INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment II

DEEP BREACH – Stage II

2020/2021

nuno.m.santos@tecnico.ulisboa.pt

Introduction

We now begin the concrete investigation of the "Deep Breach" case. This assignment will introduce you to this case and give you access to digital artifacts that you need to analyze in search of relevant evidence. This work will help you develop multiple skills in computer forensics. In this exercise, you will not immediately employ the training in vulnerability analysis that you have gained in the first assignment. However, this training will be fundamental in the third part of this project to conclude this investigation. The digital artifacts required for the second assignment are available on the course website. We suggest you analyze them using the Kali Linux distribution on a forensically sound virtual machine.

Scenario presentation

Two troubling documents have been recently published on PharmaLeaks, a well-known whistleblower website dedicated to the dissemination of information about scandals in the pharmaceutical industry. Apparently, these files have leaked from a major pharmaceutical company named XFarma. One of them consists of an internal technical report written by Penelope Pearson. Penelope is XFarma's technical director and head of the research team responsible for the development of a new vaccine for COVID-19. This report makes an account of a series of vaccine tests conducted in four trial subject populations. These results show that, in its current stage, XFarma's vaccine is not ready for public release as it causes adverse side effects in 75% of the population groups. However, despite these unsuccessful results, the company seems determined to keep pushing for the release of the vaccine to market in record time. This is suggested by an email (the second leaked document) sent by XFarma's CEO John Carson where he allegedly states that the vaccine's development has been authorized to enter into the production stage. Should these documents confirmed to be authentic, they reveal a major cover-up attempt to bypass existing vaccine development regulations which poses serious risks to public health and constitutes a crime.

The police authorities followed suit and started an investigation. They began by collecting the leaked documents from PharmaLeaks, and then interviewed Mr. John Carson who stated:

> "This email is fake! I did not give green light for our vaccine in its current development stage. This is a blatant lie, an attempt to discredit XFarma and undermine our reputation."

The authorities have then decided to track the source of the PharmaLeaks files, and investigate if (and how) the files have actually leaked from XFarma. To perform this job, they hired you to incorporate their digital forensics team. A first clue has pointed them to Rick Chick, an individual who has become suspect of having uploaded the files to PharmaLeaks. The team conducted a search on Rick's residence and found two computers: a *workstation* and a *backup server*. These computers were connected to the local network which also had Internet connectivity. The first response officer seized both computers and created two forensically sound images of the computers' hard disks. The following table lists all the collected digital artifact files. For each file, it indicates the file name, MD5 value, and a brief description (these files can be downloaded from the course website in Course Material > Lab assignments):

File	MD5 Value	Description
email.pdf	`dc1abdb8679d3ca10a7f40b5b6436a35`	Alleged leaked email from XFarma
report.pdf	`8e5a62390ef3e86a40f91be4a7eff550`	Alleged leaked technical report from XFarma
rick_disk.tar.gz	`fc28375fa552708772bb35f83d79cbca`	Hard disk image of Rick's workstation
backup_disk.tar.gz	`8fc38ceca9ae6b1315f9fdd33f74a3cc`	Hard disk image of Rick's backup server

In this exercise, your job is to analyze these digital artifacts and answer the following four 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. Can you suggest why the authorities have considered Rick to be a potential suspect of uploading the files to PharmaLeaks?

2. Do you find any traces of the PharmaLeaks files on Rick's computers?

3. Can you find any evidence that PharmaLeaks file have indeed been uploaded from Rick's computers, and what the source of these files may have been? Establish a timeline of relevant events.

4. What can you tell about the identity of the person(s) responsible for leaking the files?

Deliverables

Write a forensic report that describes your findings. The deadline for this work is November 20^{nd}. Until then, you must upload to Fenix a compressed zip file containing three deliverables:

- **Digital Forensic Report**: A document in which you answer the aforementioned questions. You must identify all relevant evidentiary items that support your claims. We recommend you to 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!