INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment III

ARCO UNDERGROUND – Stage III

2023/2024

nuno.m.santos@tecnico.ulisboa.pt

Introduction

This assignment will wrap up the investigation into the “Arco Underground” case. In Lab Assignment 2, you have analyzed the hard disk images from two computers owned by César Silva Ferro, a student from IST. Following that, your focus will shift to the computer network of IST’s Department of Computer Science (DEI). Some of the documents in question appear to be associated with Prof. Eva Rocha, a faculty member of the said department. The goal of this analysis is to determine whether (and if so, how) these documents were leaked from her workstation. For this task, you’re advised to review the network traces available on the course website. As in the previous assignment, we recommend using Kali.

Scenario presentation

In the prior assignment, you made significant progress, though the findings remain inconclusive. Upon inspecting César Ferro’s workstation and backup server, several pieces of evidence emerged: (1) The backup server housed duplicates of the documents that were covertly stored in the pen drive. (2) These documents were transmitted from the workstation directly to the pen drive. (3) Initially, César had received those documents from an unidentified individual, who delivered the files to him on a separate pen drive, which César then collected from a public locker.

While the findings provided new insights, they did not conclusively determine the authenticity of the documents or identify the responsible parties. Consequently, the police questioned Mr. Ferro, but he couldn’t provide any details beyond the content of the documents. With limited leads, the police shifted their focus to the bank statement of Prof. Eva Rocha, a faculty member of DEI at IST. Under the presumption that the documents may have been stolen, the police suspected they were taken from Prof. Rocha’s workstation in her DEI office. The police subsequently returned to DEI’s premises and sought assistance from the head of IT, Mr. Golias Matos, to help identify any signs of document exfiltration across the network. As with the initial assignment, you were enlisted to aid in this investigation. Mr. Matos introduced you to the topology of the local network and provided forensic material that could potentially reveal how the documents were illicitly obtained.

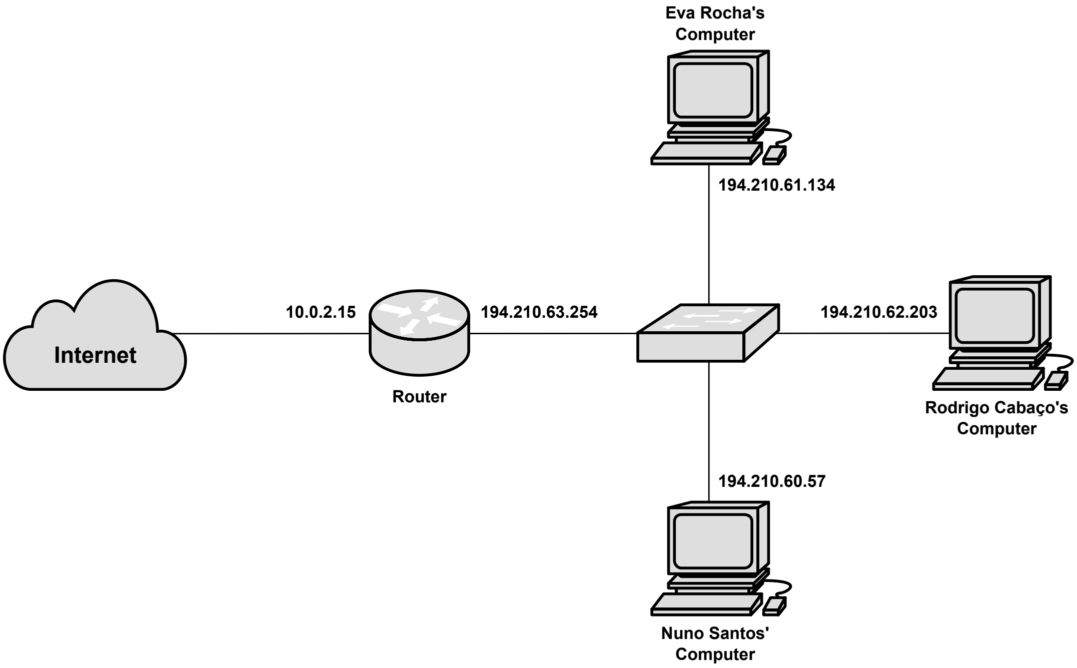

Figure 1: Diagram of the simplified network topology at DEI’s premises.

The figure above depicts a simplified reconstruction of DEI’s network topology. The network features a gateway that functions as both a router and an HTTP(S) Proxy (with the IP address 194.210.63.254).

It also includes the computers of Eva Rocha (194.210.61.134), Rodrigo Cabaço (194.210.62.203), and Nuno Santos (194.210.60.57) – these workstations belong to three professors from DEI. Notably, Prof. Cabaço currently holds the position of president at IST, while Prof. Nuno Santos instructs the Forensics Cybersecurity course. Fortuitously, due to security considerations, the HTTPS Proxy is set up to capture periodic network traffic traces. Mr. Matos has facilitated your 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 scrutinized in preceding 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 given directly as input into the tool. All relevant files are available for download under ’Course Material > Lab assignments’.

File	**SHA-256 Value**	**Description**
trace1.pcapng	`208c073305c8a467c1903e33a2cef68f885794c91bc3845b723781da2887cc5d`	Network trace 1
trace2.pcapng	`fad3df10bca45d3320cd054ea207e87d02e0645fc92e5b2dd89791b23243c7f4`	Network trace 2
trace3.pcapng	`9947619598c6f3092ecca769f107c3676a45a71134a73d56f4e6ad2532229e8c`	Network trace 3
sslkeylogfile.txt	`f0eea25f1a25afa8ce389852ada6e250b25bc47211c69a08a764eb3f696eb112`	HTTPS proxy key

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

- Eva Rocha - `eva.rrocha@proton.me`
- Nuno Santos - `nuno.santos.1970@protonmail.com`
- Rodrigo Cabaço - `presidente.rodri@mail.com`
- Golias Matos - `golias.matos@mail.com`

In this exercise, your job is to analyze the digital artifacts provided above and answer the following questions. Justify your answers by providing all the relevant evidence you can find. Make sure to explain your hypotheses and how you have proceeded to validate them.

1. Do you find any evidence of transfers involving the documents in the analyzed network traces? What can you tell about the source and authenticity of these documents?
2. What can you tell about the identity of the person(s) responsible for transferring the documents?
3. Can you establish a timeline of all relevant events that clarifies how the entire data exfiltration has taken place and the documents ended up in César Ferro’s hands?
4. From all the collected evidence in this investigation, what can you deduce about the motivation of the actor(s) responsible for the data exfiltration?

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 **September 25th**. Therefore, the absolute timestamps recorded within the provided digital artifacts are skewed by **2 weeks** in comparison to the timestamps of Lab Assignment II. For the purpose of your timeline, you must adjust the times of this trace to match those of the previous assignment **(subtract those 2 weeks, i.e., 14 days)**.

Deliverables

Write a forensic report that describes your findings. The deadline for this work is October 27th. 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 MD5 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.

Good luck!