FORENSICS CYBER-SECURITY

MEIC, METI

2022/2023 1st Semester

1st Exam November 18, 2022 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. (0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 = 4 points)

1. Consider the so-called Kruse investigation model:

   a. Indicate four tasks that need to be performed during the assessment stage.

   b. "In the acquisition stage of an investigation, if an investigator finds documents on drug-related activity on a machine while searching for evidence on child pornography, these documents will be considered inadmissible". Do you agree with this statement? Justify your answer.

   c. In the analysis stage, the forensic analyst should look for both types of evidence: inculpatory and exculpatory. What do they mean?

   d. In the reporting stage, why is it necessary to describe in detail the forensic tools – software and/or hardware tools – that were used in the investigation?

2. Consider the following investigative scenario:

> Mr. Watson is a forensic analyst that works in the police forensic lab. He was entrusted with two artifacts that were collected on site as part of a new investigation. These artifacts consist of an external SSD drive and a turned-off laptop computer accompanied by a chain of custody form. His job is to collect and preserve bitstream images of both artifacts to facilitate their future examination. To create an image of the SSD drive, Mr. Watson connected it to his Debian Linux workstation using a USB cable and let the OS automatically detect the new block device. Using the *dc3dd*, he created two bitstream copies of the entire disk, computing and validating the respective SHA256 hashes, and saving both of them securely on the lab's file server. To create an image of the laptop, Mr. Watson first observed that it was not possible to remove its hard disk. He then connected the laptop to a power supply and turned it on, letting the native operating system bootstrap – a Linux Ubuntu distribution. Unfortunately it was password-protected; therefore, he decided to reboot the laptop from a USB pen configured with Kali Linux. After mounting the laptop's disk read-only, he preserved two bitstream copies using the same procedure as for the SSD drive. Lastly, he updated the chain of custody form.

Indicate if you agree with the presented statements. Justify your responses:

a. "The procedure he employed to create the bitstream image of the SSD drive was correct."

b. "Given that it was not possible to remove the hard disk from the laptop and that the native OS was password-protected, this was the correct way to create the laptop disk image."

c. "Unless the updated chain of custody form includes the signature of the former custodian, the admissibility of the evidence can be compromised."

d. "An alternative method to create the bitstream images would have been to use the Linux command *cp* instead of *dc3dd*."

Number: ____________ Name: ____

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

1. A C&C server communicates with zombie machines by posting images on a known website. These images contain covert secret messages M. Periodically, zombies download the most recent image and extract M, which is a fixed size message of 8 bits (m_0-m_7) containing a command to the zombies. If the first bit $m_0 = 0$ then no attack should be launched and the remaining bits m_1-$m7$ are filled with random bits. Otherwise, if $m_0 = 1$, then zombies are instructed to perform a DDoS attack to a specific victim. The type of DDoS attack is indicated by the bits m_1-m_3 (3 bits) and the victim's IP by the bits m_4-m_7 (4 bits) as indicated below:

m_1-$m3$	*DDoS attack type*
101	SYN flood
110	ICMP flood
001	UDP flood
010	HTTP flood

m_4-$m7$	*Victim's IP address*
0110	142.250.178.164
1100	193.136.128.169
0010	185.15.58.226
1110	195.234.134.174

To hide M inside an image, C&C server and zombies employ a key-protected 2-bit LSB encoding scheme and use 16-bit greyscale bitmap images as carriers. Their agreed shared key is $K = 23$ (decimal). To be more robust against visual attacks, the encoding algorithm never encodes bits inside pixels that are white (i.e., `0xffff`) or black (i.e., `0x0000`), skipping pixels in the random walk sequence until a next pixel is found that does not meet these conditions. The random walk sequence of the encoding algorithm is given by:

- ∗ the first pixel (p_0) to encode bits is given by: $p_0 = K \textit{ mod } 5$;
- ∗ next pixels are found by: $p_i = p_{i-1} + 2$; encode if pixel p_i is not white/black, else skip to p_{i+1};
- ∗ the pixel numbering begins in 0, i.e., the index of the first pixel of an image is 0.

The hex dump shown below lists the pixel data of an intercepted image. Identify the embedded command, indicating the attack type and victim if that is the case. Justify your answer.

```
00: ffff ffff ffff ffff ffff ffff ffff 465b
10: 7315 e576 2ee9 1d7c 0000 0000 0000 0000
20: 0000 0000 0000 8f8e a2a9 1783 3cdf b64d
30: a614 e4d0 5c5c 14f7 ffff ffff ffff ffff
40: .... .... .... .... .... .... .... ....
```

2. An SSH server running on a machine crashed unexpectedly reporting a bad memory access at the memory address $A =$ `0x080d82a7`. An entire snapshot was taken of the 4GB-sized physical memory (i.e., memory range `0x00000000`-`0xffffffff`) and saved in a dump file. How can A be used to locate, inside the dump file, the instruction that caused the crash?

3. Consider the following output sample returned by the *fsstat* tool when applied to a bitstream image of an Ext3 file system extracted from a hard disk's partition:

```
METADATA INFORMATION
------------------------------------
Inode Range: 1 - 38401
Root Directory: 2
Free Inodes: 36976
CONTENT INFORMATION
------------------------------------
Block Range: 0 - 153599
Block Size: 4096
Free Blocks: 85287
```

   Answer the following questions and justify your answers:

   a. Based on this output, can you determine if any volume slack space exists in the partition?

   b. How does *fsstat* determine the number of free inodes and free blocks in the file system?

   c. How would you implement a forensic tool to dump the raw contents of the root directory?

4. ISO 9660 is an append-only file system commonly used for storing files on DVDs. Files are written onto the file system at once and made read-only; newly added files are appended to the end of the file system. Consider a single-pass structure-based file carver c and two bitstream images: I1 (ISO 9660) and I2 (Ext3). Based on the file systems' characteristics, how well is c likely to perform at recovering deleted files? Pick one option and justify.

   (1) c performs better on I1 (2) c performs equally on I1 and I2 (3) c performs better on I2

5. Sam wants to hide stolen industrial secrets (file *vacations.xlsx*) on his personal Windows computer. Towards this end, he executes the following command:

```
C:> type "C:\Documents and Settings\Sam\Documents\vacations.xlsx" >
    C:\Windows\System32\cmd.exe:vacations.xlsx
```

   Explain the hiding technique being employed and tell one way to detect the hidden content.

6. In Windows Registry, the following key directory holds the computer's network card settings. Give an example of one network card setting particularly important in forensic investigations.

```
HKEY\LOCAL\MACHINE\SYSTEM\CurrentControlSet\Control\
    Class{4D36E972-E325-11CE-BFC1-08002BE10318}\...
```

7. A network administrator detected abnormal traffic in the local network (192.168.1.00/24). Part of the collected *tcpdump* trace is listed below:

```
11:34:27.590380 IP 192.168.1.27 > 192.168.1.30: ICMP 192.168.1.30 unreachable, len 64
11:34:27.590402 IP 192.168.1.27 > 192.168.1.31: ICMP 192.168.1.31 unreachable, len 64
11:34:27.590419 IP 192.168.1.27 > 192.168.1.32: ICMP 192.168.1.32 unreachable, len 64
11:34:27.590432 IP 192.168.1.27 > 192.168.1.33: ICMP echo request, id 27948, len 64
11:34:27.590485 IP 192.168.1.33 > 192.168.1.27: ICMP echo reply, id 27948, len 64
11:34:27.590493 IP 192.168.1.27 > 192.168.1.34: ICMP 192.168.1.34 unreachable, len 64
11:34:27.590521 IP 192.168.1.27 > 192.168.1.35: ICMP echo request, id 27950, len 64
11:34:27.590563 IP 192.168.1.35 > 192.168.1.27: ICMP echo reply, id 27950, len 64
11:34:27.590598 IP 192.168.1.27 > 192.168.1.36: ICMP 192.168.1.36 unreachable, len 64
```

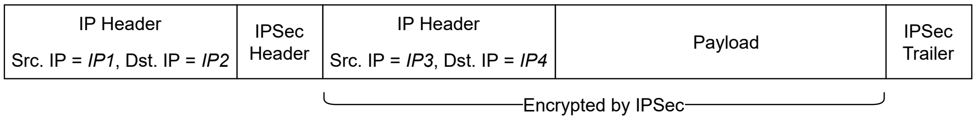
Answer the following questions. Justify all your answers.

a. State one of the most common uses for ICMP packets.

b. Suggest a possible explanation for the intended purpose of this packet sequence.

c. Given that IP 192.168.1.27 is assigned to the IDS server, what may have happened?

8. Alice wants to access Wikipedia (IP: 185.15.58.226) from home using her computer (IP: 192.168.1.2). Her home router implements NAT and exposes the public IP 146.193.41.40. First, she creates a VPN tunnel using her company's VPN server (IP: 193.136.128.169) resulting in the assignment of virtual IP 172.16.1.3 to her computer. She then accesses Wikipedia through that tunnel. Considering that IPSec packets received by the VPN server from Alice's computer have the format below, identify the *IPx* addresses. No justification needed.



IP1: *IP2*: *IP3*: *IP4*:

III. (2 + 1 + 0.5 + 0.5 + 1 + 0.5 + 0.5 + 1 + 0.5 + 0.5 = 8 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 investigating man-in-the-middle attacks in a free Wi-Fi network, we must always expect the presence of deauthentication frames sent by the attacker.

   b. ____: The IMEI can be used to identify the manufacturer and model of a specific mobile device, but not the identifier of the mobile subscriber.

   c. ____: SQL injection attacks leave traces on web server logs when the exploited web form sends user inputs using the HTTP method GET, but not when POST is used.

   d. ____: Botnets usually employ fast flux which consists in rotating the domain name addresses of the C&C server.

   e. ____: An example of file masquerading implemented by some rootkits is to overwrite shared libraries, e.g., */usr/lib/libX.a*.

   f. ____: In Android, the difference between internal storage and external storage is that the former keeps data in RAM and the latter on flash memory.

   g. ____: Chip-off cannot be performed in the context of a police investigation because it implies destroying the mobile device permanently.

   h. ____: Virtual machine introspection is a forensic analysis technique that cloud providers can freely use on customers' virtual machines, e.g., for detecting malware.

2. Regarding mobile positioning techniques for cellular networks, indicate one advantage and one disadvantage of *fingerprint matching* in comparison to *trilateration*.

3. Consider the samples of two email headers received by a user with a Tecnico email account:

   - Mail header 1:

```
Delivered-To: ist14262@mail-store.ist.utl.pt
Received: from smtp1.tecnico.ulisboa.pt ([193.136.128.21])
    by mail2.tecnico.ulisboa.pt (Postfix) with ESMTPS id 860B75600B9;
     Tue, 21 Jun 2022 20:02:33 +0100 (WEST)
Received: from mail-pf1-x444.google.com (mail-pf1-x444.google.com)
    by smtp1.tecnico.ulisboa.pt (Postfix) with ESMTPS id 259EF6008761;
    Tue, 21 Jun 2022 20:02:23 +0100 (WEST)
Received: by mail-pf1-x444.google.com with SMTP id x4so7597490pfq.2;
    Tue, 21 Jun 2022 12:02:23 -0700 (PDT)
Date: Tue, 21 Jun 2022 19:02:20 +0000
From: ABDULKHALID OMAR <johobaeu@gmail.com>
To: undisclosed-recipients:;
```

   - Mail header 2:

```
Delivered-To: ist14262@mail-store.ist.utl.pt
Received: from smtp1.tecnico.ulisboa.pt ([193.136.128.21])
    by mail1.tecnico.ulisboa.pt (Postfix) with ESMTPS id 7760D3600A3;
    Wed, 26 Oct 2022 04:14:56 +0100 (WEST)
Received: from a27-33.smtp-out.us-west-2.amazonses.com ([54.240.27.33])
    by smtp1.tecnico.ulisboa.pt (Postfix) with ESMTPS id 454186000421;
    Wed, 26 Oct 2022 04:14:52 +0100 (WEST)
Date: Wed, 26 Oct 2022 03:14:48 +0000
From: Peeref <info@peerefmail.com>
To: gaspar.santos@tecnico.ulisboa.pt
```

   Answer the following questions and justify your answers:

   a. Identify an anomaly in header 1 that prevents the complete reconstitution of its path.

   b. What can you tell about the internal SMTP server network topology at Técnico?

4. A certain piece of malware includes instructions that cause a debugger to crash. Indicate what type of malware analysis technique this anti-forensic approach is trying to mitigate.

5. Suppose that Tor developers have released a new version of the Tor software aimed to improve the performance of communications tunneled through Tor circuits. To this end, they made this change: when a client accesses a given remote website (e.g., `http://www.cnn.com`), the DNS request/response required to determine the corresponding IP address of the destination (e.g., `http://www.cnn.com` → IP 199.232.83.5) will no longer be tunneled through the Tor circuit but will be performed by accessing the DNS server directly; the Tor circuit will only tunnel the ensuing TCP session between client and destination. Answer the following questions:

   a. Represent a diagram illustrating the network path of TCP/IP packets exchanged between a Tor client (C) and a remote server (S) when tunneled through a typical Tor circuit.

   b. Explain in what way the proposed change improves the performance of Tor traffic.

   c. Explain if (and how) the proposed change will affect the anonymity properties of Tor.

6. Consider the following statements involving Bitcoin investigations and indicate whether you agree or disagree with them, justifying your answers:

   a. "By analyzing Bitcoin's transaction graph, it is possible to obtain the complete transaction history, including the public keys of all accounts involved in Bitcoin transactions."

   b. "By deploying a hacked Bitcoin miner in the system, police authorities can gain the ability to record on the Bitcoin ledger the IP addresses of users that submitted transactions."