INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment III

ARIANE 6 – Stage III

2024/2025

nuno.m.santos@tecnico.ulisboa.pt

Introduction

This assignment will conclude the investigation into the “Ariane 6” case. In the last assignment, you analyzed the hard disk images from two computers owned by João Musk. Your focus will now shift to the computer network of IST’s Satellite Lab, responsible for building ISTSat-1, the satellite developed by IST and recently deployed into orbit by the Ariane 6 rocket. Evidence discovered on João Musk’s computers suggests the possibility of information leaks from the lab, pointing to a conspiracy and an ongoing crime involving the satellite. The goal of this analysis is to investigate potential security breaches within the lab’s network and gather additional evidence to confirm or dispel the conspiracy. As in the previous assignment, we recommend using Kali.

Scenario presentation

Upon examining João Musk’s workstation and backup server, several key pieces of evidence emerged. First, the backup server contained duplicates of the covert documents found in his Sigma account, including the Fenix credentials. Further investigation revealed that these credentials had been shared with him via IRC by a user named Rootkitty, who appeared to be the true culprit behind the security breach. Under interrogation and pressure from the Policia Judiciária, Mr. Musk disclosed the real identity of Rootkitty: Catarina Pato, his colleague and a senior member of IST’s STT. This led the police to interrogate her and further investigate the Fenix credential breach.

In addition to this, evidence was uncovered on the backup server that contained five hidden documents related to ISTSat-1, which had also been found in Mr. Musk’s Sigma account. These documents had been copied from his workstation to the backup server, and before that, from a pen drive to the workstation. The pen drive had been left for Mr. Musk by an unidentified individual, who sent him an anonymous email instructing him to retrieve the drive from a public locker. Conversations with his friend Rootkitty suggest that ISTSat-1 had been altered with a mind control device, allegedly used to manipulate the population of Oeiras into frequenting certain restaurants, thereby boosting their revenues.

If confirmed, this would indicate a major crime with serious and troubling consequences for the population. In light of these findings, the Policia Judiciária has opened a new investigation and obtained a warrant to further investigate a potential leak of sensitive information from IST’s Satellite Lab, which is responsible for the development of the satellite. The objectives are to trace the origins of these documents (and identify the author of the anonymous email) and to gather further evidence that could confirm or refute the existence of the conspiracy, identifying any stakeholders involved if the conspiracy is proven.

The police have visited IST’s Satellite Lab facilities with the objective of obtaining evidence from their computer network. As with the initial assignment, you were enlisted to assist in this investigation. With the help of the network administrator, Mr. Ricardo Prado, you were introduced to the network topology and provided access to forensic material that may be useful for this case.

The figure below depicts a simplified reconstruction of the network topology. It features a gateway that functions as both a router and an HTTP(S) Proxy, with the IP address 194.210.63.254. The network also includes three workstations. The first belongs to Prof. Rafael Calhau, the lead professor responsible for the ISTSat-1 project, whose workstation’s IP address is 194.210.61.135. The second, with IP address 194.210.61.134, belongs to Virgolino Gonçalves, the lead engineer overseeing all satellite operations. The third workstation, assigned the IP address 194.210.61.136, is currently used by Miguel Estrela, a master’s student in computer engineering who has been interning at the Satellite Lab and involved in the project for the past few months.

Fortunately, due to security considerations, the HTTPS Proxy has been configured to capture periodic network traffic traces. Mr. Prado has provided access to: (1) three distinct network traces, each recorded at different times, and (2) the SSL key log file, which was secured prior to the events examined in earlier assignments. The SSL key log file allows forensic experts to decrypt SSL/TLS traffic, such as the HTTPS traffic captured by the proxy. This key file is compatible with Wireshark and can be used directly within the tool. All relevant files are available for download under ’Course Material > Lab assignments.’

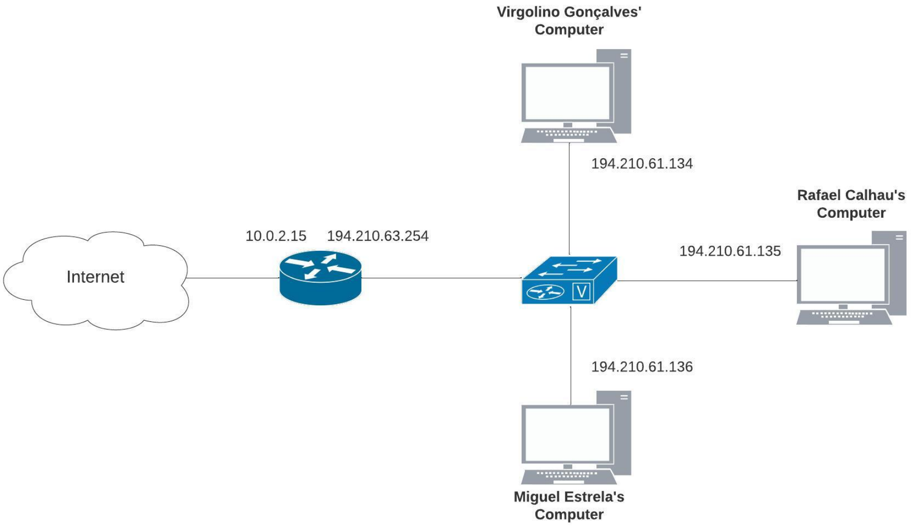

Figure 1: Diagram of the simplified network topology at IST's Satellite Lab premises.

File	**SHA-256 Value**	**Description**
trace1.pcapng	`aa3ae82d0dbbe3ec370c46477e844ee16bdbcc88e38d09df8271768518eeda20`	Network trace 1
trace2.pcapng	`da2ddeafcb22c92ec88d75e9a921e2e16500de00f4c34c86e2e170394d7e44e8`	Network trace 2
trace3.pcapng	`d445cb00e5c31486c3e1030649d0509f05614c64d74fae799ea3eb4f58802b15`	Network trace 3
sslkeylogfile.txt	`258c3e541d17c1f29f94506fb9b6c9017e62edc5786112437a8fa42304fa6c8e`	HTTPS proxy key

Mr. Prado has also confirmed the following e-mail addresses:

- Virgolino Gonçalves - virgolinogoncalves@hotmail.com
- Rafael Calhau - rafaelcalhau123@hotmail.com
- Miguel Estrela - miguel.estrela890@hotmail.com
- Ricardo Prado - ricardoprado1986@hotmail.com

In this exercise, your task is to analyze the provided digital artifacts and answer the following questions. Be sure to justify your responses by presenting all relevant evidence you uncover. Clearly explain your hypotheses and describe the steps you took to validate them.

1. Do you find any evidence of transfers involving the five hidden documents in the analyzed network traces? What can you determine about the source of these documents?
2. What can you deduce about the identity of the person(s) responsible for transferring the documents?
3. Can you establish a timeline of key events that explains how the data exfiltration occurred and how the documents ultimately ended up in João Musk's possession?
4. Based on all the evidence gathered in this investigation, what can you infer regarding the conspiracy hypothesis that initiated this inquiry? Did you find any additional evidence supporting it? If so, who might be the actors involved, and what steps would you recommend for the next phase of the investigation?

Note: Given that this exercise was emulated in a virtual environment, please consider that:

1. We used virtual machines interconnected by virtual networks running on a single host. As a result, the network has been greatly simplified when compared with a real world setting, where a much larger number of users would be connected and active.
2. The trace collection started really on **October 8th**. Therefore, the absolute timestamps recorded within the provided digital artifacts are skewed by about **1 month** in comparison to the timestamps of Lab Assignment I. For the purpose of your timeline, you must adjust the times of this trace to match those of the first assignment (go to the Time Shift, as in Tutorial 3, and apply: **-792:0:0**).

Extra Note: Assume the events of Lab Assignment II happened between Lab Assignment III and Lab Assignment I.

Deliverables

Write a forensic report that describes your findings. The deadline for this work is October 25th. Until then, you must upload to Fenix a compressed zip file containing three deliverables:

- **Report**: A document in which you answer the aforementioned questions. You must identify all relevant evidentiary items that support your claims. We recommend that you use the template that can be downloaded from the course website.
- **Evidence Artifacts:** All relevant evidence artifacts recovered during the forensic analysis. Please make sure that the respective file names and SHA-256 values are indicated in the report.
- **Auxiliary Items:** Programs, scripts, and additional documents that you have produced during the investigation which are important to justify your results must also be included.
- **Timeline:** A timeline of the most relevant events. You must identify all relevant events that support your claims. We recommend you use the template that can be downloaded from the course website.

Good luck!