]**

(c) Examine the code snippet below, please indicate what the program is doing, what time of malware this would be classified as, and then mention why it would be difficult to analyse, both statically and dynamically **[10 marks]**

Question 2 continued on next page

```
...
namespace fs = std::filesystem;
...
void DOING_STUFF(const std::string &folderPath) {
 for (const auto\& entry : fs::directory_iterator(folderPath)) {
  if (entry.is_regular_file()) {
   encryptAndSendFile(entry.path());
  }
 }
}

int main() {

 if (IsDebuggerPresent()) {
  std::cout << "Nice Try." << std::endl;
  return -1;
 }
 else {
  std::cout << "Doing normal stuff." << std::endl;
  DOING_STUFF("~/*")
  // Get the path
  char exePath[MAX\_PATH];
  GetModuleFileNameA(NULL, exePath, MAX_PATH);

  // set up the command (this is a single line)
  std::string cmd = "cmd /c ping localhost -n 3 > nul &&
  del /f /q \"" + std::string(exePath) + "\"";

  // Setup for CreateProcess
  ...
  // Convert command in cmdArray
  cmdArray = ... // cmd from above plus parameters
  ...
  // execute the command
  CreateProcessA(..., cmdArray, ...))
 ...
// Exit the program
```

Question 3

You have been tasked with examining a hard drive collected from a criminal investigation. It is said to have been targeted by a powerful malware, and they want you to find out what has been done to it. The harddrive is currently still in the computer.

(a) Describe the process you would take to analyse the hardrive and recover a proper forensic image **[8 marks]**

(b) Now that you have a forensic image of the harddrive, please describe what kind of signs you might look for to establish what the malware did, making references to tools you might use, and specific signals. **[6 marks]**

(c) You find indications that the attacker made use of several applications in it's attack. Using this clue, what kind of steps can you take to figure out what the attacker did, and the steps he took, explain making reference to specific tools and type of analysis **[6 marks]**

End of Paper

This page intentionally left blank.

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.