CSE 345/545: Foundations to Computer Security
ASSIGNMENT 3 (TOTAL OF 130 POINTS)
Deadline: December 6, 2020

Instructions:

- Do your Assignment questions individually.
- Make one PDF format file for writing your analysis/results in the format <RollNo>_HW3.pdf
- Submit the '.txt' files separately in the format "<RollNo>_7_b.txt".
- ***Do not* zip your submissions.**
- State your assumptions (if any) in your question.
- If the solution requires you to use paper, paste a good quality image of the solution in the document that you are submitting.
- All the Queries, if any can be posted on google classroom.
- **Note: Answer the questions in bullet points. Keep your responses crisp and to the point.**

Part 1

1. Amazon is testing drones for delivery, and you are the Security Analyst. View the **system as an adversary** and fill in the following table.

List of entry and exit points	
Purpose of each entry and exit point	
List of assets	
Employee / drone handlers trust levels	
Two use scenarios	
External security notes	
Internal security notes	
Any Three threats in the order of severity	
Discoverability of the 3 threats	
Damage potential of the 3 threats	

Mitigation strategy for all 3 threats	
ROI for all 3 threats	

[**20 marks**]

2. Draw data flow diagram for single Zomato food ordering cycle [customer orders food -> restaurant accepts the order -> rider assigned -> food delivered]. Use correct shapes and show the data flow between “customer”, “rider”, “restaurant” and “Zomato”. Draw appropriate trust boundaries and explain your intuition.

[**20 marks**]

3. Find the internal PCB photos from fccid.io for the Robert Bosch SVI-1609-5 smart camera .
    a. Paste the photo with “Ambarella” chip from FCCID website in your assignment.
    b. What is the function of the said “Ambarella” chip. [Search on the web with the IC number]
    c. Name 3 ICs and their packaging as found on the PCB images from FCCID website.

[**10 marks**]

4. The latest version of Google Pixel went for fingerprint to unlock, while past versions had a face ID. Users have been complaining about the iPhone that they are unable to just take a look at the phone, as the screen unlocks instantly. Comment about the pros and cons of fingerprint and face ID. Approach the argument from “usable security” standpoint. Keep in mind the “new normal” where everyone is wearing masks and sanitising hands all the time. Finally, state your favourite mobile unlock mechanism and reason about its security and usability.

[**10 marks**]

5.
    a. Give 2 ways by which Teachable moment can be used in security design / systems. Give a scenario where it can be applied for collecting data across the world.

[**10 marks**]

    b. What does **Take Down** of a website mean? What is the process of taking down a website if it is found being part of a phishing attack?

[**5 marks**]

    c. Give 2 scenarios where embedded training can be used in security problems?

[**2 X 2.5 = 5 marks**]

6. Search and read about Emotet and Agent Tesla malwares. Discuss the defence mechanisms used by these malwares? Why is it hard to detect Agent Tesla using the techniques discussed in class? What techniques can Emotet borrow from Agent Tesla to operate more sneakily?

[**10 marks**]

Part 2

7. Download the memory dump attached with the assignment. The file is protected with a password popular among the malware community. Analyze the memory dump using *'vol.py'* [volatility] and answer the following questions.
   For each of the following questions, provide screenshots [with big enough font size] of the executed commands:
   a. On which platform was the memory dump taken?
   b. Save all unique web domains captured in the memory dump to a .txt file. Did you find any suspicious websites? [Name the output file with "rollnumber_7_b.txt"]
   c. List the unique ip addresses captured in the dump. [The command can just list all ips, not necessarily unique ips]
   d. What were the processes running at the time?
   e. Which 4 processes have the same parent?
   f. What commands invoked the above 4 processes?
   g. One process is suspicious. Why?
   h. Take the process dump of the suspicious process. Save the "strings" output of the process to a .txt file. Did you find any suspicious activity? Discuss? [Name the output file with "rollnumber_7_h.txt"]

[**8 X 5 = 40 marks**]

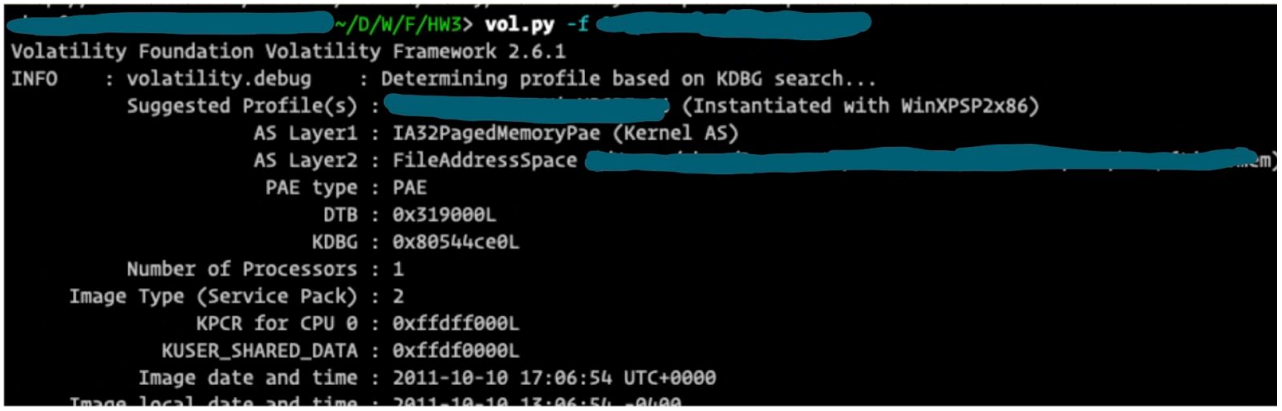
Note / suggestion : Get solution to [7.h.] before you answer [7.g.].

Example solution format:

7.a.

1. Command used : `vol.py -f file.vmem imageinfo`

2. Screenshot:



3. Discussion: I found that the platform is <platform name>. Because of the parameters captured in image info are <parameters>.