FORENSICS CYBER-SECURITY

MEIC, METI

2020/2021 1st Semester

1st Exam January 25, 2021 Duration: 2h00

- Use a pen only; no extra material is allowed, such as calculator, scratch paper, etc.
- Write your answers in the free space after each question.
- The exam can be answered in Portuguese or in English.
- Identify all sheets; **unidentified pages will not be graded!**

I. (2 + 0.5 + 0.5 + 0.5 + 0.5 = 4 points)

1. For each of the following statements, indicate whether it is true (T) or false (F). Each correct answer is awarded 0.25 points; each wrong answer is penalized by subtracting 0.10 points.

   a. ____: When applied to the digital world, the Lockard's Exchange Principle also predicts the existence of evidence transfers between the digital crime scene and the physical crime scene.

   b. ____: In digital forensics, if the authenticity of the digital evidence is not compromised, then it will almost certainly be considered admissible in court.

   c. ____: If a given act involves computers but does not violate any law, then there is no crime in doing it.

   d. ____: During the acquisition stage, only the seized hardware devices need to be accounted for in the chain of custody form.

   e. ____: Inculpatory evidence is the kind of evidence that supports a given theory as long as the evidence can be overtly recovered from a suspect's hard disk.

   f. ____: The Kruse model is very popular for its ability to deal with digital investigations that proceed in a non linear fashion.

   g. ____: The *netstat* tool is frequently used for listing the network connections of a system when performing post-mortem forensic analysis.

   h. ____: In regards to methods for extracting data from a storage device, logical acquisition may be a better option for forensic analysts to use than bit-stream copy.

2. Consider the following investigative scenario:

> Penelope is the technical director of XFarma, a major pharmaceutical company. One day, she was working at her workstation and she received an email from Mr. John Carson, the CEO of the company. The email body contained a message urging her to provide a review of the pdf document enclosed in attachment. When she opened the document, she noticed that the text made no sense whatsoever. However, after a few minutes, the computer suddenly freezes and a message was displayed on the screen saying that all her data had been encrypted and that, unless she transferred 0.01 BTC to a certain bitcoin account by the next day, all her data would be lost forever. Immediately she noticed a dreadful reality: she had fallen victim of a ransomware attack! Right away she stopped interacting with her workstation. Concerned that the hacker had also encrypted her files in the company's file server, she logged into the file server from her laptop, and realized that indeed all her files were encrypted! She stopped all her actions and reported the problem to the IT. A forensic analyst was called for assistance.

Put yourself in the shoes of the forensic analyst. Do you agree with these statements? Justify.

a. "Unplugging Penelope's workstation from the network is highly recommended as it prevents the hacker from doing more harm."

b. "Shutting down Penelope's workstation from the power supply would be the most suitable action to do for preserving all the evidence on disk."

c. "Cold boot attacks could be useful in this case."

d. "There is not much we can do to determine the provenance (i.e., the origin) of the attack."

II. (2 + 1 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 1 + 0.5 + 0.5 + 0.5 = 8 points)

1. The hex dump shown below lists the pixel data of a greyscale 16-bit bitmap image. Your task is to embed a covert payload message into these pixels using a 4-bit LSB encoding scheme.

```
00: a1cf 22c6 9cb3 4582 0533 d16b 2aaf a296
10: 705c 1e94 7b1e 878f f4cc 8163 7ad0 8f34
20: 3326 000a 562a 841b 2510 18e6 349f 52ae
30: b131 3cfb 58e7 fe55 6988 e014 898d a4b4
40: .... .... .... .... .... .... .... ....
```

   The hidden message must start with a one-byte prefix that indicates the total size of the payload message size in bytes. For example, a message of 7 bytes causes 8 bytes to be embedded; the prefix value will be 7. The message will be protected by a password. The algorithm that tells which pixels contain the encoded data (i.e., both prefix and message) is:

   * the first pixel (p_0) to encode bits is given by: $p_0 =$ password *mod* 5;
   * the next pixels are found by: $p_i = p_{i-1} + 3$;
   * pixel numbering begins in 0, i.e., the index of the first pixel of an image is 0.

   The message M to be encoded and the password P are as follows:

   * M = `1011 0111 0011 1001 0001 1011` (binary);
   * P = 7 (decimal)

   Indicate the new hexadecimal values of the <u>first four</u> modified pixels. Provide this information using the notation: $p_i = v_i$, where i is the number of the pixel, and v_i the pixel's new value.

2. There are two general approaches to memory dump analysis: i) tree/list traversal, ii) fingerprint/pattern search. Indicate one disadvantage of each of these techniques.

3. Consider below the output snippets of the *istat* tool when applied to the analysis of two filesystem meta-data structures from different forensic images: `mystery1.dd` and `mystery2.dd`:

   * Output 1 (`mystery1.dd`)

```
[REMOVED]
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-7) Name: N/A Resident size: 80
Type: $DATA (128-8) Name: $SDS Non-Resident size: 266188
10016 10017 10018 10019 10020 10021 10022 10023
10024 10025 10026 10027 10028 10029 10030 10031
10032 10033 10034 10035 10036 10037 10038 10039
[REMOVED]
```

   * Output 2 (`mystery2.dd`)

```
[REMOVED]
Direct Blocks:
14380 14381 14382 14383 14384 14385 14386 14387
14388 14389 14390 14391 14393 14394 14395 14396
[REMOVED]
16880 16881 16882 16883
Indirect Blocks:
14392 15417 15418 16443
```

   Answer the following questions:

   a. Suggest the type of the file system formatted on each of the forensic images. Justify your answer. (Unjustified answers earn 0 points.)

   b. In output 1, explain what it means "`Non-Resident`" for "`Type: $Data`". Be specific for this context; general descriptions of non-resident attributes will be insufficient.

   c. In output 2, explain the meaning of "`Indirect Blocks`". Be specific for this context; general descriptions of indirect blocks will be insufficient.

4. Consider a Windows disk image of a user who is a suspect of engaging in child pornography activities. You have two forensic tools at your disposal: i) *superreg*, a tool for inspecting the Windows registry, and ii) *bicarv*, a BGC-based file carving tool. Provide two examples of relevant digital artifacts you would search for using these tools; state one example per tool.

5. “A common strategy to detect timestomping is to search for inconsistencies in files’ timestamp formats."Do you agree? Why? (A yes/no answer without justification earns 0 points)

6. A network administrator observed abnormal traffic in the local network originating from Vick’s locally connected computer, 146.193.41.40. Below, we see a fragment of the collected *tcpdump* trace. Suggest a hypothesis for what might be happening. Justify your answer.

```
17:40:35.258314 IP 146.193.41.40.1037 > 10.10.10.10.4445: Flags [S],
    seq 553522758, win 65535, length 0
17:40:35.258390 IP 10.10.10.10.4445 > 146.193.41.40.1037: Flags [R.],
    seq 0, ack 553522759, win 0, length 0

[THE PACKET EXCHANGE ABOVE REPEATS PERIODICALLY 15 TIMES]

17:42:02.985483 IP 146.193.41.40.1044 > 10.10.10.10.4445: Flags [S],
    seq 1979373164, win 65535 , length 0
17:42:02.985580 IP 10.10.10.10.4445 > 146.193.41.40.1044: Flags [S.],
    seq 1436350344, ack 1979373165, win 5840, length 0
17:42:02.985870 IP 146.193.41.40.1044 > 10.10.10.10.4445: Flags [.],
    ack 1, win 65535, length 0
...
```

7. Explain in what way the two middleboxes below complicate the analysis of network traces:
   a. NATs

   b. VPNs

8. Indicate two limitations of existing network intrusion detection systems.

III. (1.5 + 1 + 1 + 0.5 + 0.5 + 0.5 + 1 + 0.5 + 0.5 + 0.5 + 0.5 = 8 points)

1. The network administrator at XFarma intercepted an open TCP/IP connection taking place between a computer of the company (146.193.41.42) and an external server (13.225.241.87). The local computer is from Bob Gates, a clerk that works in the company. By performing a reverse DNS lookup, the external IP address was found mapped to "smtp.free-open-relay.com".

```
13.225.241.87: 220 smtp.free-open-relay.com ESMTP Postfix
146.193.41.42: HELO 146.193.41.42
13.225.241.87: 250 Hello 146.193.41.42, I am glad to meet you
146.193.41.42: MAIL FROM:<carson@xfarma.com>
13.225.241.87: 250 Ok
146.193.41.42: RCPT TO:<penelope@xfarma.com>
13.225.241.87: 250 Ok
146.193.41.42: DATA
13.225.241.87: 354 End data with <CR><LF>.<CR><LF>
146.193.41.42: From: "John Carson" <carson@xfarma.com>
146.193.41.42: To: "Penelope Pearson" <penelope@xfarma.com>
146.193.41.42: Date: Tue, 15 January 2021 16:02:43 -0500
146.193.41.42: Subject: Need urgent feedback on report
146.193.41.42:
146.193.41.42: Hi Penelope
146.193.41.42: I need your feedback on the report in attachment.
146.193.41.42: Thanks,
146.193.41.42: John
146.193.41.42: ....
```

   Suggest a hypothesis for what might be happening. Justify your answer.

2. Alice is accessing CNN over a Tor circuit. This circuit is established across Alice's computer, entry relay R_1, middle relay R_2, and exit relay R_3. Which intermediate links of the circuit would you need to intercept to launch a traffic correlation attack? Explain your answer.

3. Indicate two defense mechanisms employed in the design of botnets that enable them to circumvent blocking countermeasures by ISPs and network administrators.

4. You were called to investigate a potential network intrusion and to inspect if the mail server of the company has been compromised. When you run the command *ps* to list the total number of running processes, the result is 156 processes. However, if you retrieve the same information from */proc*, the number of existing processes is 157. This discrepancy strongly suggests that the system has been compromised by a rootkit. Answer the questions below:

   a. Explain why the discrepancy indicated above points to the fact that the mail server has been compromised by a rootkit.

   b. What is likely the technique employed by the rootkit to conceal itself? Justify your answer (no justification means 0 points).

   c. How would you proceed to further investigate the activity of the rootkit?

5. In Bitcoin, users can make the money flow between transactions more difficult to trace by creating multiple accounts and spreading the money across said accounts. Indicate and explain one technique that forensic investigators can adopt to identify the owner of these accounts.

6. Explain what the IMSI is and how it can be useful in forensic investigations.

7. Consider a case that requires the forensic acquisition of data from an Android mobile device. Answer the following questions:
   a. Indicate two factors that make it challenging to extract data from mobile devices.

   b. Indicate one strength and one weakness of chip-off physical data extraction techniques.

   c. What kind of information can be obtained from shared preferences?